



CentOS

Community ENTERprise Operating System

E-Book CentOS Network Administrator

Muhammad An'im Fatahna

KATA PENGANTAR

Linux merupakan sebuah Sistem Operasi yang banyak digunakan untuk membuat dan mengembangkan project server, kehandalan, kemudahan dan keamanan akan anda temui di Sistem Operasi Linux, sehingga tidak salah jika saat ini Linux sudah banyak dipergunakan terutama di lingkup perusahaan Skala Enterprise. Sistem Operasi yang paling populer mengenai kehandalan adalah RHEL (*Red Hat Enterprise Linux*). RHEL merupakan software berbayar, sehingga jika anda ingin menggunakannya harus membayar sebuah lisence agar anda bisa menjalankan seluruh sistem secara sempurna. Namun jangan khawatir sebab anda bisa menggunakan sebuah Distribusi Linux yang hampir serupa dengan RHEL yaitu Linux CentOS.

CentOS (Community ENTerprise Operating System) merupakan Distro Linux Open Source yang dipergunakan dalam skala Enterprise dan dibuat dari source code Red Hat Enterprise (RHEL) yang dikembangkan oleh sebuah komunitas yang disebut CentOS Project. CentOS pada dasarnya dibuat dari source code Red Hat Enterprise. Software ini dirilis dibawah General Public License (GPL) yang selanjutnya dikembangkan oleh sebuah komunitas yang disebut CentOS Project. Kedekatannya dengan RHEL menyebabkan CentOS memiliki dukungan yang nyaris sama, sehingga beberapa vendor hardware dan Software yang saat ini support dengan RHEL akan berlaku sama dengan CentOS.

Didalam buku ini penulis mencoba menjelaskan step by step dalam membangun infrastruktur jaringan dimulai dari dasar hingga ketinggian lebih tinggi. Langkah demi langkah dibahas dengan singkat, padat dan mudah dipahami merupakan kelebihan tersendiri dalam buku ini. Selain itu juga terdapat beberapa tips dan trik bagaimana cara menyelesaikan troubleshooting ketika anda menemui hambatan dan kesulitan dalam menerapkan tutorial di buku ini.

Akhir kata tidak ada yang sempurna dalam sebuah penciptaan seorang manusia, sehingga jika terdapat beberapa kekurangan yang terdapat di dalam buku ini maka penulis mengharapkan partisipasi pembaca dalam memberikan saran dan kritik membangun, sehingga bisa menjadi pelajaran tersendiri bagi penulis.

Surabaya, 30 Juli 2011

Muhammad An'im Fatahna

<http://mafatahna.web.id>

Daftar Isi

Halaman Judul	i
Halaman Copyright	ii
Halaman Persembahan	iii
Kata Pengantar	iv
Daftar Isi	v
1. Pendahuluan	x
1.1. Pengenalan CentOS	x
1.2. Instalasi CentOS	x
2. Memulai dengan CentOS	x
2.1. Memahami Perintah Dasar Linux	x
2.2. Editor File	x
2.3. Menggunakan YUM	x
2.4. Repository CentOS	x
2.5. Repository Pihak Ketiga	x
2.6. Konfigurasi IP Address	x
2.7. Memahami File Permissions	x
3. SSH Server	x
3.1. Menggunakan Protokol 2 pada SSH	x
3.2. Mengganti Port Default	x
3.3. Membatasi Akses SSH pada User	x
3.4. Konfigurasi Idle Timeout	x
3.5. Disabled Login Root via SSH	x
4. DNS Server	x
4.1. Instalasi DNS Server	x
4.2. Konfigurasi DNS Server	x
4.3. Uji Coba	x
4.4. Konfigurasi DNS Slave	x
4.5. Konfigurasi Multidomain	x
4.6. Registrasi Domain ke Pandi	x
5. DHCP Server	x
5.1. Instalasi DHCP Server	x
5.2. Konfigurasi DHCP Server	x
5.3. Konfigurasi DHCP Server 2 Network	x
6. File Sharing	x
6.1. Pengertian Samba	x
6.2. Instalasi Samba	x
6.3. Membatasi Samba	x
6.4. Akses Samba dari Klien	x
6.5. Menambahkan Fitur Recycle Bin	x
7. FTP Server	x
7.1. Instalasi VSFTPD	x
7.2. Mengaktifkan User Anonymous	x
7.3. Membatasi Akses User	x
7.4. Membatasi Akses User Dengan Chroot	x
7.5. Menganti Direktori Default User Anonymous	x
7.6. Sistem Keamanan Dengan OpenSSL	x
7.7. Koneksi Klien Menggunakan SSL	x
8. Web Server	x
8.1. Instalasi Web Server	x

8.2. Membuat Multiple Domain.....	X
8.3. Redirect Domain	X
8.4. Autentikasi Web Server	X
8.5. Meningkatkan Keamanan dengan SSL	X
8.6. OpenSSL dengan Multidomain.....	X
8.7. Instalasi MySQL dan PHP	X
8.8. Instalasi PHPMyadmin.....	X
8.9. Monitoring Log Apache dengan Visitors	X
8.10. Monitoring Log Apache dengan Awstats	X
8.11. Monitoring Log Apache dengan Piwik	X
9. Proxy Server	X
9.1. Instalasi Squid	X
9.2. Autentikasi Password	X
9.3. Filtering Content	X
9.4. Limit Berdasarkan Waktu	X
9.5. Partisi Cache di Squid	X
9.6. Transparent Proxy	X
9.7. Membatasi Bandwidth dengan Delay Pools.....	X
9.8. File Squid.conf.....	X

Pendahuluan

1.1. Pengenalan CentOS

CentOS (Community ENTerprise Operating System) merupakan Distro Linux yang cocok dipergunakan dalam skala Enterprise selain itu juga gratis. CentOS di buat dari source code Red Hat Enterprise (RHEL) yang dikembangkan oleh sebuah komunitas yang disebut CentOS Project. CentOS pada dasarnya dibuat dari source code Red Hat Enterprise yang bisa di unduh di <ftp://mirrors.kernel.org/redhat/redhat/linux/enterprise>. Software ini dirilis dibawah General Public License (GPL) yang selanjutnya dikembangkan oleh sebuah komunitas yang disebut CentOS Project, untuk lebih jelasnya silahkan mengunjungi situs resminya di <http://www.centos.org>.

CentOS saat ini sudah digunakan di seluruh dunia, beberapa komunitas, mailing list, IRC dan website tutorial dibuka dengan lebar agar semua orang bisa mempelajarinya. Sehingga untuk dukungan dan support mengenai bagaimana membuat sebuah server dengan distro ini anda tidak perlu khawatir, sebab seluruh pengguna yang tersebar di dunia yang aktif di komunitas, siap untuk membantu anda.

Ada 2 alasan dasar kenapa penulis memilih CentOS sebagai sistem operasi utama sebuah server. Dalam hal dukungan, CentOS memiliki dukungan yang lebih baik, dukungan mengenai software dan hardware adalah salah satu alasan yang terpenting dari sebuah Distro skala Enterprise, selain itu anda tidak perlu khawatir, dengan dukungan software paket untuk update sebab jika anda menggunakan sebuah Operating System commercial maka anda harus membayar terlebih dahulu agar mendapatkan update yang terbaru, lain halnya dengan CentOS, dimana vendor CentOS Project memberikan support dalam produknya secara berkala. Jika anda ingin membayar dengan alasan rasa terima kasih atas dukungan yang diberikan bisa saja, tetapi tidak wajib. Biasanya Distro Linux memiliki dukungan (Life Cycles) yang relatif pendek, disini penulis tidak akan memberikan contoh distro yang dijadikan perbandingan. Misalnya sebuah distro memiliki dukungan hanya 2 tahun, setelah 2 tahun kedepan diharuskan untuk melakukan upgrade ke release yang terbaru sebab dari itu anda akan memiliki sedikit pilihan yaitu upgrade ke release terbaru atau membiarkan sistem tersebut dan menghiraukan update security pada Distro tersebut, padahal security adalah hal yang terpenting.

Diasumsikan anda memiliki sebuah server, anda ingin server tersebut dalam kondisi aman dan terjaga dalam paket yang digunakan, yaitu dengan cara upgrade sistem. Ada beberapa kemungkinan terburuk yang akan anda alami.

Pertama, dalam proses upgrade sistem bukanlah perkara mudah, biasanya proses upgrade merupakan pergantian software yang lama diganti dengan software yang terbaru sehingga pasti akan ada beberapa software aplikasi lama yang tidak support dengan aplikasi yang terbaru sesuai dengan konfigurasi lama.

Kedua, setelah upgrade versi paket software yang terbaru, kebanyakan memiliki perubahan signifikan yang berbeda dengan versi sebelumnya. Jika server anda adalah sebuah server yang harus online 24 jam maka anda menginginkan server tersebut tetap berjalan dengan baik setelah proses upgrade dan meminimalisir downtime. Tetapi pada dasarnya proses upgrade sistem akan mengganti semua software menjadi yang terbaru dan tidak mempedulikan konfigurasi lama anda, dengan begitu anda harus menulis ulang source code konfigurasi anda yang lama dan melakukan pengetestan pada semua konfigurasi, dan hal tersebut dilakukan

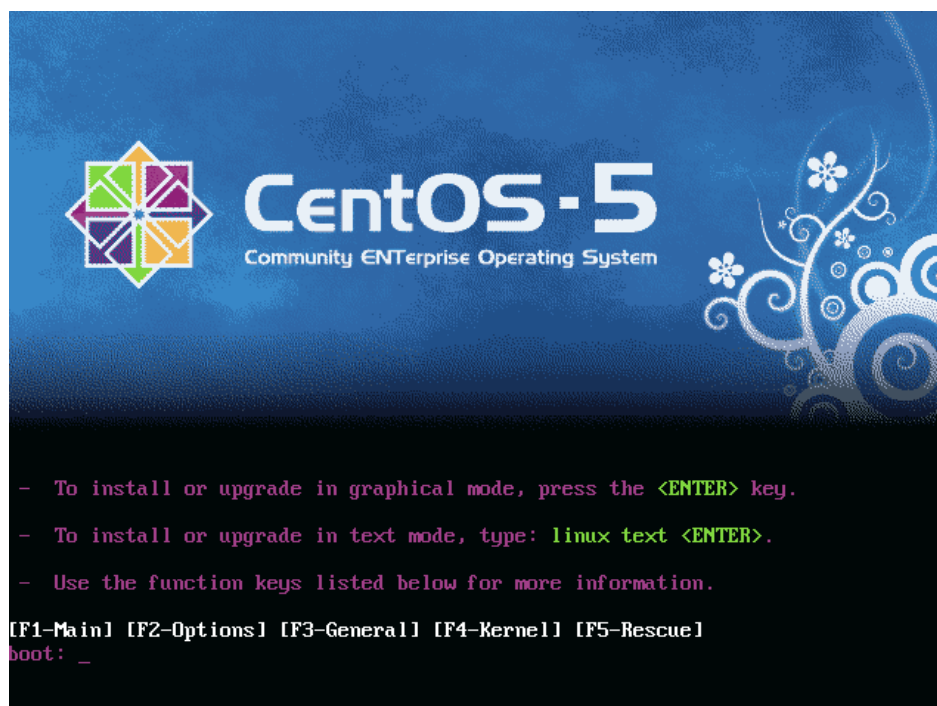
untuk memastikan bahwa sistem anda bisa berjalan dengan baik, hal tersebut merupakan pekerjaan besar dan selain itu anda mengakibatkan downtime pada server yang relatif lebih lama.

CentOS dengan platform Linux Enterprise mencegah 2 permasalahan tersebut sebab release pada CentOS memiliki release yang memiliki kesamaan dengan versi sebelumnya hingga beberapa tahun, sehingga CentOS memiliki waktu dukungan secara berkala dari 5 tahun sampai dengan 10 tahun. hal tersebut penting diperhatikan sebab bisa memberikan anda banyak kesempatan untuk upgrade dan melakukan testing pada versi yang terbaru. Beberapa hal yang perlu diperhatikan bahwa Linux CentOS merupakan salah satu turunan dari Distro Red Hat yang saat ini masih menguasai pangsa pasar server seluruh dunia, CentOS saat ini menjadi alternatif Open Source yang digunakan hampir sebagian perusahaan hosting didunia.

1.2. Instalasi CentOS

Tahapan yang perlu dipersiapkan sebelum instalasi CentOS adalah mempersiapkan media yang digunakan. Anda bisa menggunakan media DVD yang sudah terlampir didalam buku ini, atau bisa juga menggunakan media USB Drive yaitu dengan mendownload terlebih dahulu disitus resminya <http://mirror.centos.org/centos/>, anda bisa menggunakan beberapa software seperti unetbooting untuk membuat Live USB CentOS.

Berikut adalah langkah-langkah instalasi CentOS. Nyalakan komputer anda, letakkan DVD kedalam DVD-ROM, tunggu beberapa saat hingga anda melihat tampilan pertama instalasi. Jika dalam proses booting tersebut tidak ada maka, maka cek kembali konfigurasi pada BIOS di PC anda dan pastikan *first boot* sudah di setting CD/DVD. Lanjutkan tekan tombol *enter* untuk memulai instalasi



Selanjutnya merupakan proses testing kelayakan DVD yang dipergunakan. Sehingga sebelum melanjutkan proses instalasi anda bisa melakukan pengecekan terlebih dahulu, sebab hal tersebut untuk meminimalisir proses gagalnya instalasi disebabkan DVD yang digunakan

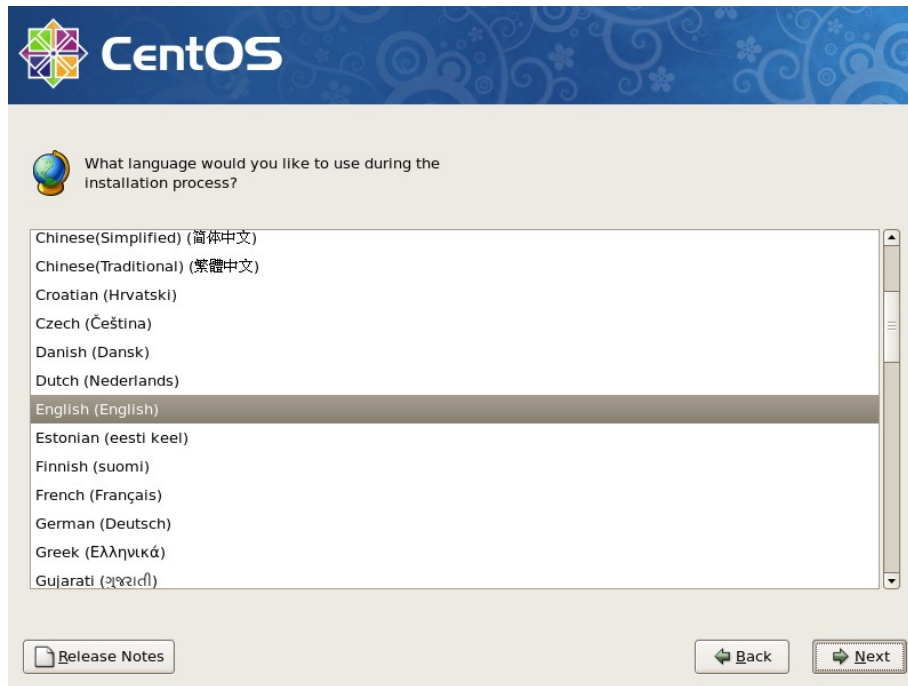
error atau corrupt. Proses pengecekan ini memakan waktu yang lamayan lama sehingga jika kondisi media yang anda pergunakan yakin masih layak digunakan maka anda bisa mengabaikannya dengan memilih Skip



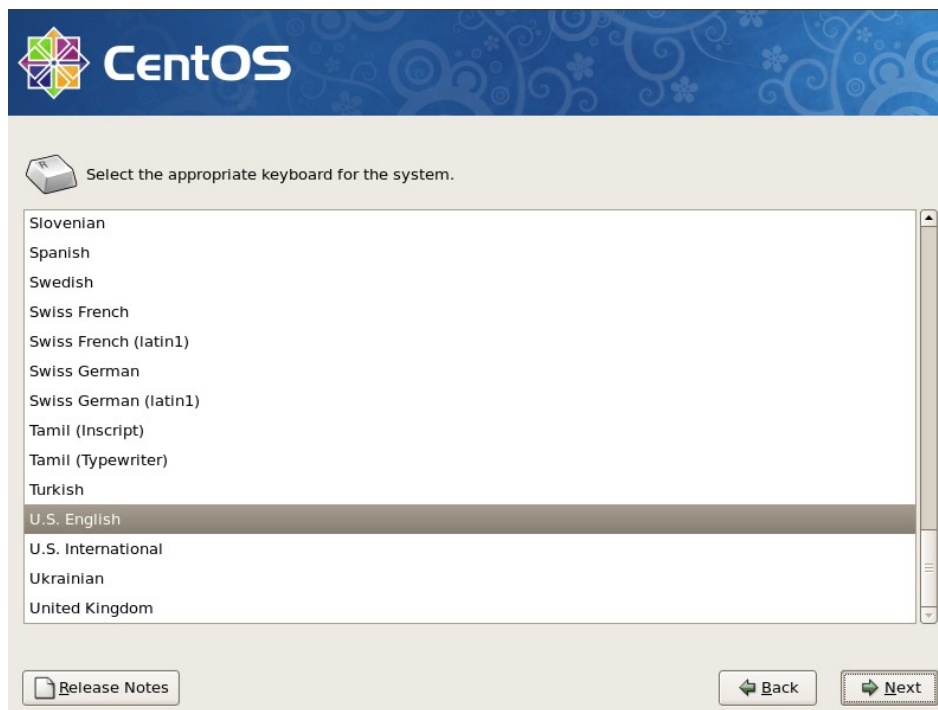
Tunggu beberapa saat hingga proses pengecekan media selesai, jika anda memilih *Skip* maka anda akan melihat tampilan instalasi *graphical* pada layar. Anda dapat klik *Release Notes* yang menjelaskan informasi versi dari CentOS yang sedang anda install. Klik *Next* untuk melanjutkan



Langkah selanjutnya merupakan bahasa yang digunakan ketika proses instalasi berlangsung, secara *default* menggunakan bahasa English, selain itu anda juga bisa memilih bahasa lain agar memudahkan dalam proses instalasi. Klik *Next* untuk melanjutkan

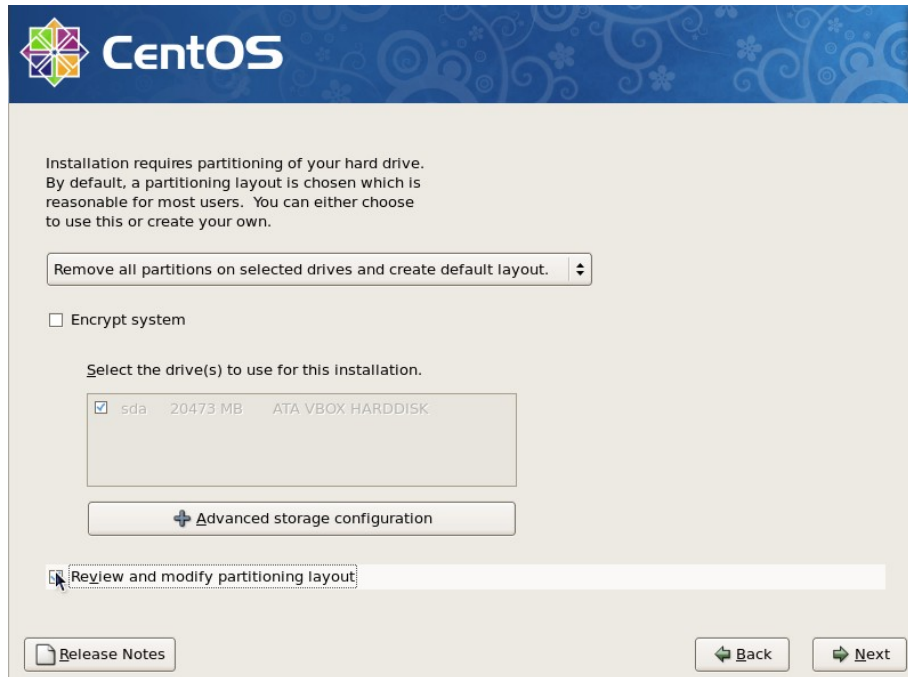


Selanjutnya anda juga bisa memilih *standart keyboard* yang digunakan, silahkan pilih beberapa tipe *keyboard* yang sesuai. Klik *Next*



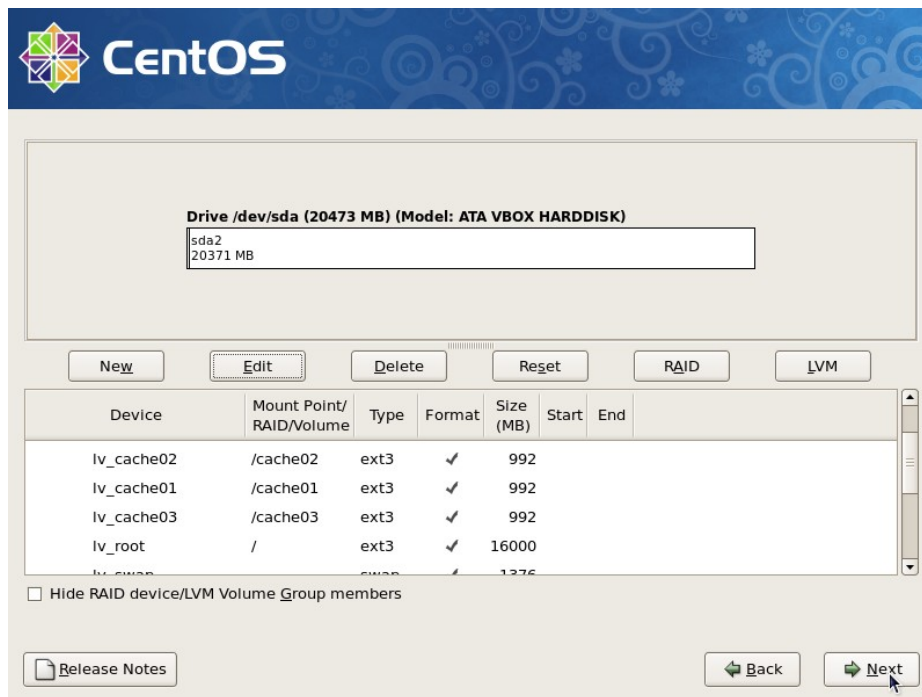
Selanjutnya anda akan dihadapkan dengan proses partisi *harddisk*. Secara *default* partisi CentOS hanya membutuhkan 3 partisi yaitu : *root (/)*, *swap* dan direktori *home (/home)*. Proses penentuan partisi tergantung dengan kebutuhan server yang digunakan, penulis memberikan contoh partisi yang digunakan untuk Proxy Server. Dalam membuat sebuah Server Proxy dibutuhkan beberapa partisi yang penting yaitu : *root (/)*, *swap* dan *cache*. Partisi pertama adalah *root* yang digunakan sebagai lokasi *file system* utama yang menjalankan berbagai *service*. Kedua *swap* merupakan cadangan memori yang digunakan

dalam *Linux System* secara default ukuran swap adalah 2 kali besar memori. Ketiga cache digunakan untuk penyimpanan *cache* ketika klien melakukan aktifitas browsing. Dengan menyediakan partisi tersendiri maka *cache* bisa disimpan dan dikelola lebih maksimal. Langkah-langkah partisi silahkan pilih menu pada *drop down* “*Remove all partitions on selected drives and create default layout*”, selanjutnya pilih “*Review and modify partitioning layout*” agar partisi bisa dimodifikasi



Pada proses partisi ini menggunakan Harddisk dengan kapasitas 20 GB, dibagi menjadi beberapa partisi meliputi *root*, *swap* dan *cache*. Partisi *cache* memiliki 3 partisi yaitu *cache01*, *cache02* dan *cache03*. Masing-masing *cache* memiliki kapasitas 1 GB. Jumlah kapasitas swap 1,3 GB dan sisanya digunakan sebagai *root* (/). klik *Next* untuk memulai partisi.

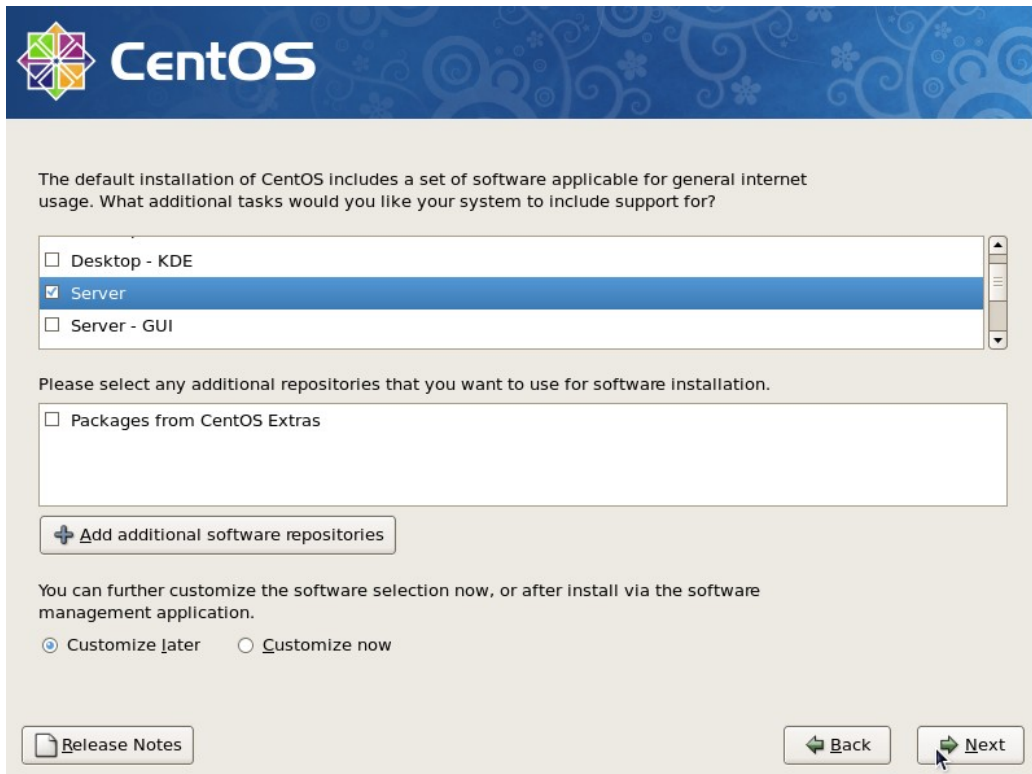
selanjutnya memulai proses instalasi. Tekan tombol *Next*



Ikuti beberapa pertanyaan pada dialog selanjutnya meliputi pengaturan *time* dan konfigurasi *IP Address*, pada proses tersebut bisa anda lewati yaitu dengan menekan tombol *Next* sebab konfigurasi tersebut bisa disetting kembali ketika proses instalasi selesai. Selanjutnya anda diminta memasukkan password *root*. Hak akses *root* dipergunakan untuk mengontrol semua system sehingga diharapkan menggunakan password yang sulit untuk ditebak



CentOS selain digunakan sebagai *Server*, juga bisa dipergunakan sebagai sistem pada Dekstop anda dengan dasar tampilan KDE dan GNOME. Pilih *Server* lanjutkan dengan menekan tombol *Next*



Tunggu beberapa saat hingga proses instalasi beberapa paket yang dibutuhkan untuk sebuah *Server* selesai.



Setelah proses instalasi berlangsung akan terlihat informasi bahwa proses instalasi berhasil, agar instalasi tersebut sempurna *restart* komputer anda dengan menekan tombol *Reboot*



Selamat proses instalasi selesai, anda bisa memulai membuat sebuah server.

```
CentOS release 5.5 (Final)
Kernel 2.6.18-194.el5 on an i686

localhost login: _
```

Memulai Dengan CentOS

CentOS (Community ENTERprise Operating System) merupakan Operating System yang sangat disarankan jika dipergunakan sebagai server, sama halnya dengan beberapa Distro yang lain CentOS dalam implementasinya hampir semua code dan perintah-perintah dasar hampir sepenuhnya menggunakan mode text. CentOS pada dasarnya memiliki banyak sekali perintah dasar sehingga kali ini penulis hanya menjelaskan beberapa perintah yang secara umum dipergunakan untuk implementasi Project Server pada bab selanjutnya.

2.1 Memahami Perintah Dasar Linux

Jika anda belum pernah menjalankan perintah dasar Linux maka anda perlu memperhatikan beberapa perintah dasar yang sering sekali dipergunakan dalam membuat sebuah server. Tetapi jika anda sudah mengetahui tentang seluk beluk perintah-perintah yang digunakan, maka anda bisa melewati bab ini dan melanjutkan pada bab berikutnya.

pwd

Fungsi perintah pwd adalah perintah yang bisa anda pergunakan untuk mengetahui dimana lokasi direktori anda berada. misalnya anda ingin mengedit/membuat sebuah file, sedangkan anda tidak tahu apakah dalam posisi sub directory yang benar atau tidak, maka pwd akan bisa membantu anda menghindari kesalahan ketika mengedit/membuat sebuah file

```
[root@srv1 etc]# pwd
/var/named/chroot/etc
[root@srv1 etc]#
```

Terlihat saat ini anda berada pada directory chroot (/var/named/chroot/etc). Perintah pwd akan sangat membantu anda sebelum menjalankan perintah.

mkdir

Jika anda ingin membuat sebuah directory, maka anda bisa menggunakan perintah ini, proses pembuatan directory hanya bisa digunakan sekali dengan sebuah nama, misalnya

```
[root@srv1 home]# mkdir data
```

Setelah anda menjalankan perintah tersebut maka secara tidak langsung anda sudah berhasil membuat sebuah direktori dalam directory /home, setelah anda membuat directory anda tidak bisa membuat directory dengan nama yang sama seperti pada contoh dibawah ini

```
[root@srv1 home]# mkdir data
mkdir: cannot create directory `data': File exists
```

Terlihat bahwa anda tidak bisa membuat sebuah directory. Perintah mkdir juga bisa membuat beberapa direktori secara langsung, misalnya

```
[root@srv1 home]# mkdir -p data/linux/server
[root@srv1 home]# tree
.
|-- data
    |-- linux
```

```
    `-- server

3 directory, 0 files
[root@srv1 home]#
```

Dari perintah tersebut yaitu dengan menggunakan parameter -p anda bisa membuat beberapa directory secara bersamaan.

mv

Dengan perintah mv anda bisa memindah/menganti nama dari directory/file, misalnya anda ingin memindahkan file yang terdapat di /etc, anda ingin memindahkannya ke directory /home maka anda bisa melakukannya dengan perintah berikut ini

```
[root@srv1 etc]# mv /etc/server.txt /home/data/
[root@srv1 etc]# ls /home/data/
linux server.txt
[root@srv1 etc]#
```

Tulisan yang tercetak tebal adalah contoh file yang penulis pergunakan sebagai contoh, terlihat file server.txt sebelumnya berada pada directory /etc dipindah ke directory /home. Selain digunakan untuk memindahkan file/direktori, perintah mv juga bisa dipergunakan untuk mengganti nama file.

```
[root@srv1 data]# ls
linux server.txt
[root@srv1 data]# mv server.txt linux.txt
[root@srv1 data]# ls
linux linux.txt
[root@srv1 data]#
```

Dengan perintah mv, file sebelumnya dengan nama server.txt diganti dengan nama linux.txt

cd

Digunakan untuk berpindah ke lokasi directory lain. Misalnya anda saat ini berada di directory /home dan ingin berpindah ke directory lain, maka anda bisa menggunakan perintah ini, berikut beberapa contoh penerapan perintah cd

```
[root@srv1 server]# pwd
/home/data/linux/server
[root@srv1 server]# cd ..
[root@srv1 linux]# pwd
/home/data/linux
```

Perintah dasar cd<space>.. Pergunakan untuk berpindah satu tahap directory di atasnya

```
[root@srv1 linux]# cd\
>
[root@srv1 ~]# pwd
/root
```

perintah dasar `cd` digunakan untuk berpindah ke directory utama yaitu root. Berbeda dengan perintah hanya “`cd`” perintah tersebut digunakan untuk masuk pada default user

```
[user1@srv1 data]$ pwd
/home/data
[user1@srv1 data]$ cd
[user1@srv1 ~]$ pwd
/home/user1
[user1@srv1 ~]$
```

Maka dengan perintah tersebut, jika anda menggunakan user1 maka secara otomatis anda akan berada di directory home dengan nama user anda. Apabila anda ingin masuk di direktori anda bisa menggunakan perintah dibawah ini

```
[user1@srv1 ~]$ cd /home/data/linux/server/
[user1@srv1 server]$ pwd
/home/data/linux/server
[user1@srv1 server]$
```

Setelah masuk pada direktori yang di inginkan, anda bisa menggunakan perintah `pwd` untuk melihat lokasi anda berada

touch

Perintah ini digunakan untuk membuat sebuah file, untuk membuat file anda bisa membuatnya tidak harus dilokasi directory anda berada, tetapi anda bisa membuat file darimanapun anda berada seperti pada contoh berikut ini

```
[root@srv1 data]# pwd
/home/data
[root@srv1 data]# touch data.txt
[root@srv1 data]# ls
data.txt linux linux.txt
[root@srv1 data]# touch /home/data/linux/server/data.txt
[root@srv1 data]# ls /home/data/linux/server/
data.txt
```

rmdir

Perintah `rmdir` digunakan untuk menghapus directory, tetapi kekurangan perintah `rmdir` ini tidak bisa menghapus directory yang didalamnya masih terdapat file, coba perhatikan contoh dibawah ini

```
[root@srv1 linux]# rmdir server/
[root@srv1 home]# rmdir data
rmdir: data: Directory not empty
```

Pada perintah pertama directory `rmdir` mampu menghapus directory server, tetapi pada perintah yang kedua `rmdir` tidak bisa menghapus directory data dengan di ikuti informasi error “`rmdir : data : Directory not empty`” yang artinya `rmdir` tidak bisa menghapus directory yang masih mempunyai file didalamnya

rm

Secara default perintah `rm` digunakan untuk menghapus sebuah file, tetapi `rm` sendiri bisa menghapus directory secara manual hingga directory yang didalamnya masih memiliki file, yaitu dengan menambahkan beberapa parameter, seperti contoh berikut ini

```
[root@srv1 home]# ls
data data.txt user1
[root@srv1 home]# rm -fr data
[root@srv1 home]# ls
data.txt user1
[root@srv1 home]#
```

Kemampuannya yang multifungsi tersebut semakin membuat pengguna merasa nyaman dengan menggunakan perintah `rm` dibandingkan dengan perintah `rmdir`.

cat

Perintah `cat` digunakan untuk melihat isi file tanpa harus membuka file terlebih dahulu, `cat` sering dipergunakan untuk melihat hasil preview sebuah file. Anda bisa menggunakan perintah ini seperti pada contoh berikut ini

```
[root@srv1 home]# cat data.txt
pesan singkat untuk anda
[root@srv1 home]#
```

Kelemahan perintah ini jika digunakan untuk preview isi file yang memiliki banyak tulisan, sebab `cat` akan melakukan review semua isi file hingga isi paling dibawah, sehingga jika digunakan untuk mengkoreksi hasil tulisan akan mengalami kendala sebab pengguna akan kesulitan dalam melihat isi file paling atas.

more

Perintah `more` memiliki kesamaan fungsi dengan perintah `cat`, yang membedakannya hanyalah dari segi review isi file. Jika anda menggunakan `more` maka anda bisa melihat isi file secara bertahap sehingga perintah `more` terkadang lebih banyak digunakan dari pada perintah `cat`.

2.2 Editor File

CentOS memiliki berapa editor text yang digunakan untuk memodifikasi isi file, selain itu editor ini juga digunakan untuk membuat sebuah file. Pada kenyataannya terdapat beberapa editor yang digunakan untuk kebutuhan editing text, misalnya `vi/vim`, `pico/nano` dan `mcedit`. Kali ini penulis hanya menjelaskan editor text `vim`, sebab `vim` merupakan editor yang saat ini paling populer untuk editor text selain itu juga lebih menarik sebab `vim` disertai beberapa perpaduan warna yang bisa memudahkan para scripting dan programming dalam menuliskan source code.

Editor VIM

`vim` merupakan editor yang selalu ada pada Operating System Unix/Linux, sebab `vim` merupakan editor default yang secara otomatis terinstall pada sistem tersebut. Seperti halnya editor notepad yang selalu ada pada Microsoft Windows. Berbeda dengan `vim`, `vim` terkesan sulit untuk digunakan, kesulitan pertama yang pasti akan dihadapi jika anda sudah terbiasa

dengan editor notepad dengan disertai beberapa menu yang terdapat ditoolbar yang memudahkan para pengguna, dalam vim berbeda. Vim tidak memiliki toolbar dan perintahnya pun tersembunyi. Harapannya dengan ulasan seputar vim anda bisa semakin terbiasa dengan editor tersebut. Vim seharusnya secara default sudah terinstall di CentOS, tetapi tidak ada salahnya untuk melakukan pengecekan terlebih dahulu dengan perintah dibawah ini

```
[root@srv1 home]# rpm -qa | grep vim
vim-common-7.0.109-6.el5
vim-minimal-7.0.109-6.el5
vim-enhanced-7.0.109-6.el5
[root@srv1 home]#
```

Output dari perintah tersebut menjelaskan bahwa, vim sudah terinstall pada sistem. Maka langkah selanjutnya adalah melakukan editing text dengan vim yaitu membuat terlebih dahulu file yang akan anda edit dengan perintah touch, langkah selanjutnya adalah memulai editor vim seperti pada contoh berikut ini

```
[root@srv1 home]# touch file
[root@srv1 home]# vim file
```

Setelah perintah vim dijalankan untuk memulainya anda bisa menekan tombol [i] untuk memulai menulis text atau code, berikut ini adalah tampilan utama setelah anda mengedit file dengan perintah vim



Dalam gambar tersebut pada baris pertama yaitu “Mencoba menulis Text” adalah tulisan pertama setelah anda menekan tombol [i], petunjuk dibawah yaitu (– INSERT –) menunjukkan bahwa anda bisa memulai menulis, sedangkan nomor yang terletak dikanan bawah (1. 20) merupakan informasi bahwa lokasi ketika tulisan diatas pada baris 1 dan jumlah

Berpindah Text

- [h] : Berpidah satu karakter ke kiri
- [j] : Berpidah satu karakter ke bawah
- [k] : Berpidah satu karakter ke atas
- [l] : Berpidah satu karakter ke kanan
- [w] : Maju satu kata (berikutnya)
- [b] : Mundur satu kata (sebelumnya)

Pembatalan

- [u] : Pembatalkan penghapusan (undo)
- [U] : Pembatalkan penghapusan semua dalam satu line (undo)
- [ctrl + r] : Mengembalikan penghapusan (redo)

Perintah Akhir

- [:wq] : Menyimpan file dan keluar
- [:q] : Keluar dari editor
- [:q!] : Keluar dari aplikasi editor tanpa menyimpang file
- [:w] : Menyimpang text yang sudah ditulis

Pencarian Text

Perintah dasar untuk mencari text di vim adalah /<kata>, sehingga ketika anda menekan tombol Esc untuk memulai anda bisa menetikkan parameter

```
/<kata_yang_dicari>
```

Selanjutnya untuk melanjutkan pencarian kata bisa menekan tombol [n] atau kembali mencari (opposite) dengan perintah [N].

2.3 Menggunakan YUM

Langkah yang tepat agar server yang anda berjalan dengan baik, maka usahakan sistem selalu up to date. Update tidak hanya digunakan agar bugs yang terdapat pada Operating System diperbaiki, tetapi juga dipergunakan untuk meningkatkan kinerja server dengan update beberapa software yang dibutuhkan.

Yum (Yellowdog Updater Modified) merupakan perintah yang digunakan untuk mencari paket, install dan update sistem dengan mudah serta memiliki hasil yang maksimal. Anda bisa dengan mudah update sistem anda saat ini dengan perintah yum update, perintah tersebut cukup digunakan untuk update seluruh sistem. Yum sangat powerful digunakan untuk mencari beberapa paket yang terdapat direpository dan mampu mencari sendiri beberapa paket dependency yang dibutuhkan ketika instalasi berlangsung.

Mengenal Paket RPM

CentOS menggunakan paket RPM sebagai paket sistem, RPM tidak hanya sebuah jenis software paket di dalam Operating System, tetapi juga sebagai semua dasar paket software yang digunakan di CentOS. Kemudahan yang diberikan RPM ketika proses instalasi mungkin adalah sebuah alasan kenapa Enterprise Linux menggunakan paket ini (RPM) di dalam sistemnya. beberapa Distro telah banyak yang menggunakan paket RPM, seperti Fedora, Mandriva dan scientificlinux. Yum adalah manajemen sistem paket yang ditujukan kepada

Distro Linux berbasis RPM, sedangkan RPM sendiri dibuat oleh Seth Vidal yang saat ini bekerja di Red Hat. Selain itu yum adalah standart tools yang digunakan oleh seluruh Distro Linux berbasis RPM seperti halnya SUSE dengan paket sistem YaST

2.4 Repository CentOS

Dalam administrasi sistem Linux CentOS secara praktis tidak jauh berbeda dengan RHEL dan Fedora sehingga secara tidak langsung jika anda saat ini sudah pernah menggunakan salah satu dari Distro yang sudah penulis sebutkan, maka anda tidak akan kesulitan dalam menerapkan perintah tersebut di CentOS. Beberapa hal yang perlu diperhatikan ketika menggunakan CentOS adalah perihal repository. Repository adalah kumpulan beberapa paket yang terkumpul secara lengkap, sehingga memudahkan pengguna dalam proses instalasi, update dan upgrade sistem. Secara default lokasi repository bisa anda lihat di direktori `/etc/yum.repos.d`. Repository yang terdapat di CentOS ada berbagai macam diantaranya :

Base merupakan repository yang mengandung paket RPM yang didapatkan dari paket ISO versi CentOS yang anda install. Code :

```
[base]
name=CentOS-$releasever - Base
mirrorlist=http://mirrorlist.centos.org/?release=$releasever&arch=$basearch&repo=os
gpgcheck=1
gpgkey=file:///etc/pki/rpm-gpg/RPM-GPG-KEY-CentOS-5
```

Updates repository yang menyediakan seluruh paket update security, bugs yang sudah di perbaiki dan update dari repository base.

```
[updates]
name=CentOS-$releasever - Updates
mirrorlist=http://mirrorlist.centos.org/?release=$releasever&arch=$basearch&repo=updates
gpgcheck=1
gpgkey=file:///etc/pki/rpm-gpg/RPM-GPG-KEY-CentOS-5
```

Addons repository yang berisi beberapa paket yang sudah di release, khususnya yang terdahulu serta beberapa paket dependency yang diperlukan sebagai tambahan dalam proses instalasi.

```
[addons]
name=CentOS-$releasever - Addons
mirrorlist=http://mirrorlist.centos.org/?release=$releasever&arch=$basearch&repo=addons
gpgcheck=1
gpgkey=file:///etc/pki/rpm-gpg/RPM-GPG-KEY-CentOS-5
```

Extras repository tambahan yang distribusinya langsung dari para pengembang CentOS, paket ini juga baik untuk digunakan sebab sudah mengalami pengujian sebelumnya.

```
[extras]
name=CentOS-$releasever - Extras
mirrorlist=http://mirrorlist.centos.org/?release=$releasever&arch=$basearch&repo=extras
gpgcheck=1
gpgkey=file:///etc/pki/rpm-gpg/RPM-GPG-KEY-CentOS-5
```

Centosplus repository ini hampir sama dengan contrib yaitu repository yang didapatkan dari komunitas CentOS, hanya saja yang membedakannya adalah repository ini memiliki beberapa paket update yang terbaru sehingga sangat baik jika digunakan untuk memperbarui (update) paket yang sudah lama terinstal

```
[centosplus]
name=CentOS-$releasever - Plus
mirrorlist=http://mirrorlist.centos.org/?release=$releasever&arch=$basearch&repo=centosplus
gpgcheck=1
enabled=0
gpgkey=file:///etc/pki/rpm-gpg/RPM-GPG-KEY-CentOS-5
```

Contrib merupakan kumpulan paket yang disediakan dari kontribusi komunitas CentOS (CentOS Project). Perangkat lunak yang terdapat di repository ini tidak akan mengakibatkan konflik dengan paket dasar CentOS, repository contrib ini aman sebab sudah di uji sebelumnya oleh komunitas.

```
[contrib]
name=CentOS-$releasever - Contrib
mirrorlist=http://mirrorlist.centos.org/?release=$releasever&arch=$basearch&repo=contrib
gpgcheck=1
enabled=0
gpgkey=file:///etc/pki/rpm-gpg/RPM-GPG-KEY-CentOS-5
```

Update Sistem

Cara untuk membuat sistem agar berjalan lebih baik adalah dengan update sistem tersebut, adapun langkahnya dengan mengetikkan perintah berikut ini

```
[root@srv1 yum.repos.d]# yum update
Loaded plugins: fastestmirror
Loading mirror speeds from cached hostfile
 * base: centos.biz.net.id
 * extras: mirror.nus.edu.sg
 * updates: mirror.nus.edu.sg
Setting up Update Process
Resolving Dependencies
--> Running transaction check
---> Package NetworkManager.i386 1:0.7.0-13.el5 set to be updated
---> Package NetworkManager-glib.i386 1:0.7.0-13.el5 set to be updated
---> Package SysVinit.i386 0:2.86-17.el5 set to be updated
---> Package acl.i386 0:2.2.39-8.el5 set to be updated
Transaction Summary
```

=====

```
Install      5 Package(s)
Upgrade     217 Package(s)
```

```
Total download size: 228 M
Is this ok [y/N]:
```

Proses update juga bisa digunakan untuk update beberapa paket saja, misalnya anda ingin update paket php pada sistem anda, maka anda tinggal jalankan perintah berikut ini

```
[root@srv1 yum.repos.d]# yum update php
```

Install Paket

Instalasi dengan menggunakan yum sangatlah mudah, yang anda perlukan hanya mengetahui nama paket yang diperlukan untuk instalasi. Misalnya instalasi paket mysql maka anda bisa menjalankan perintah dibawah ini

```
[root@srv1 yum.repos.d]# yum install mysql-server
Loaded plugins: fastestmirror
Loading mirror speeds from cached hostfile
 * base: centos.biz.net.id
 * extras: mirror.nus.edu.sg
 * updates: mirror.nus.edu.sg
Setting up Install Process
Resolving Dependencies
--> Running transaction check
---> Package mysql-server.i386 0:5.0.95-1.el5_7.1 set to be updated
--> Processing Dependency: mysql = 5.0.95-1.el5_7.1 for package: mysql-server
--> Processing Dependency: perl-DBD-MySQL for package: mysql-server
--> Running transaction check
```

```
=====
Package          Arch  Version              Repository           Size
=====
Installing:
mysql-server     i386  5.0.95-1.el5_7.1    updates              9.8 M
Installing for dependencies:
perl-DBD-MySQL  i386  3.0007-2.el5        base                  148 k
Updating for dependencies:
mysql           i386  5.0.95-1.el5_7.1    updates              4.9 M
```

Transaction Summary

```
=====
Install      2 Package(s)
Upgrade     1 Package(s)
```

```
Total download size: 15 M
Is this ok [y/N]:
```

Sebelum anda menekan pilihan (Y) untuk melanjutkan instalasi maka coba periksa terlebih dahulu perintah yang sudah anda berikan, disitu terlihat secara otomatis yum mencari beberapa fungsi dependency yang digunakan untuk melengkapi paket mysql-server seperti mysql dan perl-dbd-mysql

Remove Paket

Yum, selain digunakan untuk instalasi paket yang dibutuhkan untuk keperluan sebuah server, juga bisa digunakan untuk menghapus paket yang sudah terinstall. Untuk menghapus paket yang sudah terinstall pada sistem anda bisa menggunakan perintah yum remove <nama_paket> misalnya anda akan menghapus paket mysql-server maka anda bisa menjalankan perintah dibawah ini

```
[root@srv1 yum.repos.d]# yum remove mysql-server
```

Mencari Paket

Paket yang digunakan untuk instalasi di CentOS sangat banyak sehingga mungkin akan menyulitkan dalam menghafal beberapa paket tersebut. Dengan perintah yum list anda bisa mencari paket yang dibutuhkan sebelum instalasi, berikut contoh dalam mencari paket mc

```
[root@srv1 ~]# yum list mc
Loaded plugins: fastestmirror
Loading mirror speeds from cached hostfile
 * base: centos.biz.net.id
 * extras: mirror.nus.edu.sg
 * updates: mirror.nus.edu.sg
Available Packages
mc.i386                1:4.6.1a-35.el5          base
[root@srv1 ~]#
```

2.5 Repository Pihak ketiga

Paket ketiga merupakan paket yang dibutuhkan dalam melengkapi implementasi server CentOS yang tidak terdapat dalam standart repository. Beberapa komunitas yang mendukung RPM rata-rata membuat sebuah repository yang bisa dipergunakan secara gratis untuk pengguna RPM Linux, sehingga dengan begitu CentOS bisa mengambil manfaat yang disediakan komunitas tersebut. Anda bisa melakukan pengecekan beberapa repository apa saja yang bisa digunakan pada centos pada situs dibawah ini

[1] <http://wiki.centos.org/AdditionalResources/Repositories>

Menambahkan RPMforge direpository CentOS

Sebelum menambahkan RPMforge direpository terlebih dahulu anda perlu mendownload paket yang dibutuhkan

```
[root@serv1 ~]# wget http://dag.wieers.com/rpm/packages/RPM-GPG-KEY.dag.txt
[root@serv1 ~]# rpm --import RPM-GPG-KEY.dag.txt
[root@serv1 ~]# rm -f RPM-GPG-KEY.dag.txt
```

Buatlah sebuah file dan letakkan pada lokasi default repository

```
[root@serv1 ~]# vim /etc/yum.repos.d/rpmforge.repo
```

Selanjutnya tambahkan source code repository seperti dengan code di bawah ini

```
[dag]
name=Dag RPM Repository for Red Hat Enterprise Linux
baseurl=http://apt.sw.be/redhat/el5/en/$basearch/dag/
gpgcheck=1
enabled=0
```

Sedangkan untuk instalasi paket menggunakan repository tersebut, anda bisa menggunakan perintah dibawah ini

```
[root@serv1 ~]# yum --enablerepo=rpmforge install [nama paket]
```

Menambahkan EPEL direpository CentOS

Langkah-langkah untuk menambahkan repository EPEL tidak berbeda dengan RPMforge, hanya saja mungkin perbedaan terletak pada lokasi file yang didownload

```
[root@serv1~]# wget http://ftp.riken.jp/Linux/fedora/epel/RPM-GPG-KEY-EPEL-5
[root@serv1~]# rpm --import RPM-GPG-KEY-EPEL-5
[root@serv1~]# rm -f RPM-GPG-KEY-EPEL-5
```

Tambahkan file untuk deklarasi repository seperti di bawah ini

```
[root@serv1 ~]# vim /etc/yum.repos.d/epel.repo
[epel]
name=EPEL RPM Repository for Red Hat Enterprise Linux
baseurl=http://ftp.riken.jp/Linux/fedora/epel/5/$basearch/
gpgcheck=1
enabled=0
```

Sedangkan untuk instalasi paket menggunakan repository tersebut, anda bisa menggunakan perintah dibawah ini

```
[root@serv1 ~]# yum --enablerepo=epel install [nama paket]
```

Jika anda ingin memasukkan repository yang berbeda anda bisa menggunakan langkah-langkah seperti diatas, sebab cara yang digunakan sama dan mungkin yang berbeda adalah isi dari repository tersebut.

2.6 Konfigurasi IP Address

IP Address merupakan jalan yang digunakan untuk melakukan koneksi dengan PC pada sebuah infrastruktur jaringan, sehingga IP Address sangat penting untuk diperhatikan. Sebab dengan IP Address sebuah PC bisa terhubung dengan jaringan yang lebih luas seperti internet. Dalam konfigurasi IP Address di CentOS memiliki beberapa cara yaitu dalam mode GUI dan mode text, tapi kali ini penulis akan menjelaskan bagaimana konfigurasi dalam mode text.

IP Address Automatic

Konfigurasi ini biasanya digunakan ketika komputer server terhubung dengan sebuah perangkat yang memiliki DHCP Server seperti pada router dan modem. Anda bisa menambahkan fitur *automatic* pada server anda agar mendapatkan IP Address secara otomatis yaitu dengan konfigurasi seperti dibawah ini :

```
[root@serv1 ~]# vim /etc/sysconfig/network-scripts/ifcfg-eth0
DEVICE=eth0
HWADDR=08:00:27:74:FB:84
NM_CONTROLLED=yes
ONBOOT=yes
BOOTPROTO=dhcp
TYPE=Ethernet
IPV6INIT=no
```

```
USERCTL=no
```

IP Address Static

Pada konfigurasi IP Address Static tidak jauh berbeda dengan konfigurasi sebelumnya hanya saja yang membedakannya yaitu menggunakan IP Address yang sudah ditentukan

```
[root@serv1 ~]# vim /etc/sysconfig/network-scripts/ifcfg-eth0
DEVICE=eth0
HWADDR=08:00:27:5f:57:2a
NM_CONTROLLED=yes
ONBOOT=yes
IPADDR=129.93.88.11
BOOTPROTO=none
NETMASK=255.255.255.192
TYPE=Ethernet
IPV6INIT=no
USERCTL=no
```

IP Address Alias

IP Address mode alias digunakan jika memerlukan penambahan IP Address pada network yang berbeda, sehingga dengan menggunakan metode ini tidak hanya memudahkan untuk terkoneksi dengan network yang berbeda, juga tidak merubah konfigurasi IP Address network sebelumnya

```
[root@serv1 ~]# cd /etc/sysconfig/network-scripts/
[root@serv1 network-scripts]# cp ifcfg-eth0 ifcfg-eth0:0
[root@serv1 network-scripts]# vim ifcfg-eth0:0
```

```
DEVICE=eth0:0
HWADDR=08:00:27:5f:57:2a
NM_CONTROLLED=yes
ONBOOT=yes
IPADDR=129.93.88.12
BOOTPROTO=none
NETMASK=255.255.255.192
TYPE=Ethernet
IPV6INIT=no
USERCTL=no
```

Setelah anda selesai konfigurasi pada network dengan beberapa tutorial diatas maka langkah selanjutnya adalah restart network, agar sistem menerapkan beberapa konfigurasi yang sudah anda rubah

```
# service network restart
# chkconfig network on
```

IP Address Bridge

CentOS bisa digunakan menjadi bridge, sehingga bisa difungsikan seperti sebuah switch. Paket yang diperlukan untuk membuat bridge yaitu bridge-utils yang sudah tersedia di repository, sehingga proses instalasi bisa menggunakan yum install seperti pada perintah berikut ini

```
[root@serv1 ~]# yum install bridge-utils
Loaded plugins: fastestmirror
Loading mirror speeds from cached hostfile
 * base: mirror.vietoss.com
 * extras: mirror.vietoss.com
 * updates: mirror.overthewire.com.au
Setting up Install Process
Package bridge-utils-1.2-9.el6.i686 already installed and latest version
Nothing to do
```

Setelah menjalankan perintah diatas anda mendapatkan pesan “*already installed and latest version*” maka hal tersebut menjelaskan bahwa secara default CentOS sudah menyertakan paket tersebut disistem. Langkah selanjutnya adalah anda cukup membuat sebuah file untuk menambahkan interface baru

```
[root@serv1 ~]# cd /etc/sysconfig/network-scripts/
[root@serv1 network-scripts]# cp ifcfg-eth1 ifcfg-br0
DEVICE=br0
HWADDR=08:00:27:3c:93:ba
NM_CONTROLLED=yes
ONBOOT=yes
IPADDR=129.93.88.13
BOOTPROTO=none
NETMASK=255.255.255.192
TYPE=Bridge
```

2.7 Memahami File Permissions

Permission merupakan sebuah metode untuk mengamankan sebuah file, dengan permission setiap file bisa diberikan sebuah hak akses. Sehingga administrator bisa mengatur file tersebut sesuai dengan kebijakan yang ditetapkan administrator. File dan direktori bisa diatur sedemikian rupa hingga lebih spesifik sehingga mempermudah para Network Administrator dalam mengelola file / direktori.

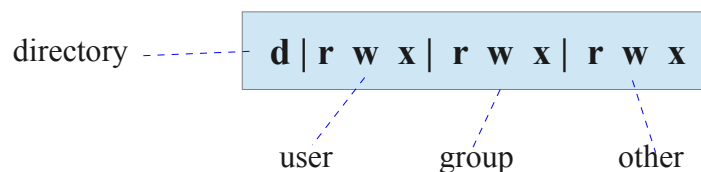
Menggunakan bilangan bit

Dalam sebuah permission file dalam bilangan bit sendiri memiliki 3 kelompok yaitu User, Group dan Other setiap kelompok tersebut memiliki 3 digit binari yaitu Read, Write dan Execute atau di kelompokkan dengan (r w x)

Contoh Studi Kasus :

Sebuah file dengan nama CentOS.txt memiliki permission User (membaca, menulis dan eksekusi), Group (membaca dan menulis) dan Other (membaca). Tentukan nilai permission pada file tersebut.

Sebuah File/direktori pada hakekatnya memiliki sebuah permission, sehingga keamanan file lebih terjamin sebab siapa saja yang berhak mengakses dan merubah bisa diatur.



Keterangan :

r = read

w = write
x = execute

Dari studi kasus tersebut didapatkan perhitungan seperti pada berikut ini

$$2^2 + 2^1 + 2^0 = 4 + 2 + 1$$

Jika yang diinginkan adalah User (membaca, menulis dan eksekusi), Group (membaca dan menulis) dan Other (membaca) maka :

User	= r + w + x	= $2^2 + 2^1 + 2^0$	= 4 + 2 + 1	= 7
Group	= r + w	= $2^2 + 2^1 + -$	= 4 + 2	= 6
Other	= r	= $2^2 + - + -$	= 4	= 4

Sehingga angka yang didapatkan untuk menentukan permission dalam studi kasus tersebut adalah 764, untuk membuat permission silahkan mengikuti perintah dibawah ini :

Buat file terlebih dahulu

```
# touch CentOS.txt
```

Setting angka permission yang ditetapkan

```
# chmod 0764 CentOS.tx
```

1. menggunakan simbol

Metode permission menggunakan simbol lebih murah dari pada menggunakan binari, pada metode ini hanya menerapkan 2 konsep yaitu :

+ = Memberikan permission

- = Menghapus permission

Pertanyaanya bagaimana jika kasusnya seperti diatas? Mudah saja sebab cukup membuat sebuah permission seperti pada contoh dibawah ini :

```
# chmod u+rwx CentOS.txt
```

```
# chmod g+rw CentOS.txt
```

```
# chmod o+r CentOS.txt
```

Keterangan : r = read, w = write, x = execute.

SSH Server

Kebutuhan untuk mengendalikan server dari jarak jauh adalah hal yang terpenting dari seorang Administrator, dengan kemampuan remote dari jarak jauh seorang Administrator mempermudah beberapa pekerjaan yang bersangkutan dengan server, sebab tidak harus berada di lokasi dimana server berada, terutama kerusakan dalam segi software maka pengendalian hak akses jarak jauh sangat dibutuhkan. SSH merupakan service yang paling banyak digunakan untuk kebutuhan remote sebuah server. SSH merupakan alternative pengganti dari telnet, telnet adalah software yang digunakan untuk aktifitas remote server, tapi telnet sendiri memiliki beberapa kekurangan diantaranya dari segi keamanan yang dengan mudahnya diambil alih dari pihak lain, sebab telnet dalam pengiriman berupa data tidak disertakan encripsi, sehingga keamanan data kurang terjamin.

Walaupun SSH memiliki keamanan yang bisa diandalkan, tetapi SSH juga perlu ditingkatkan dalam segi keamanan sehingga tidak mudah untuk diambil alih oleh orang yang tidak di ijin, berikut ini adalah beberapa tahap yang perlu dilakukan dalam mengamankan SSH Server.

3.1. Menggunakan protokol 2 pada SSH

Protokol 2 adalah protokol baru yang dimiliki SSH dengan beberapa keamanan yang sudah di uji dan lebih baik dari protokol 1

```
[root@serv1 ~]# nano /etc/ssh/sshd_config
Protocol 2
```

3.2. Mengganti Port Default

Secara default SSH menggunakan port 22, sehingga secara tidak langsung akan memudahkan pada attacker dalam mengambil alih SSH jika port tersebut tidak diganti. Agar lebih aman maka ganti port tersebut sesuai dengan keinginan anda

```
[root@serv1 ~]# nano /etc/ssh/sshd_config
# Port 22 ganti standart port pada SSH Server dengan 1290
Port 1290
```

3.3. Membatasi Akses SSH pada User

Sebuah server bisa diakses dengan mudah melalui service SSH, hal tersebut memberikan kesempatan beberapa user untuk mengaksesnya secara penuh sehingga perlu adanya batasan akses sehingga tidak semua user memiliki hak akses secara penuh. Misalnya administrator menambahkan nama user yaitu user1 dan user2, setelah mendaftarkan user kedalam sistem selanjutnya memberikan batasan hak akses.

```
[root@serv1 ~]# useradd user1
[root@serv1 ~]# useradd user2
[root@serv1 ~]# passwd user1
Changing password for user user1.
New password:
Retype new password:
passwd: all authentication tokens updated successfully.
[root@serv1 ~]# passwd user2
Changing password for user user2.
New password:
Retype new password:
passwd: all authentication tokens updated successfully.
```

Setelah anda menambahkan user pada server langkah selanjutnya adalah menambahkan konfigurasi pada file /etc/ssh/sshd_config yaitu mendaftarkan user2 untuk diijinkan akses ke server, secara default script tersebut tidak terdapat di file sshd_config, sehingga anda harus menambahkannya sendiri di paling bawah script

```
[root@serv1 ~]# nano /etc/ssh/sshd_config
AllowUsers user2
```

Sekarang kita lakukan uji coba apakah script tersebut sudah berjalan dengan baik yaitu dengan restart terlebih dahulu service sshd dengan perintah dibawah ini

```
[root@serv1 ~]# service sshd restart
Stopping sshd: [ OK ]
Starting sshd: [ OK ]
[root@serv1 ~]#
```

Uji coba pertama dengan user yang tidak didefinisikan pada sshd_config, Port yang digunakan tidak 22 melainkan 1290 sehingga cara login pada ssh berbeda dengan sebelumnya, melainkan disertai port yang sudah didaftarkan, yaitu

```
mafatahna@mafatahna:~$ ssh user1@129.93.88.11 -p 1290
maya@129.93.88.11's password:
Permission denied, please try again.
maya@129.93.88.11's password:
```

Gagal! Berarti script yang anda masukkan tadi sudah berjalan dengan sukses, selanjutnya login dengan user yang sudah didaftarkan pada sshd_config

```
mafatahna@mafatahna:~$ ssh user2@129.93.88.11 -p 1290
mafatahna@129.93.88.11's password:
[mafatahna@serv1 ~]$
```

Login berhasil !!

Silahkan anda menambahkan user yang anda inginkan dan jangan lupa untuk limit user yang di ijinan untuk akses ke server.

3.4. Konfigurasi idle timeout

Ketika seorang user sedang login dan tidak ada aktifitas apapun (*idle*) maka kita bisa memberikan batasan dalam bentuk timer pada user tersebut, misalnya jika user tidak melakukan aktifitas selama 1 menit maka secara otomatis sistem akan menutup koneksi SSH user tersebut

```
[root@serv1 ~]# nano /etc/ssh/sshd_config
#ClientAliveInterval 0
#ClientAliveCountMax 3
```

Hilangkan tanda pagar (#) pada script tersebut, angka yang digunakan menggunakan satuan detik sehingga jika anda menginginkan timeout 1 menit berarti $1 \times 60 = 60s$. Edit script tersebut seperti dengan dibawah ini

```
ClientAliveInterval 60
```

```
ClientAliveCountMax 0
```

Selanjutnya restart service SSH anda dan lakukan uji coba dengan login pada SSH dan membiarkan user tersebut tanpa aktifitas selama lebih dari 1 menit

```
mafatahna@mafatahna:~$ ssh mafatahna@129.93.88.11 -p 1290
mafatahna@129.93.88.11's password:
Last login: Tue May  1 09:31:29 2012 from 192.168.10.1
[mafatahna@serv1 ~]$ Connection to 129.93.88.11 closed by remote host.
Connection to 129.93.88.11 closed.
```

Setelah lebih dari 1 menit maka server secara otomatis akan menutup koneksi service SSH server, sehingga anda diharuskan login lagi jika ingin mengakses SSH.

3.5. Disable login root via SSH

Hak akses root jika dibiarkan terbuka akan sangat berbahaya sebab hal tersebut akan dimanfaatkan para attacker untuk melakukan brute force untuk mendapatkan hak akses root, sehingga untuk mengatasinya anda bisa menutup akses yang menggunakan user root, untuk menutup user root agar tidak bisa login via ssh anda hanya merubah konfigurasi *Permitrootlogin* menjadi *no* seperti pada konfigurasi dibawah ini

```
[root@serv1 ~]# nano /etc/ssh/sshd_config
#PermitRootLogin yes
```

Hilangkan tanda pagar (#) ganti parameter *yes* menjadi *no* seperti pada perintah dibawah ini

```
[root@serv1 ~]# nano /etc/ssh/sshd_config
#PermitRootLogin yes
PermitRootLogin no
```

Langkah selanjutnya adalah menguji apakah perintah yang sudah ditambahkan pada server SSH bisa berjalan dengan baik, login menggunakan user root

```
mafatahna@mafatahna:~$ ssh root@129.93.88.11 -p 1290
root@129.93.88.11's password:
Permission denied, please try again.
root@129.93.88.11's password:
```

Login gagal! Berarti konfigurasi yang anda lakukan sudah berhasil, selanjutnya login menggunakan user yang di ijinkan mengaksesnya SSH Server.

```
mafatahna@mafatahna:~$ ssh mafatahna@129.93.88.11 -p 1290
mafatahna@129.93.88.11's password:
Last login: Tue May  1 09:56:11 2012 from 192.168.10.1
[mafatahna@serv1 ~]$ su
Password:
[root@serv1 mafatahna]#
```

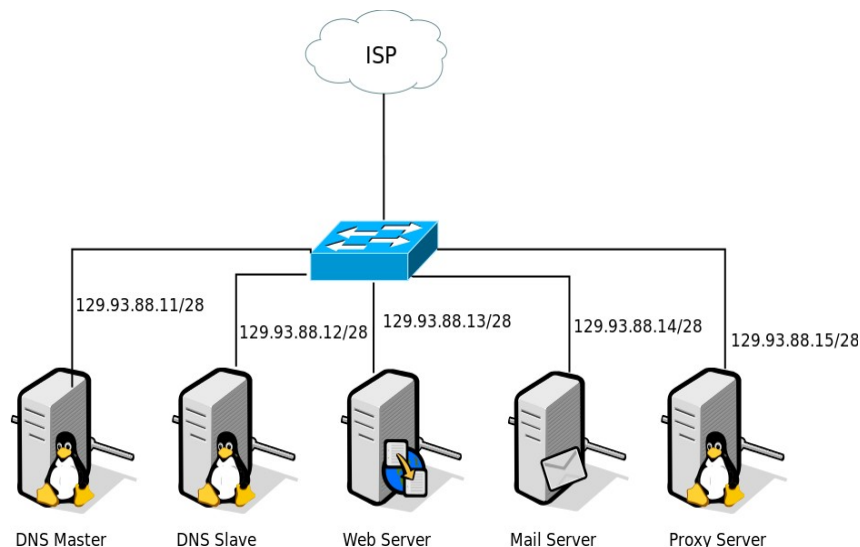
DNS Server

Aktifitas menjelajahi dunia maya merupakan kegiatan yang sering kita lakukan, dengan semakin banyaknya beberapa situs yang mungkin bisa dikatakan situs wajib yang harus dikunjungi misalnya jejaring sosial, sehingga mampu meningkatkan pengguna internet, pada dasarnya untuk beroperasi pada jaringan internet sebuah komputer sebenarnya merupakan pengelamatan sebuah komputer yang dilakukan menggunakan angka yang lebih dikenal dengan Internet Protocol Address (IP Address) yang berjumlah 32 bit dan diterjemahkan dalam bentuk bilangan desimal.

Tentunya akan sukar untuk menghafalkan ribuan bilangan desimal yang ada didunia ini mengingat banyak sekali situs berbeda yang dibuka pada setiap harinya. Untuk itu dikembangkan sebuah sistem untuk menerjemahkan IP Address tersebut menjadi sebuah nama domain yang saat ini dikenal dengan istilah Domain Name System (DNS). Bagi seorang network administrator pengetahuan seputar DNS ini sangatlah penting sebab merupakan dasar utama sebelum membuat sebuah server DNS disusul dengan Web server yang dibutuhkan oleh Perusahaan atau lingkup Universitas untuk membuat sebuah Web Server sendiri.

4.1 Installasi DNS Server

Pada sistem operasi Linux CentOS DNS Server di implementasikan dengan menggunakan software Berkeley Internet Name Domain (BIND), secara default implementasi DNS terdiri atas DNS Master dan DNS Slave (backup) sebagai cadangan jika DNS utama terjadi masalah sehingga secara otomatis akan diarahkan ke DNS Slave. Pada implementasi kali ini akan menggunakan domain <http://centos.co.id> dengan IP Address (Public) 129.93.88.11, sedangkan untuk IP Address (Local) menggunakan 192.168.10.11. Lebih jelasnya bisa dilihat pada topologi berikut ini



Paket yang digunakan untuk membuat DNS Server sudah tersedia di CentOS, sehingga anda hanya perlu mengetikkan perintah dengan yum install untuk memulai membangun sebuah DNS Server. Langkah awal yang perlu dilakukan sebelum installasi DNS Server adalah disabled service Selinux yang terdapat pada /etc/sysconfig/selinux. Langkah-langkah sebagai berikut

```
[root@srv1 ~]# vim /etc/sysconfig/selinux
```

Setelah anda berhasil masuk pada editor vim maka langkah selanjutnya ganti status SELINUX menjadi disabled, sedangkan SELINUXTYPE ganti dengan targeted

```
# This file controls the state of SELinux on the system.
# SELINUX= can take one of these three values:
#     enforcing - SELinux security policy is enforced.
#     permissive - SELinux prints warnings instead of enforcing.
#     disabled - SELinux is fully disabled.
SELINUX=disabled
# SELINUXTYPE= type of policy in use. Possible values are:
#     targeted - Only targeted network daemons are protected.
#     strict - Full SELinux protection.
SELINUXTYPE=targeted
```

Jika anda sudah merubah konfigurasi tersebut langkah selanjutnya menyimpan dan keluar dari editor dengan menekan tombol Esc dan ketik :wq, perintah tersebut digunakan untuk keluar dengan menyimpan file. Setelah SELINUX berhasil anda disabled maka berikutnya anda bisa memulai instalasi paket bind, tetapi pastikan saat ini anda sudah terkoneksi dengan internet. Jalankan perintah dibawah ini untuk memulai proses instalasi

```
[root@srv1 ~]# yum install bind bind-utils bind-*
```

Perintah instalasi bind diatas akan sekaligus menyertakan beberapa paket bind, bind-utils, bind-sdb, bind-chroot, bind-devel, bind-libs, bind-utils dan libbind-devel. Setelah proses instalasi selesai dan berjalan dengan sempurna langkah selanjutnya adalah melakukan konfigurasi dasar pada script bind. Dalam melakukan konfigurasi bind ada beberapa perbedaan lokasi file antara CentOS 5 dan CentOS 6, perbedaan tersebut diantaranya adalah

CentOS 5, lokasi file named.conf tidak terdapat pada versi ini tetapi kita bisa membuat filenya dan diletakkan pada /var/named/chroot/etc/ sedangkan untuk lokasi data domain dan reverse DNS terletak pada /var/named/chroot/var/named.

CentOS 6, lokasi file named.conf terletak pada /etc/named.conf, file tersebut secara otomatis sudah tersedia sehingga lebih memudahkan pengguna. Sedangkan lokasi domain dan reverse DNS terletak pada /var/named

Secara umum langkah-langkah dalam konfigurasi DNS memiliki kesamaan hanya saja kemungkinan yang terjadi mengakibatkan pengguna kebingungan hanyalah lokasi file tersebut. Pada penerapan DNS Server ini penulis menggunakan CentOS 5 sesuai dengan DVD yang sudah dilampirkan dalam buku ini. Sehingga jika anda menggunakan CentOS 6 anda bisa menggunakan langkah-langkah ini dengan catatan lokasi file sesuai dengan penjelasan diatas.

CentOS 5 secara default sama sekali tidak menyertakan file konfigurasi pada direktori chroot, tetapi anda tidak perlu khawatir, sebab file konfigurasi tersebut bisa anda dapatkan dengan mudah di file dokumentasi yang terdapat pada sistem anda. Ada beberapa file yang sudah di siapkan pada direktori sample, yaitu pada /usr/share/doc/bind-9.3.6/sample. Didalam file tersebut terdapat semua file konfigurasi yang dibutuhkan dalam proses instalasi DNS Server.

4.2 Konfigurasi DNS Server

Setelah anda mempelajari lokasi file yang dibutuhkan untuk implementasi DNS Server, maka langkah yang dilakukan selanjutnya adalah memulai konfigurasi yaitu dengan membuat sebuah file named.conf pada direktori /var/named/chroot/etc. Lebih jelasnya silahkan lihat pada konfigurasi dibawah ini
Masuk terlebih dahulu pada direktori sample DNS Server

```
[root@srv1 ~]# cd /usr/share/doc/bind-9.3.6/sample/
[root@srv1 sample]#
```

Selanjutnya copy semua file yang terdapat pada direktori etc dan var ke dalam direktori chroot

```
[root@srv1 sample]# cp * etc/* /var/named/chroot/etc/
[root@srv1 sample]# cp * var/named/* /var/named/chroot/var/named/
```

Ketika anda menjalankan perintah tersebut akan di berikan informasi ada beberapa file yang sudah ada, maka lanjutkan saja dengan mengetikkan persetujuan (*y*). Langkah selanjutnya agar memudahkan dalam konfigurasi silahkan masuk pada direktori chroot, seperti pada contoh dibawah ini

```
[root@srv1 sample]# cd /var/named/chroot/
[root@srv1 chroot]#
```

CentOS 5 tidak menyertakan file named.conf sehingga anda harus membuatnya terlebih dahulu dengan perintah vim, seperti pada contoh berikut ini

```
[root@srv1 chroot]# vim etc/named.conf
```

Selanjutnya tuliskan beberapa parameter dan script seperti dengan contoh dibawah ini

```
[root@srv1 chroot]# vim etc/named.conf
options {
    listen-on-v6 {none;};
    directory "/var/named";
    allow-query { localhost; 192.168.10.0/24; };
    allow-transfer { localhost; 192.168.10.0/24;};
    recursion yes;
};
controls {
    inet 127.0.0.1 allow { localhost; } keys { rndckey; };
};
view "internal" {
    match-clients {
        localhost;
    };
zone "." IN {
    type hint;
    file "named.ca";
};
zone "centos.co.id" IN {
    type master;
    file "centos.co.id.lan";
    allow-update { none; };
};
```

```

zone "10.168.192.in-addr.arpa" IN {
    type master;
    file "10.168.192.db";
    allow-update { none; };
};
zone "localdomain" IN {
    type master;
    file "localdomain.zone";
    allow-update { none; };
};
zone "localhost" IN {
    type master;
    file "localhost.zone";
    allow-update { none; };
};
zone "0.0.127.in-addr.arpa" IN {
    type master;
    file "named.local";
    allow-update { none; };
zone "255.in-addr.arpa" IN {
    type master;
    file "named.broadcast";
    allow-update { none; };
};
zone "0.in-addr.arpa" IN {
    type master;
    file "named.zero";
    allow-update { none; };
};
};
view "external" {
    match-clients { any; };
    allow-query { any; };
    recursion yes;
    zone "centos.co.id" IN {
        type master;
        file "centos.co.id.wan";
        allow-update { none; };
    };
    zone "88.93.129.in-addr.arpa" IN {
        type master;
        file "88.93.129.db";
        allow-update { none; };
    };
};
include "/etc/rndc.key";

```

Simpan konfigurasi tersebut dengan Esc dan ketik perintah :wq. Dalam penulisan script ingat dan perhatikan pada karakter kurung kurawal {} dan titik koma ; sebab beberapa perintah tersebut menjadi salah satu penyebab konfigurasi DNS Server gagal. Selain named.conf, DNS Server pada CentOS 5 juga tidak menyertakan named.ca sehingga pengguna harus membuat sendiri file tersebut. Seperti pada perintah di bawah ini

```

[root@srv1 chroot]# vim etc/named.ca
; <<>> DiG 9.5.0b2 <<>> +bufsize=1200 +norec NS . @a.root-servers.net
;; global options: printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 34420
;; flags: qr aa; QUERY: 1, ANSWER: 13, AUTHORITY: 0, ADDITIONAL: 20

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;.                               IN           NS

;; ANSWER SECTION:
.                               518400     IN         NS         M.ROOT-SERVERS.NET.
.                               518400     IN         NS         A.ROOT-SERVERS.NET.
.                               518400     IN         NS         B.ROOT-SERVERS.NET.
.                               518400     IN         NS         C.ROOT-SERVERS.NET.
.                               518400     IN         NS         D.ROOT-SERVERS.NET.
.                               518400     IN         NS         E.ROOT-SERVERS.NET.
.                               518400     IN         NS         F.ROOT-SERVERS.NET.
.                               518400     IN         NS         G.ROOT-SERVERS.NET.
.                               518400     IN         NS         H.ROOT-SERVERS.NET.
.                               518400     IN         NS         I.ROOT-SERVERS.NET.
.                               518400     IN         NS         J.ROOT-SERVERS.NET.
.                               518400     IN         NS         K.ROOT-SERVERS.NET.
.                               518400     IN         NS         L.ROOT-SERVERS.NET.

;; ADDITIONAL SECTION:
A.ROOT-SERVERS.NET.           3600000   IN         A          198.41.0.4
A.ROOT-SERVERS.NET.           3600000   IN         AAAA       2001:503:ba3e::2:30
B.ROOT-SERVERS.NET.           3600000   IN         A          192.228.79.201
C.ROOT-SERVERS.NET.           3600000   IN         A          192.33.4.12
D.ROOT-SERVERS.NET.           3600000   IN         A          128.8.10.90
E.ROOT-SERVERS.NET.           3600000   IN         A          192.203.230.10
F.ROOT-SERVERS.NET.           3600000   IN         A          192.5.5.241
F.ROOT-SERVERS.NET.           3600000   IN         AAAA       2001:500:2f::f
G.ROOT-SERVERS.NET.           3600000   IN         A          192.112.36.4
H.ROOT-SERVERS.NET.           3600000   IN         A          128.63.2.53
H.ROOT-SERVERS.NET.           3600000   IN         AAAA       2001:500:1::803f:235
I.ROOT-SERVERS.NET.           3600000   IN         A          192.36.148.17
J.ROOT-SERVERS.NET.           3600000   IN         A          192.58.128.30
J.ROOT-SERVERS.NET.           3600000   IN         AAAA       2001:503:c27::2:30
K.ROOT-SERVERS.NET.           3600000   IN         A          193.0.14.129
K.ROOT-SERVERS.NET.           3600000   IN         AAAA       2001:7fd::1
L.ROOT-SERVERS.NET.           3600000   IN         A          199.7.83.42

```

Simpan konfigurasi tersebut, script yang dibutuhkan untuk konfigurasi DNS Server memang lumayan banyak, tetapi anda tidak perlu khawatir sebab seluruh konfigurasi yang terdapat pada buku ini penulis telah sertakan semua dalam DVD terlampir pada buku ini.

Setelah file utama selesai dibuat yaitu named.conf maka langkah-langkah selanjutnya adalah membuat file sebagai dasar DNS Server sekaligus reverse DNS. Domain yang penulis pergunakan dalam project DNS Server adalah centos.co.id. Didalam file named.conf telah dijelaskan bahwa file centos.co.id

memiliki 2 file yaitu file yang ditujukan ke IP Public (129.93.88.11) dan IP Lokal (192.168.10.11) sehingga pada penerapannya pastikan anda sudah memiliki IP Address tersebut yaitu public dan lokal. Langkah selanjutnya adalah membuat file untuk melengkapi file utama (named.conf)

Jika posisi anda saat ini berada di direktori chroot, maka jalankan perintah dibawah ini

```
[root@srv1 chroot]# vim var/named/centos.co.id.wan
```

Perintah tersebut digunakan untuk membuat sebuah file baru dengan nama centos.co.id.wan. Selanjutnya isi file tersebut dengan script dibawah ini

```
$TTL 86400
@ IN SOA      srv1.centos.co.id. root.centos.co.id. (
    20120522    ;Serial
    3600        ;Refresh
    1800        ;Retry
    604800     ;Expire
    86400      ;Minimum TTL
)
    IN NS      srv1.centos.co.id.
    IN NS      srv2.centos.co.id.
    IN A       129.93.88.11
    IN MX 10   mail.centos.co.id.
srv1 IN A       129.93.88.11
www  IN CNAME  srv1.centos.co.id.
```

Simpan file tersebut, tahapan selanjutnya adalah membuat file untuk centos.co.id.lan. Jika ada pertanyaan, kenapa harus dibedakan antara LAN dan WAN? Deklarasi sebuah domain dengan 2 IP Address akan memudahkan user terutama dalam 1 jaringan lokal tersebut untuk mengakses domain lebih cepat, sehingga ketika user mengakses domain tidak akan menuju ke internet terlebih dahulu melainkan akan menuju ke lokal, sehingga proses caching DNS lebih cepat.

Selanjutnya membuat file centos.co.id.lan dengan perintah dasar vim

```
[root@srv1 chroot]# vim var/named/centos.co.id.lan
```

Setelah berhasil masuk pada menu editor vim, maka tulislah script seperti di bawah ini

```
$TTL 86400
@ IN SOA      srv1.centos.co.id. root.centos.co.id. (
    20120522    ;Serial
    3600        ;Refresh
    1800        ;Retry
    604800     ;Expire
    86400      ;Minimum TTL
)
    IN NS      srv1.centos.co.id.
    IN NS      srv2.centos.co.id.
    IN A       192.168.10.11
    IN MX 10   mail.centos.co.id.
srv1 IN A       192.168.10.11
www  IN CNAME  srv1.centos.co.id.
```

Jangan lupa untuk menyimpan file konfigurasi tersebut. Setelah file centos.co.id untuk pendeklarasian DNS selesai, langkah berikutnya adalah membuat file yang digunakan untuk reverse DNS. Lanjutkan dengan membuat file lagi seperti berikut ini

```
[root@srv1 chroot]# vim var/named/88.93.129.db
```

File yang sudah dibuat tersebut isi dengan beberapa script berikut

```
$TTL 86400
@   IN  SOA    srv1.centos.co.id. root.centos.co.id. (
        20120522  ;Serial
        3600      ;Refresh
        1800      ;Retry
        604800    ;Expire
        86400     ;Minimum TTL
)
      IN  NS   srv1.centos.co.id.
      IN  PTR   centos.co.id.
      IN  A    255.255.255.192
11     IN  PTR   srv1.centos.co.id.
```

Simpan dan keluar dari editor, selanjutnya membuat reverse DNS yang digunakan jaringan lokal

```
[root@srv1 chroot]# vim var/named/10.168.192.db
```

File yang sudah terbuat tersebut isi dengan perintah dibawah ini

```
$TTL 86400
@   IN  SOA    srv1.centos.co.id. root.centos.co.id. (
        20120522  ;Serial
        3600      ;Refresh
        1800      ;Retry
        604800    ;Expire
        86400     ;Minimum TTL
)
      IN  NS   srv1.centos.co.id.
      IN  PTR   centos.co.id.
      IN  A    255.255.255.0
11     IN  PTR   srv1.centos.co.id.
```

Konfigurasi DNS Server sudah selesai, selanjutnya restart service DNS Server anda dengan perintah

```
[root@srv1 chroot]# service named restart
Stopping named: [ OK ]
Starting named: [ OK ]
[root@srv1 chroot]#
```

Pada saat anda restart DNS Server, pastikan tidak terdapat error. Jika anda menemui kendala dalam proses implementasi DNS Server anda bisa melihat error pada Server dengan melihatnya pada log. Adapun langkah-langkahnya anda bisa menjalankan perintah dibawah ini

```
[root@srv1 chroot]# tail -f /var/log/messages
May 24 20:16:04 srv1 named[2638]: zone 10.168.192.in-addr.arpa/IN/internal:
loaded serial 20120522
May 24 20:16:04 srv1 named[2638]: zone 255.in-addr.arpa/IN/internal: loaded
serial 42
May 24 20:16:04 srv1 named[2638]: zone centos.co.id/IN/internal: loaded
serial 20120522
```

4.3 Uji Coba

Uji coba apakah DNS Server sudah berjalan dengan baik, bisa dilakukan dengan komputer server DNS Server atau dengan klien yang memiliki IP Berbeda berikut ini beberapa pengecekannya DNS Server.

```
[root@srv1 chroot]# nslookup centos.co.id
Server:          127.0.0.1
Address:         127.0.0.1#53
```

```
Name: centos.co.id
Address: 192.168.10.11
```

```
[root@srv1 chroot]# nslookup www.centos.co.id
Server:          127.0.0.1
Address:         127.0.0.1#53
```

```
www.centos.co.idcanonical name = srv1.centos.co.id.
Name: srv1.centos.co.id
Address: 192.168.10.11
```

```
[root@srv1 chroot]# nslookup 192.168.10.11
Server:          127.0.0.1
Address:         127.0.0.1#53
```

```
11.10.168.192.in-addr.arpa name = srv1.centos.co.id.
```

```
[root@srv1 chroot]#
```

4.4 konfigurasi DNS Slave

DNS Slave digunakan sebagai backup jika DNS Utama (Master) mengalami masalah atau down. DNS Slave akan mengambil alih fungsi DNS Master, sehingga ketika DNS utama mengalami kerusakan misalnya dalam segi hardware maka sebuah DNS server tidak akan down sebab data-data yang dibutuhkan untuk DNS Server semua sudah tersedia pada DNS Slave. Cara kerja DNS Slave yaitu menggandakan semua konfigurasi yang sudah ada dan disimpan sebagai cadangan, sehingga jika ada perubahan yang terjadi pada DNS Master maka DNS Slave akan menyimpan perubahan konfigurasi tersebut secara otomatis. Dalam pembuatan Server DNS pasti anda sudah mengetahui bahwa didalam konfigurasi tersebut terdapat kode yang disebut serial, seperti pada contoh dibawah ini

```
$TTL 86400
@ IN SOA      srv1.centos.co.id. root.centos.co.id. (
      20120522 ;Serial
      3600     ;Refresh
```

Dalam penulisan serial merupakan perpaduan dari tanggal, bulan dan tahun. Pada kode nomor tersebut bisa dijelaskan 20120522 maksudnya penulis terakhir melakukan perubahan pada konfigurasi DNS

Server pada Tanggal 22 Mei 2012. Serial harus ditulis secara manual, sehingga jika nanti anda melakukan perubahan pada server jangan lupa untuk mengupdate tanggal serial. Hal tersebut digunakan agar proses transfer data pada DNS Master ke DNS Slave bisa terlaksana.

Langkah-langkah yang perlu dilakukan dalam membuat DNS Slave adalah edit konfigurasi named.conf pada DNS Master yaitu pada script pada

```
options {
    listen-on-v6 {none;};
    directory "/var/named";
    allow-query { localhost; 192.168.10.0/24; };
    allow-transfer { localhost; 192.168.10.0/24;};
    recursion yes;
};
```

Ganti default allow-transfer menjadi

```
[root@srv1 chroot]# vim etc/named.conf
options {
    listen-on-v6 {none;};
    directory "/var/named";
    allow-query { localhost; 192.168.10.0/24; };
    allow-transfer { localhost; 129.93.88.12;};
    recursion yes;
};
```

IP Address 129.93.88.12 adalah IP Public yang di miliki DNS Slave. Langkah selanjutnya adalah update serial yang terdapat di file centos.co.id.wan dan menambahkan ns yang digunakan sebagai DNS Slave, lebih jelasnya silahkan lihat pada contoh konfigurasi dibawah ini

```
[root@srv1 chroot]# vim var/named/centos.co.id.wan
$TTL 86400
@    IN    SOA    srv1.centos.co.id. root.centos.co.id. (
        20120524      ;Serial
        3600          ;Refresh
        1800          ;Retry
        604800       ;Expire
        86400        ;Minimum TTL
)
      IN    NS     srv1.centos.co.id.
IN NS     srv2.centos.co.id.
      IN    A      129.93.88.12
      IN    MX 10   mail.centos.co.id.
srv1   IN    A      129.93.88.11
srv2   IN    A      129.93.88.12
mail   IN    CNAME  srv1.centos.co.id.
www    IN    CNAME  srv2.centos.co.id.
```

Simpan hasil konfigurasi anda. Selanjutnya edit file pada reverse domain dengan menambahkan IP DNS Server pada file tersebut seperti pada contoh berikut ini

```

[root@srv1 chroot]# vim var/named/88.93.129.db
$TTL 86400
@   IN  SOA      srv1.centos.co.id. root.centos.co.id. (
        20120524      ;Serial
        3600         ;Refresh
        1800         ;Retry
        604800      ;Expire
        86400        ;Minimum TTL
)
      IN  NS      srv1.centos.co.id.
      IN  PTR     centos.co.id.
      IN  A       255.255.255.192
11     IN  PTR     srv1.centos.co.id.
12     IN  PTR     srv2.centos.co.id.

```

Simpan terlebih dahulu script yang sudah anda ketik, selanjutnya restart bind dan rndc pada DNS Server

```

[root@srv1 chroot]# service named restart
Stopping named: [ OK ]
Starting named: [ OK ]
[root@srv1 chroot]# rndc reload
server reload successful

```

Setelah anda menambahkan NS pada file domain dan reverse DNS maka, langkah selanjutnya adalah menambahkan file named.conf di Server yang digunakan sebagai DNS Slave dengan asumsi paket bind sudah terinstall dengan baik. Agar mempermudah konfigurasi masuk terlebih dahulu pada direktori chroot, selanjutnya edit/buat file named.conf pada direktori etc yang terletak di dalam chroot seperti pada perintah di bawah ini

```

[root@srv2 ~]# cd /var/named/chroot/
[root@srv2 chroot]# vim etc/named.conf
options {
    listen-on-v6 {none;};
    directory "/var/named";
    recursion yes;
};

zone "centos.co.id" IN {
    type slave;
    masters { 129.93.88.11; };
    file "slaves/centos.co.id.wan";
    notify no;
};

zone "88.93.129.in-addr.arpa" IN {
    type slave;
    masters { 129.93.88.11; };
    file "slaves/88.93.129.db";
    notify no;
};

```

Simpan hasil konfigurasi anda dan restart service bind dengan perintah dibawah ini

```
[root@srv2 chroot]# service named restart
Stopping named: [ OK ]
Starting named: [ OK ]
```

Pastikan ketika proses restart berlangsung tidak terdapat error dalam proses tersebut. Selanjutnya jalankan perintah rndc untuk memulai mengaktifkan proses transfer DNS dengan perintah berikut ini

```
[root@srv2 chroot]# service named restart
Stopping named: [ OK ]
Starting named: r [ OK ]
[root@srv2 chroot]# rndc reload
server reload successful
```

Jika proses konfigurasi yang anda lakukan sudah benar, silahkan coba melakukan pengecekan apakah file domain dan reverse DNS yang terletak pada DNS Master sudah tertransfer di DNS Slave.

```
[root@srv2 chroot]# ls var/named/slaves/
88.93.129.db centos.co.id.wan
[root@srv2 chroot]#
```

Jika sudah ada berarti proses pembuatan DNS Slave anda sudah berhasil, berikut ini adalah file hasil dari transfer dari DNS Master ke DNS Slave

```
[root@srv2 chroot]# vim var/named/slaves/centos.co.id.wan
$ORIGIN .
$TTL 86400 ; 1 day
centos.co.id IN SOA srv1.centos.co.id. root.centos.co.id. (
                20120523 ; serial
                3600 ; refresh (1 hour)
                1800 ; retry (30 minutes)
                604800 ; expire (1 week)
                86400 ; minimum (1 day)
                )
                NS srv1.centos.co.id.
                NS srv2.centos.co.id.
                A 129.93.88.12
                MX 10 mail.centos.co.id.
$ORIGIN centos.co.id.
www CNAME srv2
srv1 A 129.93.88.11
srv2 A 129.93.88.12
mail CNAME srv1
```

```
[root@srv2 chroot]# vim var/named/slaves/88.93.129.db
$ORIGIN .
$TTL 86400 ; 1 day
88.93.129.in-addr.arpa IN SOA srv1.centos.co.id. root.centos.co.id. (
                20120522 ; serial
                3600 ; refresh (1 hour)
                1800 ; retry (30 minutes)
                604800 ; expire (1 week)
                86400 ; minimum (1 day)
                )
```

```

NS      srv1.centos.co.id.
A      255.255.255.192
PTR    centos.co.id.
$ORIGIN 88.93.129.in-addr.arpa.
11     PTR      srv1.centos.co.id.
12     PTR      srv2.centos.co.id.

```

Sedangkan untuk uji coba bisa dilakukan dengan mematikan terlebih dahulu Server DNS Master, sehingga DNS Slave benar-benar bisa digunakan sebagai pengganti dari DNS Master

```

[root@srv2 chroot]# nslookup centos.co.id
Server:      129.93.88.12
Address:    129.93.88.12#53

```

```

Name: centos.co.id
Address: 129.93.88.12

```

```

[root@srv2 chroot]#

```

Terlihat pada server mengarah ke IP Address 129.93.88.12. Maka DNS Slave sudah berjalan dengan sempurna.

4.5 Konfigurasi Mutidomain

Multidomain adalah sebuah fitur yang dimiliki DNS Server, fitur ini digunakan untuk konfigurasi menggunakan 2 domain atau lebih. Fitur ini biasanya digunakan perusahaan web hosting untuk menampung domain yang berbeda dalam satu server. Konfigurasi dalam multidomain sangat sederhana, anda hanya menambahkan beberapa rule yang terdapat di file named.conf

```

[root@srv1 ~]# cd /var/named/chroot/
[root@srv1 chroot]# vim etc/named.conf
zone "centos.co.id" IN {
    type master;
    file "centos.co.id.lan";
    allow-update { none; };
};
zone "centos.org" IN {
    type master;
    file "centos.org.lan";
    allow-update { none; };
};
.....
zone "centos.co.id" IN {
    type slave;
    masters { 129.93.88.11; };
    file "centos.co.id.wan";
    notify no;
};
zone "centos.org" IN {
    type slave;
    masters { 129.93.88.11; };
    file "centos.org.wan";
    notify no;
};

```

```
};
```

Text tercetak tebal adalah konfigurasi yang ditambahkan dalam multidomain DNS, selanjutnya copy file centos.co.id.lan dan centos.co.id.wan menjadi centos.org.lan dan centos.org.wan

```
[root@srv1 chroot]# cp var/named/centos.co.id.lan var/named/centos.org.lan
[root@srv1 chroot]# cp var/named/centos.co.id.wan var/named/centos.org.wan
```

Ganti beberapa parameter yang dibutuhkan pada file centos.org.lan dan centos.org.wan

```
[root@srv1 chroot]# vim var/named/centos.org.lan
$TTL 86400
@      IN      SOA      srv1.centos.co.id. root.centos.co.id. (
        20120526      ;Serial
        3600          ;Refresh
        1800          ;Retry
        604800        ;Expire
        86400         ;Minimum TTL
)
      IN      NS       srv1.centos.co.id.
      IN      NS       srv2.centos.co.id.
      IN      A        192.168.10.12
      IN      MX 10    mail.centos.org.
srv1    IN      A        192.168.10.11
srv2    IN      A        192.168.10.12
mail    IN      CNAME   srv1.centos.org.
www     IN      CNAME   srv2.centos.org.
```

```
[root@srv1 chroot]# vim var/named/centos.org.wan
$TTL 86400
@      IN      SOA      srv1.centos.co.id. root.centos.co.id. (
        20120526      ;Serial
        3600          ;Refresh
        1800          ;Retry
        604800        ;Expire
        86400         ;Minimum TTL
)
      IN      NS       srv1.centos.co.id.
      IN      NS       srv2.centos.co.id.
      IN      A        129.93.88.12
      IN      MX 10    mail.centos.org.
srv1    IN      A        129.93.88.11
srv2    IN      A        129.93.88.12
mail    IN      CNAME   srv1.centos.org.
www     IN      CNAME   srv2.centos.org.
```

Simpan hasil konfigurasi dan restart DNS Server

```
[root@srv1 chroot]# service named restart
Stopping named: [ OK ]
Starting named: [ OK ]
[root@srv1 chroot]# rndc reload
server reload successful
```

Tambahkan juga konfigurasi yang terdapat di Server DNS Slave, edit file named.conf. Tambahkan parameter domain centos.org

```
[root@srv2 ~]# cd /var/named/chroot/
[root@srv2 chroot]# vim etc/named.conf
options {
    listen-on-v6 {none;};
    directory "/var/named";
    recursion yes;
};

zone "centos.co.id" IN {
    type slave;
    masters { 129.93.88.11; };
    file "slaves/centos.co.id.wan";
    notify no;
};

zone "centos.org" IN {
    type slave;
    masters { 129.93.88.11; };
    file "slaves/centos.org.wan";
    notify no;
};
zone "88.93.129.in-addr.arpa" IN {
    type slave;
    masters { 129.93.88.11; };
    file "slaves/88.93.129.db";
    notify no;
};
```

Selanjutnya restart DNS Server dan jalankan reload layanan rndc

```
[root@srv2 chroot]# service named restart
Stopping named: [ OK ]
Starting named: [ OK ]
[root@srv2 chroot]# rndc reload
server reload successful
[root@srv2 chroot]#
```

Pastikan file centos.org.wan sudah berada di direktori slave

```
[root@srv2 chroot]# ls var/named/slaves/
88.93.129.db centos.co.id.wan centos.org.wan
```

Langkah terakhir lakukan uji coba dengan menjalankan perintah nslookup dari server DNS Slave

```
[root@srv2 chroot]# nslookup www.centos.org
Server:          129.93.88.11
Address:        129.93.88.11#53

www.centos.org canonical name = srv2.centos.org.
Name: srv2.centos.org
Address: 129.93.88.12
```

DHCP Server

DHCP (Dynamic Host Configuration Protocol) merupakan suatu adalah layanan yang mengatur pemberian IP Address, Netmask, Gateway dan beberapa parameter yang dibutuhkan untuk terkoneksi dengan jaringan. Kemudahan yang didapatkan dari layanan ini adalah anda tidak perlu melakukan konfigurasi di semua komputer yang terdapat di kantor anda, sebab dengan layanan ini semua komputer yang terhubung dengan jaringan akan mendapatkan IP Address secara otomatis.

Layanan ini sangat diperlukan jika pada suatu perusahaan memiliki beberapa unit komputer yang terhubung dalam jaringan sedangkan lokasinya berjauhan, sehingga akan memudahkan pada administrator dalam melakukan konfigurasi networking tanpa perlu mendatangi lokasi tempat komputer berada.

5.1. Instalasi DHCP Server

Paket yang dibutuhkan untuk membangun server DHCP adalah paket dhcp yang terdapat di repositori, secara umum paket tersebut sudah disiapkan, sehingga implementasi dhcp semakin memudahkan pengguna. Berikut ini beberapa langkah yang dibutuhkan dalam implementasi dhcp

Instalasi terlebih dahulu dhcp menggunakan perintah yum install di bawah ini

```
[root@proxy ~]# yum install dhcp
Loaded plugins: fastestmirror
Loading mirror speeds from cached hostfile
 * base: centos.idrepo.or.id
 * extras: mirror.vietoss.com
=====
Package   Arch Version           Repository Size
=====
Installing:
  dhcp     i386 12:3.0.5-31.el5 base          873 k

Transaction Summary
=====
Install      1 Package(s)
Upgrade     0 Package(s)

Total download size: 873 k
Is this ok [y/N]:
```

Ketik tombol Y untuk melanjutkan proses instalasi, jika anda menggunakan CentOS 6 maka dalam menjalankan perintah instalasi sedikit berbeda. Hal tersebut disebabkan paket dhcp yang terdapat di CentOS 6 conflicts dengan paket yang sudah terinstall yaitu dhclient.i686. Sehingga sebelum anda menjalankan instalasi, sebaiknya anda hapus terlebih dahulu paket dhclient.i686

```
[root@proxy ~]# yum install -y dhcp
Transaction Check Error:
  file /usr/share/man/man5/dhcp-eval.5.gz from install of dhcp-common-
12:4.1.1-25.P1.el6_2.1.i686 conflicts with file from package dhclient-
12:4.1.1-12.P1.el6.i686
  file /usr/share/man/man5/dhcp-options.5.gz from install of dhcp-common-
12:4.1.1-25.P1.el6_2.1.i686 conflicts with file from package dhclient-
```

```
12:4.1.1-12.P1.el6.i686
Error Summary
```

Dalam proses tersebut `dhclient.i686` conflicts dengan paket `dhcp` sehingga anda harus menghapusnya terlebih dahulu, seperti perintah dibawah ini

```
[root@proxy ~]# yum remove dhclient -y
Running Transaction
Erasing          : 12:dhclient-4.1.1-12.P1.el6.i686
 1/1 Removed:
dhclient.i686 12:4.1.1-12.P1.el6
Complete!
[root@proxy ~]# yum install -y dhcp
Running Transaction
Installing       : 12:dhcp-common-4.1.1-25.P1.el6_2.1.i686
 1/2 Installing  : 12:dhcp-4.1.1-25.P1.el6_2.1.i686
 2/2 Installed:
dhcp.i686 12:4.1.1-25.P1.el6_2.1
Dependency Installed:
dhcp-common.i686 12:4.1.1-25.P1.el6_2.1
Complete!
```

5.2. Konfigurasi DHCP Server

Setelah proses instalasi berjalan dengan baik anda bisa melanjutkan dengan konfigurasi `dhcpd.conf` yang terletak di direktori `/etc`, hanya saja ada sedikit perbedaan lokasi antara CentOS 5 dan CentOS 6. Jika CentOS 5 lokasi file `dhcpd.conf` berada pada direktori `/etc` sedangkan CentOS 6 berada pada file `/etc/dhcp`. File utama `dhcp` yang terletak pada direktori `/etc` merupakan lokasi dimana anda akan menerapkan beberapa parameter yang digunakan `dhcp` server. Coba kita masuk pada file tersebut dengan perintah di bawah ini

```
[root@proxy ~]# vim /etc/dhcpd.conf
#
# DHCP Server Configuration file.
#   see /usr/share/doc/dhcp*/dhcpd.conf.sample
#
```

Secara default isi file `dhcpd.conf` kosong, sehingga anda bisa melihat detail contoh konfigurasi `dhcp` pada direktori berikut ini, masuk terlebih dahulu ke dokumentasi `dhcp` dengan perintah

```
[root@proxy ~]# cd /usr/share/doc/dhcp-3.0.5/
[root@proxy dhcp-3.0.5]# ls
dhcpd.conf.sample draft-ietf-dhc-failover-07.txt
[root@proxy dhcp-3.0.5]#
```

file `dhcpd.conf.sample` adalah contoh konfigurasi `dhcp` server, sehingga backup terlebih dahulu file konfigurasi utama selanjutnya copy file tersebut ke direktori `/etc`

```
[root@proxy dhcp-3.0.5]# mv /etc/dhcpd.conf /etc/dhcpd.conf.back
[root@proxy dhcp-3.0.5]# cp dhcpd.conf.sample /etc/dhcpd.conf
```

Setelah anda berhasil copy file `sample` ke direktori `/etc` maka anda bisa memulai memodifikasi file

sample tersebut sesuai dengan kebutuhan.

```
[root@proxy ~]# vim /etc/dhcpd.conf
ddns-update-style interim;
ignore client-updates;

subnet 192.168.10.0 netmask 255.255.255.0 {

# --- default gateway
    option routers                192.168.10.1;
    option subnet-mask            255.255.255.0;

    option nis-domain             "proxy.centos.co.id";
    option domain-name            "proxy.centos.co.id";
    option domain-name-servers   192.168.10.1;

    option time-offset            -18000; # Eastern Standard Time
#    option ntp-servers           192.168.10.1;
#    option netbios-name-servers 192.168.10.1;
# --- Selects point-to-point node (default is hybrid). Don't change this
unless
# -- you understand Netbios very well
#    option netbios-node-type 2;

    range dynamic-bootp 192.168.10.100 192.168.10.100;
    default-lease-time 21600;
    max-lease-time 43200;

#    # we want the nameserver to appear at a fixed address
#    host ns {
#        next-server marvin.redhat.com;
#        hardware ethernet 12:34:56:78:AB:CD;
#        fixed-address 207.175.42.254;
#    }
}
```

Agar memudahkan pengguna maka penulis cetak tebal beberapa konfigurasi standart yang sudah dirubah. Selanjutnya menentukan Ethernet (LAN) yang digunakan sebagai pusat dhcp server.

```
[root@proxy ~]# vim /etc/sysconfig/dhcpd
# Command line options here
DHCPDARGS=eth1
```

Tambahkan eth1, simpan dan tutup editor vim. Langkah selanjutnya restart layanan dhcp server

```
[root@proxy ~]# service dhcpd start
Starting dhcpd: [ OK ]
[root@proxy ~]# chkconfig dhcpd on
```

Jika anda ingin menetapkan IP berdasarkan MAC Address maka pada baris paling bawah tambahkan script seperti pada contoh berikut, atau membuka beberapa parameter paling bawah (we want the nameserver to appear at a fixed address host ns)

```
host pc01 {
hardware ethernet 08:00:07:26:c0:a5;
fixed-address 192.168.10.100;
}
```

Setelah anda menambahkan konfigurasi dari setiap layanan, jangan lupa restart kembali layanan tersebut agar perintah yang anda rubah bisa berjalan di service tersebut. Jika beberapa konfigurasi diatas sudah selesai anda bisa mencobanya dengan menghubungkan PC/Laptop ke server tersebut, dengan catatan jangan lupa untuk setting mode automatic agar klien mendapatkan IP Address dari Server.

5.3. Konfigurasi DHCP Server 2 Network

Layanan DHCP selain digunakan untuk memberikan IP Address dalam satu jaringan, ternyata bisa juga digunakan untuk beberapa IP Address, dan hal tersebut tergantung berapa banyak Ethernet (LAN Card) yang dimiliki Server. Server yang digunakan kali ini menggunakan 3 Lan Card masing-masing di pergunakan sebagai jalur internet dan 2 Lan Card sebagai distribusi IP Address. Konfigurasi yang digunakan hanya sederhana yaitu menambahkan IP lagi di file utama dhcpd.conf seperti pada contoh berikut ini

```
[root@proxy ~]# vim /etc/dhcpd.conf
subnet 192.168.10.0 netmask 255.255.255.0 {
    range 192.168.10.100 192.168.10.200;
    option domain-name-servers 129.93.88.11, 129.93.88.11;
    option domain-name "192.168.10.1";
    option routers 192.168.10.1;
    option broadcast-address 192.168.10.255;
    default-lease-time 600;
    max-lease-time 7200;
}
subnet 192.168.20.0 netmask 255.255.255.0 {
    range 192.168.20.100 192.168.20.200;
    option domain-name-servers 129.93.88.11, 129.93.88.11;
    option domain-name "192.168.20.1";
    option routers 192.168.20.1;
    option broadcast-address 192.168.20.255;
    default-lease-time 600;
    max-lease-time 7200;
}
```

Simpan file konfigurasi tersebut, lanjutkan dengan menambahkan interface yang digunakan pada file dhcpd

```
[root@proxy ~]# nano /etc/sysconfig/dhcpd
# Command line options here
DHCPDARGS="eth2 eth1"
```

Terakhir restart DHCP Server dengan perintah berikut ini

```
[root@proxy ~]# service dhcpd restart
```

File Sharing

6.1. Pengertian Samba

Samba, merupakan protokol yang digunakan untuk menjembatani hubungan pertukaran data yang di miliki Unix/Linux agar bisa berhubungan dengan sistem operasi yang berbeda. Dalam proses pertukaran data terhadap sistem operasi Linux berbeda dengan Microsoft Windows. Linux memiliki sistem pertukaran data yang lebih spesifik dan lengkap. Selain digunakan dalam sharing data, Samba memiliki beberapa fitur yang tidak dimiliki sharing data yang lain, diantaranya authentication user, filtering extension dan beberapa parameter yang lain. Sehingga samba memang pantas diandalkan jika dipergunakan dalam File Sharing.

Project Samba dikembangkan Andrew Rridgell pada tahun 1991. Project tersebut dimulai ketika Andrew R. menciptakan File Server di rumahnya yang mendukung protokol DEC dari Digital Pathworks. Hingga saat ini protocol ini dikembangkan para programmer pengembang Open Source diseluruh dunia.

6.2. Instalasi Samba

Paket samba sebelumnya sudah tersedia di dalam repositori sehingga anda bisa melakukan instalasi dengan mudah yaitu menggunakan perintah di bawah ini

```
[root@proxy ~]# yum install samba
Loaded plugins: fastestmirror
Loading mirror speeds from cached hostfile
Dependencies Resolved

=====
Package            Arch      Version              Repository           Size
=====
Updating:
samba              i386     3.0.33-3.39.el5_8   updates             16 M
Updating for dependencies:
libsmbclient      i386     3.0.33-3.39.el5_8   updates             909 k
samba-client      i386     3.0.33-3.39.el5_8   updates             5.7 M
samba-common      i386     3.0.33-3.39.el5_8   updates             6.7 M
Transaction Summary
=====
Install           0 Package(s)
Upgrade          4 Package(s)

Total download size: 30 M
Is this ok [y/N]:
```

Lanjutkan dengan mengetik tombol Y, tunggu beberapa saat hingga proses unduh paket dan proses instalasi selesai di kerjakan. Untuk menghindari kesalahan dalam menambahkan perintah, maka backup terlebih dahulu file utama yaitu smb.conf

```
[root@proxy ~]# cd /etc/samba/
[root@proxy samba]# cp smb.conf smb.conf.back
[root@proxy samba]# vim smb.conf
```

Ganti standart konfigurasi security = user menjadi share, perintah tersebut dipergunakan untuk mengijinkan user yang tidak memiliki account password pada samba agar bisa mengakses file sharing yang tersedia.

```
security = share
```

Buatlah sebuah folder sebagai file sharing pada direktori home dengan perintah di bawah ini

```
[root@proxy home]# mkdir data
[root@proxy home]# chmod 777 data/
[root@proxy home]# vim /etc/samba/smb.conf
```

Setelah direktori selesai dibuat maka tetapkan permission terhadap direktori tersebut. Pada akhir script file smb.conf tambahkan konfigurasi di bawah ini

```
[data]
path = /home/data
guest ok = yes
writeable = yes
browseable = yes
create mode = 0770
directory mode = 0770
```

Konfigurasi tersebut merupakan contoh sederhana dalam pembuatan file sharing, selanjutnya agar konfigurasi yang sudah anda buat bisa berjalan maka restart terlebih dahulu layanan samba dengan perintah seperti di bawah ini

```
[root@proxy samba]# service smb restart
Shutting down SMB services:           [ OK ]
Starting SMB services:                [ OK ]
[root@proxy samba]#
[root@proxy samba]# chkconfig smb on
[root@proxy samba]# chkconfig nmb on
```

6.3. Membatasi Samba

Layanan ini selain digunakan sebagai folder sharing juga memiliki fitur memberikan password pada setiap direktori, sehingga akan lebih aman jika beberapa folder yang memang dianggap rahasia diberikan sebuah password. Misalnya di File Server mempunyai 2 direktori yaitu accounting dan production. Kedua direktori tersebut akan di berikan hak akses dengan aturan yang sudah dibuat administrator yaitu pada direktori accounting hanya bisa diakses oleh user1, sebaliknya direktori production hanya bisa diakses oleh user2. Pada contoh konfigurasi kali ini penulis menggunakan fitur group pada CentOS sehingga direktori sharing bisa diakses lebih dari satu user.

Buatlah group dan direktori accounting dan production, selanjutnya berikan permission pada tiap-tiap direktori tersebut, berikut penjelasannya

```
[root@proxy ~]# groupadd accounting
[root@proxy ~]# groupadd production
[root@proxy ~]# mkdir /home/accounting
[root@proxy ~]# mkdir /home/production
[root@proxy ~]# chgrp accounting /home/accounting/
[root@proxy ~]# chgrp production /home/production/
[root@proxy ~]# chmod 0770 /home/accounting/
[root@proxy ~]# chmod 0770 /home/production/
```

Setelah direktori di buat maka langkah selanjutnya adalah membuat user dan password dari setiap user, berikut caranya

```
[root@proxy ~]# useradd user1
[root@proxy ~]# passwd user1
Changing password for user user1.
```

```
New password:
Retype new password:
passwd: all authentication tokens updated successfully.
[root@proxy ~]# useradd user2
[root@proxy ~]# passwd user2
Changing password for user user2.
New password:
Retype new password:
passwd: all authentication tokens updated successfully.
```

Selanjutnya tambahkan user yang sudah dibuat kedalam group

```
[root@proxy ~]# nano /etc/group
accounting:x:500:user1
production:x:501:user2
```

Setelah user yang diinginkan dibuat langkah selanjutnya adalah memberikan password smb pada masing-masing user, seperti pada perintah dibawah ini

```
[root@proxy ~]# smbpasswd -a user1
New SMB password:
Retype new SMB password:
Added user user1.
[root@proxy ~]# smbpasswd -a user2
New SMB password:
Retype new SMB password:
Added user user2.
```

Tambahkan script untuk authentication file sharing seperti pada contoh pada konfigurasi samba

```
[root@proxy home]# vim /etc/samba/smb.conf
security = user // ubah dari share jadi user
[accounting]
path = /home/accounting
writable = yes
create mode = 0770
directory mode = 0770
guest ok = no
valid users = @accounting

[production]
path = /home/production
writable = yes
create mode = 0770
directory mode = 0770
guest ok = no
valid users = @production
```

Setelah anda selesai menambahkan script pada samba langkah selanjutnya adalah restart samba dengan perintah di bawah ini

```
[root@proxy ~]# service smb restart
Shutting down SMB services:          [ OK ]
Starting SMB services:              [ OK ]
[root@proxy ~]#
```

6.4. Akses Samba dari Klien

Samba merupakan paket software yang bisa di akses di berbagai Operating System seperti Microsoft Windows, Linux dan Mac OS. Berikut ini penulis akan menunjukkan bagaimana mengkoneksikan klien ke File Sharing Samba.

Jika anda menggunakan Microsoft Windows maka buka run selanjutnya ketik “\\192.168.10.1” tanpa tanda petik, maka akan terlihat dialog untuk konfirmasi password samba berikut ini



Jika klien yang anda pergunakan adalah Linux maka ketikkan pada menu network di nautitus dengan perintah “smb://192.168.10.1” tanpa tanda petik, sehingga akan tampil menu password berikut ini



Maka akan terlihat dialog konfirmasi user dan password, isi form yang telah disediakan tersebut, klik connect untuk melanjutkan

6.5. Menambahkan Fitur Recycle Bin

Banyak sekali fitur yang dimiliki Samba, diantaranya mampu membuat virtual Recycle Bin. Fitur ini merupakan tempat penyimpanan sementara dari beberapa file yang sudah dihapus, sehingga akan membantu anda ketika akan mengembalikan file yang sudah dihapus tersebut. Ada beberapa hal yang perlu dipersiapkan dalam menerapkan media penyimpanan sementara pada Samba, diantaranya adalah

Buatlah sebuah file recycle.conf dan letakkan di direktori samba, file tersebut digunakan sebagai

lokasi penulisan script pembuatan recycle bin atau penyimpanan sementara

```
[root@proxy ~]# vim /etc/samba/recycle.conf
```

Setelah anda masuk pada direktori recycle.conf selanjutnya tambahkan script berikut ini

```
name = Recycle Bin
mode = KEEP_DIRECTORIES|VERSIONS|TOUCH
maxsize = 0
exclude = *.tmp|*.temp|*.o|*.obj|~$*|*.~??|*.log|*.trace
excludedir = /tmp|/temp|/cache
noverisons = *.doc|*.ppt|*.dat|*.ini|*.xls|*.pdf|*.txt
```

Simpan dan keluar dari direktori vim, selanjutnya tambahkan beberapa parameter di file utama samba. Agar memudahkan beberapa parameter yang sudah ditambahkan penulis cetak tebal

```
[root@proxy ~]# vim /etc/samba/smb.conf
[data]
path = /home/data
guest ok = yes
writeable = yes
browseable = yes
create mode = 0770
directory mode = 0770
vfs object = recycle
config-file = /etc/samba/recycle.conf
recycle:repository = Recycle Bin
recycle:keeptree = Yes
recycle:versions = Yes
# Konfigurasi tambahan
# hosts allow = 192.168.10.100
# veto files = /*.eml/*.*.nws/*.*.dll/*.*.mp3/*.*.MP3/*.*.mpg/*.*.MPG/*.*.vbs/*.*.VBS/
```

Simpan dan keluar dari editor tersebut. Konfigurasi diatas terdapat beberapa tambahan yaitu rule **hosts allow** digunakan sebagai mendaftarkan IP Address yang di ijinan akses direktori tersebut sedangkan pada rule

veto files digunakan sebagai block extension, misalnya pada konfigurasi diatas. Extensi yang sudah terdaftar maka jika ada user yang meletakkan extensi tersebut akan di block secara otomatis. Agar fitur tersebut dijalankan buka tanda pagar (#)

Selanjutnya restart layanan samba agar perintah tersebut berjalan di sistem anda

```
[root@proxy ~]# service smb restart
Shutting down SMB services:          [ OK ]
Shutting down NMB services:         [ OK ]
Starting SMB services:              [ OK ]
Starting NMB services:              [ OK ]
[root@proxy ~]#
```

Pastikan dalam konfigurasi tersebut tidak terdapat error sehingga hasil dari pembuatan file server tidak terdapat kendala.

FTP Server

FTP (File Transfer Protocol) merupakan salah satu protokol TCP/IP yang dipergunakan sebagai pengiriman dan pertukaran data, pada umumnya FTP dipergunakan jika pengguna akan melakukan aktifitas upload data misalnya website dan database, sehingga jika anda sudah akrab dengan web hosting maka FTP merupakan istilah yang tidak asing bagi anda, pada kali ini penulis akan mencoba membahas mengenai bagaimana cara membuat sebuah FTP Server. Secara teknis dalam penerapan FTP harus mempunyai 2 konsep yaitu FTP Server dan FTP Client

7.1. Instalasi VSFTPD

Dalam implementasi FTP Server Linux memiliki beberapa pilihan yang digunakan sebagai Server FTP yaitu vsftpd, proftpd, pureftpd dll, dari setiap paket software memiliki kelebihan dan kekurangan yang ditonjolkan, hanya saja bagi penulis vsftpd adalah paket FTP Se server yang paling aman dinilai dari segi fitur dan keamanannya. Walaupun tidak ada sistem yang 100% aman tapi vsftpd memiliki beberapa security yang bisa diandalkan, berikut ini adalah langkah-langkah dalam membangun FTP Server menggunakan vsftpd.

```
[root@ftp ~]# yum install vsftpd
=====
Package Arch Version Repository Size
=====
Updating:
vsftpd i386 2.0.5-24.el5_8.1 updates 144 k

Transaction Summary
=====
Install 0 Package(s)
Upgrade 1 Package(s)

Total download size: 144 k
Is this ok [y/N]
```

Setelah instalasi vsftpd selesai jalankan layanan vsftpd dengan perintah dibawah ini

```
[root@ftp ~]# service vsftpd start
Starting vsftpd for vsftpd: [ OK ]
[root@ftp ~]# chkconfig vsftpd on
[root@ftp ~]# chkconfig --list vsftpd
vsftpd 0:off1:off2:on 3:on 4:on 5:on 6:off
[root@ftp ~]# netstat -anp | grep vsftpd
tcp 0 0 0.0.0.0:21 0.0.0.0:* LISTEN
8793/vsftpd
```

Selanjutnya adalah login pada pada FTP Server, secara default Linux CentOS 6 belum memiliki paket FTP untuk klien sehingga sebelum menjalankan perintah ftp maka anda install terlebih dahulu dengan perintah dibawah ini, tetapi jika anda menggunakan CentOS 5 sudah otomatis terinstall pada sistem

```
[root@ftp ~]# yum install ftp -y
[root@ftp ~]# ftp localhost
Trying ::1...
ftp: connect to address ::1Connection refused
Trying 127.0.0.1...
Connected to localhost (127.0.0.1).
220 (vsFTPD 2.2.2)
Name (localhost:root): root
530 Permission denied.
Login failed.
```

Proses login menggunakan hak akses root akan selalu mendapatkan peringatan permission denied, hal tersebut disebabkan bahwa default user root tidak di ijinan untuk login pada vsftpd, sehingga anda perlu membuat user baru agar bisa masuk pada vsftpd

```
[root@ftp ~]# adduser mafatahna
[root@ftp ~]# passwd mafatahna
Changing password for user mafatahna.
New password:
Retype new password:
passwd: all authentication tokens updated successfully.
```

Setelah anda menambahkan user baru maka coba login lagi di vsftpd menggunakan perintah

```
[root@ftp ~]# ftp localhost
Connected to localhost.localdomain.
220 (vsFTPD 2.0.5)
530 Please login with USER and PASS.
530 Please login with USER and PASS.
KERBEROS_V4 rejected as an authentication type
Name (localhost:root): mafatahna
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp>
```

Jika anda menggunakan CentOS 6 ada beberapa hal yang perlu diperhatikan, berikut ini adalah contoh informasi error ketika login vsftpd

```
[root@ftp ~]# ftp localhost
Trying ::1...
ftp: connect to address ::1Connection refused
Trying 127.0.0.1...
Connected to localhost (127.0.0.1).
220 (vsFTPD 2.2.2)
Name (localhost:root): mafatahna
331 Please specify the password.
Password:
```

```
500 OOPS: cannot change directory:/home/mafatahna
Login failed.
```

Informasi error pada perintah diatas yaitu 500 OOPS: cannot change directory:/home/mafatahna, maksud dari informasi tersebut adalah SELinux menolak akses terhadap direktori tersebut sehingga coba lakukan pengecekan dengan menjalankan “getenforce”

```
[root@ftp ~]# getenforce
Enforcing
[root@ftp ~]# getsebool -a | grep ftp
allow_ftp_anon_write --> off
allow_ftp_full_access --> off
allow_ftp_use_cifs --> off
allow_ftp_use_nfs --> off
ftp_home_dir --> off
ftpd_connect_db --> off
httpd_enable_ftp_server --> off
sftpd_anon_write --> off
sftpd_enable_homedirs --> off
sftpd_full_access --> off
sftpd_write_ssh_home --> off
tftp_anon_write --> off
[root@ftp ~]#
```

Jika pada hasil getenforce dijelaskan bahwa ftp_home_dir masih dalam kondisi off, maka aktifkan terlebih dahulu dengan menggunakan perintah dibawah ini

```
[root@ftp ~]# setsebool -P ftp_home_dir=1
atau
[root@ftp ~]# setsebool -P ftp_home_dir on
```

Selanjutnya lakukan login lagi dengan perintah

```
[root@ftp ~]# ftp localhost
Trying ::1...
ftp: connect to address ::1: Connection refused
Trying 127.0.0.1...
Connected to localhost (127.0.0.1).
220 (vsFTPd 2.2.2)
Name (localhost:root): mafatahna
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> pwd
257 "/home/mafatahna"
ftp>
```

Jika muncul informasi bahawa “Login Successful” berarti login anda ke FTP sudah sukses.

7.2. Mengaktifkan User Anonymous

Anonymous adalah user yang terbuat secara otomatis ketika instalasi vsftpd sehingga untuk login ke FTP Server bisa menggunakan user anonymous, user ini tidak memiliki password sehingga jika anda memiliki data sangat penting di FTP Server tersebut maka jangan pernah aktifkan fitur ini. Edit file utama vsftpd.conf seperti dibawah ini

```
[root@ftp ~]# vim /etc/vsftpd/vsftpd.conf
# Allow anonymous FTP? (Beware - allowed by default if you comment this
out).
anonymous_enable=YES
```

Pastikan pada rule `anonymous_enable` anda setting YES, sehingga user anonymous aktif. Setelah user tersebut di ijinakan maka anda bisa melakukan uploading file. Misalnya anda mempunyai file `data.txt`, dan akan anda upload ke FTP Server menggunakan user anonymous. Perintahnya adalah

```
mafatahna@mafatahna:~/Documents$ touch data.txt
mafatahna@mafatahna:~/Documents$ ftp 192.168.10.16
Connected to 192.168.10.16.
220 (vsFTPd 2.2.2)
Name (192.168.10.16:mafatahna): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> put data.txt
local: data.txt remote: data.txt
200 PORT command successful. Consider using PASV.
550 Permission denied.
ftp>
```

Dalam dialog diatas terdapat informasi bahwa ketika upload file terdapat peringatan `Permission denied`, informasi tersebut disebabkan fitur upload untuk anonymous belum diaktifkan hak aksesnya adalah edit file utama dan rubah beberapa parameter di bawah ini

```
[root@ftp ~]# vim /etc/vsftpd/vsftpd.conf
# Allow anonymous FTP? (Beware - allowed by default if you comment this
out).
anonymous_enable=YES
#
# Uncomment this to allow local users to log in.
local_enable=YES
#
# Uncomment this to enable any form of FTP write command.
write_enable=YES
# Uncomment this to allow the anonymous FTP user to upload files. This
only
# has an effect if the above global write enable is activated. Also,
you will
# obviously need to create a directory writable by the FTP user.
```

```
anon_upload_enable=YES
```

```
# Uncomment this if you want the anonymous FTP user to be able to  
create
```

```
# new directories.
```

```
anon_mkdir_write_enable=YES
```

Simpan dan keluar dari editor vim. Konfigurasi permission direktori tersebut dengan perintah dibawah ini

```
[root@ftp ~]# cd /var/ftp/  
[root@ftp ftp]# mkdir upload  
[root@ftp ftp]# chown ftp.ftp upload/  
[root@ftp ftp]# chmod 755 upload/  
[root@ftp ftp]# ls -la  
total 16  
drwxr-xr-x.  4 root root 4096 May 12 10:42 .  
drwxr-xr-x. 22 root root 4096 May 12 09:23 ..  
drwxr-xr-x.  2 root root 4096 Jan  3 08:21 pub  
drwxr-xr-x   2 ftp  ftp  4096 May 12 10:42 upload  
[root@ftp ftp]# service vsftpd restart  
Shutting down vsftpd:                [ OK ]  
Starting vsftpd for vsftpd:          [ OK ]
```

Setelah konfigurasi selesai coba lakukan login dengan user anonymous

```
mafatahna@mafatahna:~/Documents$ ftp 192.168.10.16  
Connected to 192.168.10.16.  
220 (vsFTPd 2.2.2)  
Name (192.168.10.16:mafatahna): anonymous  
331 Please specify the password.  
Password:  
230 Login successful.  
Remote system type is UNIX.  
Using binary mode to transfer files.  
ftp> dir  
200 PORT command successful. Consider using PASV.  
150 Here comes the directory listing.  
drwxr-xr-x   2 0          0          4096 Jan 03 01:21 pub  
drwxr-xr-x   2 14         50          4096 May 12 03:42 upload  
226 Directory send OK.  
ftp> cd upload  
250 Directory successfully changed.  
ftp> put data.txt  
local: data.txt remote: data.txt  
200 PORT command successful. Consider using PASV.  
150 Ok to send data.  
226 Transfer complete.  
ftp>
```

7.3. Membatasi Akses User

Sebelumnya, anda mencoba login menggunakan user root muncul informasi permission denied, hal tersebut merupakan default konfigurasi pada vsftpd, sehingga jika ingin user lain dibatasi hak aksesnya maka anda hanya perlu edit file ftpusers seperti pada contoh dibawah ini

```
mafatahna@mafatahna:~$ ftp 192.168.10.16
Connected to 192.168.10.16.
220 (vsFTPD 2.2.2)
Name (192.168.10.16:mafatahna): mafatahna
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
```

Login menggunakan user mafatahna dalam contoh diatas login berhasil, jika anda ingin block user tersebut caranya adalah edit file ftpusers seperti dibawah ini

```
[root@ftp ftp]# vim /etc/vsftpd/ftpusers
# Users that are not allowed to login via ftp
root      # user root
bin
daemon
adm
lp
sync
shutdown
halt
mail
news
uucp
operator
games
nobody
mafatahna # Tambahkan user mafatahna
```

Lakukan login sekali lagi pada user yang sudah terdaftar pada ftpusers yaitu mafatahna

```
mafatahna@mafatahna:~$ ftp 192.168.10.16
Connected to 192.168.10.16.
220 (vsFTPD 2.2.2)
Name (192.168.10.16:mafatahna): mafatahna
331 Please specify the password.
Password:
530 Login incorrect.
Login failed.
ftp>
```

7.4. Membatasi Akses User dengan Chroot

Account pada user FTP ada kalanya di ijin untuk download / upload pada sebuah file yang sudah disediakan pada Server FTP, tetapi ada kalanya file tersebut tidak boleh di download sehingga perlu beberapa konfigurasi tambahan yaitu dengan memanfaatkan chroot FTP.

Buat terlebih dahulu user yang dipergunakan untuk download / upload (misalnya user fatahna), sedangkan user yang pertama (mafatahna) dibatasi

```
[root@ftp ftp]# adduser fatahna
[root@ftp ftp]# passwd fatahna
[root@ftp home]# vim /etc/vsftpd/vsftpd.conf
# You may specify an explicit list of local users to chroot() to their
# home
# directory. If chroot_local_user is YES, then this list becomes a list
# of
# users to NOT chroot().
#chroot_local_user=YES
chroot_list_enable=YES
# (default follows)
chroot_list_file=/etc/vsftpd/chroot_list
[root@ftp home]# cd /etc/vsftpd/
[root@ftp vsftpd]# touch chroot_list
[root@ftp vsftpd]# vi chroot_list
mafatahna # Tambahkan pada akhir script
[root@ftp vsftpd]# service vsftpd restart
Shutting down vsftpd:          [ OK ]
Starting vsftpd for vsftpd:   [ OK ]
[root@ftp vsftpd]#
```

Langkah selanjutnya adalah melakukan ujicoba user dengan hak akses user mafatahna (dibatasi) dan user fatahna (tidak dibatasi)

```
mafatahna@mafatahna:~$ ftp 192.168.10.16
Connected to 192.168.10.16.
220 (vsFTPd 2.2.2)
Name (192.168.10.16:mafatahna): mafatahna
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> cd /etc/
550 Failed to change directory.
```

Disebutkan diatas bahwa user mafatahna tidak bisa memasuki direktori /etc, disebabkan pada script chroot vsftpd user mafatahna sudah di masukkan.

Selanjutnya menggunakan user fatahna, dalam hal ini user ini tidak dibatasi akses ke FTP Server

```

mafatahna@mafatahna:~$ ftp 192.168.10.16
Connected to 192.168.10.16.
220 (vsFTPD 2.2.2)
Name (192.168.10.16:mafatahna): fatahna
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> cd /etc/
250 Directory successfully changed.

```

Login berhasil, disebabkan user tersebut tidak terdaftar di file `chroot_list`.

7.5. Menganti Direktori Default User Anonymous

Secara default direktori pada user anonymous lokasinya terdapat di “`/var/ftp`”, jika FTP Server yang dipergunakan saat ini menjadi mirror atau biasa dikatakan dengan tempat repository Linux maka biasaya ketika instalasi server terdapat partisi yang sudah dipersiapkan sebagai penyimpanan file, sehingga sangat penting sekali untuk mengetahui bagaimana caranya untuk mengubah default direktori pada anonymous ke direktori yang di inginkan.

Berikut ini beberapa langkah yang dibutuhkan, edit terlebih dahulu konfigurasi pada `vsftpd.conf` selanjutnya tambahkan rule “`local_root=/home`” home bisa diganti dengan posisi direktori anda

```

[root@ftp vsftpd]# vim /etc/vsftpd/vsftpd.conf
local_root=/home          // Tambahkan pada script
[root@ftp vsftpd]# vim /etc/passwd
ftp:x:14:50:FTP User:/var/ftp:/sbin/nologin
Ganti konfigurasi dengan
ftp:x:14:50:FTP User:/home:/sbin/nologin

[root@ftp ~]# service vsftpd restart
Shutting down vsftpd:          [ OK ]
Starting vsftpd for vsftpd:   [ OK ]

```

Implementasi User Group

Hak akses dalam mode group bisa anda pergunakan jika anda mempunyai satu direktori saja yang akan anda share ke FTP Server dan user yang di ijin akses ke direktori tersebut lebih dari satu. Sehingga anda perlu mengelompokkan beberapa user tersebut pada sebuah group. Dengan begitu administrator tidak akan kesulitan dalam konfigurasi satu persatu dalam setiap user, berikut ini adalah langkah-langkah yang dibutuhkan dalam konfigurasi tersebut.

Ganti konfigurasi `anonymous_enable` menjadi `no`, seperti konfigurasi berikut ini

```

[root@ftp vsftpd]# vim /etc/vsftpd/vsftpd.conf
# Allow anonymous FTP? (Beware - allowed by default if you comment this
out).
anonymous_enable=NO

```

Setelah user anonymous di non-aktifkan maka langkah selanjutnya adalah membuat sebuah group dan beberapa user serta pengaturan hak akses user tersebut

```
[root@ftp ~]# groupadd ftp-document
[root@ftp ~]# mkdir /home/ftp-document

[root@ftp ~]# chmod 750 /home/ftp-document/
[root@ftp ~]# chown root:ftp-document /home/ftp-document/

[root@ftp ~]# useradd -g ftp-document -d /home/ftp-document user1
[root@ftp ~]# useradd -g ftp-document -d /home/ftp-document user2
[root@ftp ~]# useradd -g ftp-document -d /home/ftp-document user3
[root@ftp ~]# useradd -g ftp-document -d /home/ftp-document user4
```

Selanjutnya tambahkan password setiap user dengan massal seperti perintah berikut

```
[root@ftp ~]# passwd user1; passwd user2; passwd user3; passwd user4
```

Setelah anda menjalankan perintah passwd seperti diatas, maka anda akan diminta memasukkan 4 buat password masing-masing untuk setiap user yang sudah anda inputkan pada perintah passwd, selanjutnya buat sebuah folder dan atur hak aksesnya, kali ini penulis menentukan hak akses pada setiap group yaitu read only sehingga user yang sudah terdaftar pada group hanya bisa membaca direktori tersebut

```
[root@ftp ~]# mkdir /home/ftp-document/data
[root@ftp ~]# chown root:ftp-document /home/ftp-document/*
[root@ftp ~]# chmod 740 /home/ftp-document/*
[root@ftp ~]# [root@ftp ~]# passwd user4

[root@ftp ~]# vim /etc/vsftpd/vsftpd.conf
# Uncomment this to enable any form of FTP write command.
write_enable=NO

[root@ftp ~]# service vsftpd restart
Shutting down vsftpd: [ OK ]
Starting vsftpd for vsftpd: [ OK ]
```

Uji hasil konfigurasi tersebut dengan mengakses alamat ftp di web browser anda.

7.6. Sistem Keamanan Dengan OpenSSL

Secara Umum FTP dalam pengiriman dan pengambilan data atau biasanya disebut dengan upload download masih belum aman, sebab ketika seorang user memasukkan user dan password pada FTP maka akan dikirimkan dengan murni clear text sehingga hal tersebut menjadikan FTP tidak aman dalam penerapannya, tetapi hal tersebut bisa diatasi dengan sebuah integrasi OpenSSL sehingga ketika seorang user memasukkan username dan password maka, password tersebut akan dienkripsi terlebih dahulu sehingga tingkat keamanan data lebih terjamin. Berikut ini adalah langkah-langkah implementasi vsftpd dengan OpenSSL

Buatlah sebuah certificate yang digunakan sebagai awal integrasi vsftpd dengan SSL.

```
[root@ftp ~]# OpenSSL req -x509 -nodes -days 365 -newkey rsa:1024
-keyout /etc/vsftpd/vsftpd.pem -out /etc/vsftpd/vsftpd.pem
Generating a 1024 bit RSA private key
.....+++++
.....+++++
writing new private key to '/etc/vsftpd/vsftpd.pem'
-----
You are about to be asked to enter information that will be
incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a
DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [XX]:id
State or Province Name (full name) []:Jawa Timur
Locality Name (eg, city) [Default City]:Surabaya
Organization Name (eg, company) [Default Company Ltd]:mafatahna.web.id
Organizational Unit Name (eg, section) []:mafatahna
Common Name (eg, your name or your server's hostname)
[]:mafatahna.web.id
Email Address []:mafatahna@gmail.com
[root@ftp ~]# ls /etc/vsftpd/
chroot_list  ftpusers  user_list  vsftpd.conf  vsftpd_conf_migrate.sh
vsftpd.pem
```

Terlihat OpenSSL sudah selesai dibuat dengan nama vsftpd.pem. Selanjutnya gabungkan vsftpd dengan OpenSSL. Edit terlebih dahulu file vsftpd.conf dan tambahkan script berada paling bawah pada vsftpd.conf untuk integrasi OpenSSL

```
[root@ftp ~]# vim /etc/vsftpd/vsftpd.conf
# Mengaktifkan fitur SSL
ssl_enable=YES
# Mengizinkan user anonymous menggunakan SSL
allow_anon_ssl=YES
# Semua user non-anonymous login menggunakan SSL untuk
#pengiriman dan penerima data
```

```

force_local_data_ssl=YES
# Semua user non-anonymous login menggunakan SSL ketika terkoneksi dan
pengiriman password
force_local_logins_ssl=YES
# Pemberian ijin untuk TLS v1 dalam koneksi FTP Server
ssl_tlsv1=YES
ssl_sslv2=NO
ssl_sslv3=NO
# Lokasi dimana penulis membuat RSA certificate yang digunakan untuk
SSL encrypted
rsa_cert_file=/etc/vsftpd/vsftpd.pem

```

Simpan konfigurasi tersebut. Lanjutkan dengan restart layanan vsftpd dengan perintah

```

[root@ftp ~]# service vsftpd restart
Shutting down vsftpd:                [ OK ]
Starting vsftpd for vsftpd:          [ OK ]

```

7.7. Koneksi klien Menggunakan SSL

Pastikan bahwa integrasi OpenSSL sudah sukses, jika masih terdapat error ketika anda restart vsftpd maka periksa kembali konfigurasi yang sudah anda tetapkan. Koneksi vsftpd menggunakan OpenSSL sedikit berbeda dengan koneksi sebelumnya, kali ini penulis akan melakukan koneksi vsftpd dengan ftp klien pada Linux Ubuntu

```

mafatahna@mafatahna:~$ ftp 192.168.10.16
Connected to 192.168.10.16.
220 (vsFTPd 2.2.2)
Name (192.168.10.16:mafatahna): fatahna
530 Non-anonymous sessions must use encryption.
Login failed.
ftp>

```

Error!, ketika anda melakukan koneksi ke server FTP akan terdapat peringatan bahwa *non-anonymous sessions must use encryption* artinya user non-anonymous harus menggunakan encryption agar terkoneksi dengan vsftpd. Beberapa FTP Client Open Source saat ini ada beberapa yang sudah mempunyai fitur untuk encryption data sehingga anda bisa download aplikasi tersebut secara gratis. Silahkan anda mencari di internet.

Pada uji coba kali ini penulis akan menggunakan Linux Ubuntu dengan aplikasi ftp-ssl yang nantinya akan saya pergunakan untuk koneksi FTP Client. Software yang lain seperti WSFTPD, FileZilla dll tidak penulis bahas dalam buku ini sebab caranya kurang lebih tidak berbeda dengan ftp-ssl Ubuntu.

Install terlebih dahulu ftp-ssl di Linux Ubuntu dengan perintah

```

mafatahna@mafatahna:~$ sudo apt-get install ftp-ssl
[sudo] password for mafatahna:
Reading package lists... Done
Building dependency tree

```

```
Reading state information... Done
The following extra packages will be installed:
  libeditline0
The following packages will be REMOVED:
  ftp
The following NEW packages will be installed:
  ftp-ssl libeditline0
0 upgraded, 2 newly installed, 1 to remove and 0 not upgraded.
Need to get 70.7 kB of archives.
After this operation, 86.0 kB of additional disk space will be used.
Do you want to continue [Y/n]? y
```

Setelah instalasi selesai, langkah selanjutnya adalah login FTP menggunakan aplikasi ftp-ssl mode text

```
mafatahna@mafatahna:~$ ftp-ssl 192.168.10.16
Connected to 192.168.10.16.
220 (vsFTPd 2.2.2)
Name (192.168.10.16:mafatahna): fatahna
234 Proceed with negotiation.
[SSL Cipher DES-CBC3-SHA]
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp>
```

Jika proses login ke FTP Server menggunakan SSL berhasil, berarti fitur SSL sudah berjalan dengan baik di Server anda. Silahkan melakukan uji coba sendiri dengan aplikasi yang lain.

Web Server

Web Server merupakan software penting didalam dunia teknologi informasi, dengan adanya software ini maka semakin memudahkan pengguna dalam memberikan berbagai macam informasi dalam bentuk website, forum dan blog. Selain itu Web Server juga bisa gunakan dalam teknologi pertukaran data dalam bentuk video dan foto. Linux CentOS merupakan salah satu Distro Linux terbesar yang paling banyak digunakan untuk membangun Web Server, kemampuan dan sistem keamanan yang handal adalah nilai tambah bagi Linux CentOS. Dalam hal ini penulis akan mencoba mengupas tuntas mengenai pembuatan sebuah Web Server yaitu dengan menggabungkan beberapa paket seperti Apache, PHP, MySQL, OpenSSL dll. Beberapa paket yang sudah penulis sebutkan merupakan salah satu dari sekian paket yang akan kita implementasi dalam Project Web Server.

8.1. Instalasi Web Server

Web Server secara umum sudah tersedia di dalam repository Linux CentOS sehingga dalam implementasinya bisa menggunakan perintah yum install seperti di bawah ini

```
[root@srv2 ~]# yum install httpd
```

Setelah instalasi selesai maka langkah selanjutnya adalah konfigurasi httpd. Dalam konfigurasi httpd ada beberapa parameter yang perlu dirubah dan ditambahkan agar Web Server berjalan dengan baik diantaranya yaitu

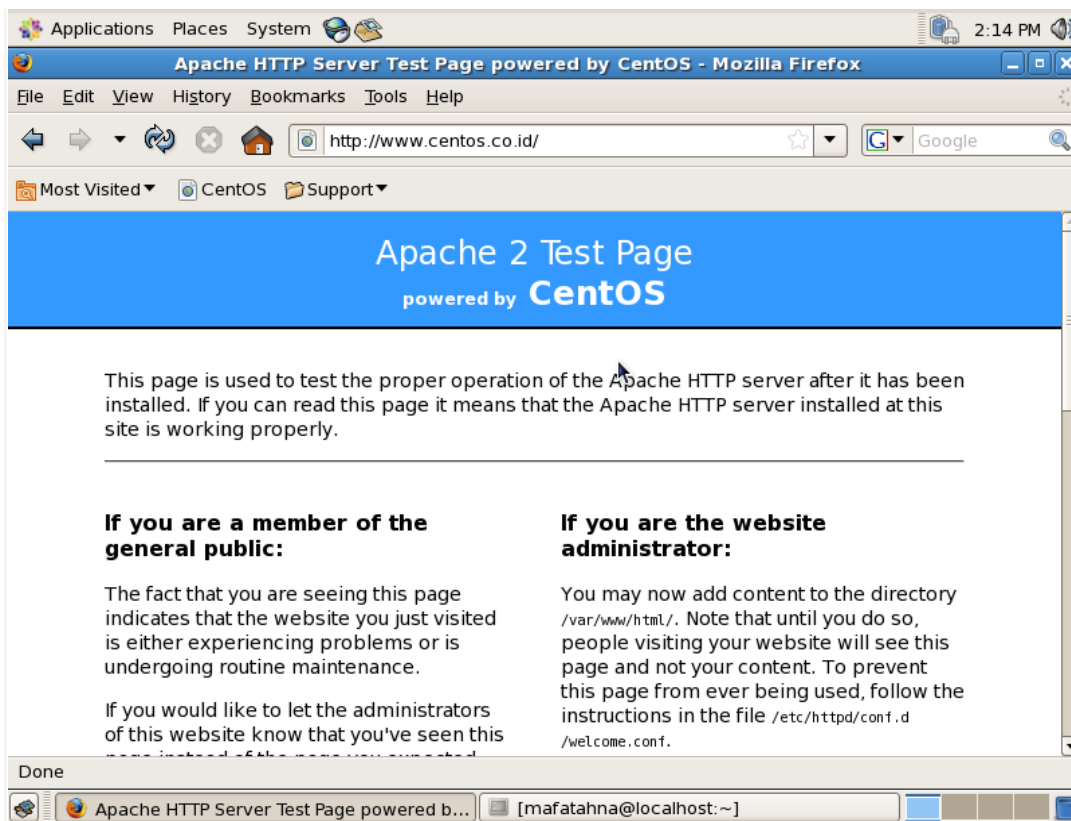
```
[root@srv2 ~]# vim /etc/httpd/conf/httpd.conf
ServerTokens Prod # baris 44, ganti menjadi Prod
KeepAlive On # baris 74, ganti menjadi ON
ServerAdmin root@server-centos.org # baris 251, alamat serber admin
ServerName www.server-centos.org:80 # baris 265, isi dengan nama domain
Options FollowSymLinks ExecCGI # baris 320, mengaktifkan CGI
AllowOverride All # baris 327
DirectoryIndex index.html index.cgi index.php # baris 391
ServerSignature Off # baris 524, signature ketika user
# salah link Site
# AddDefaultCharset UTF-8 # baris 747, non-aktifkan
AddHandler cgi-script .cgi .pl # baris 778
```

Setelah menambahkan dan merubah beberapa parameter yang terdapat pada httpd.conf, konfigurasi sederhana membuat Web Server sudah selesai. Aktifkan layanan Web Server dengan perintah

```
[root@srv2 ~]# service httpd start
Starting httpd: [ OK ]
[root@srv2 ~]# chkconfig httpd on
```

Ada beberapa parameter yang perlu dilakukan setelah instalasi httpd seperti beberapa paket yang dibutuhkan untuk Database (MySQL), PHP, Perl dan lain sebagainya.

Sebelum melangkah ke tahap berikutnya lakukan uji coba dengan mengakses domain yang sudah terdaftar di DNS Server melalui web browser. Di buku ini domain yang digunakan adalah <http://www.centos.co.id>



Pada gambar diatas menunjukkan bahwa apache 2 sudah berhasil berjalan di sistem anda. Selanjutnya adalah menghapus halaman selamat datang tersebut. Sehingga secara default halaman tersebut di ganti dengan website yang sudah administrator sediakan. Hapus welcome.conf dan noindex.html

```
[root@srv2 ~]# rm -f /etc/httpd/conf.d/welcome.conf
[root@srv2 ~]# rm -f /var/www/error/noindex.html
```

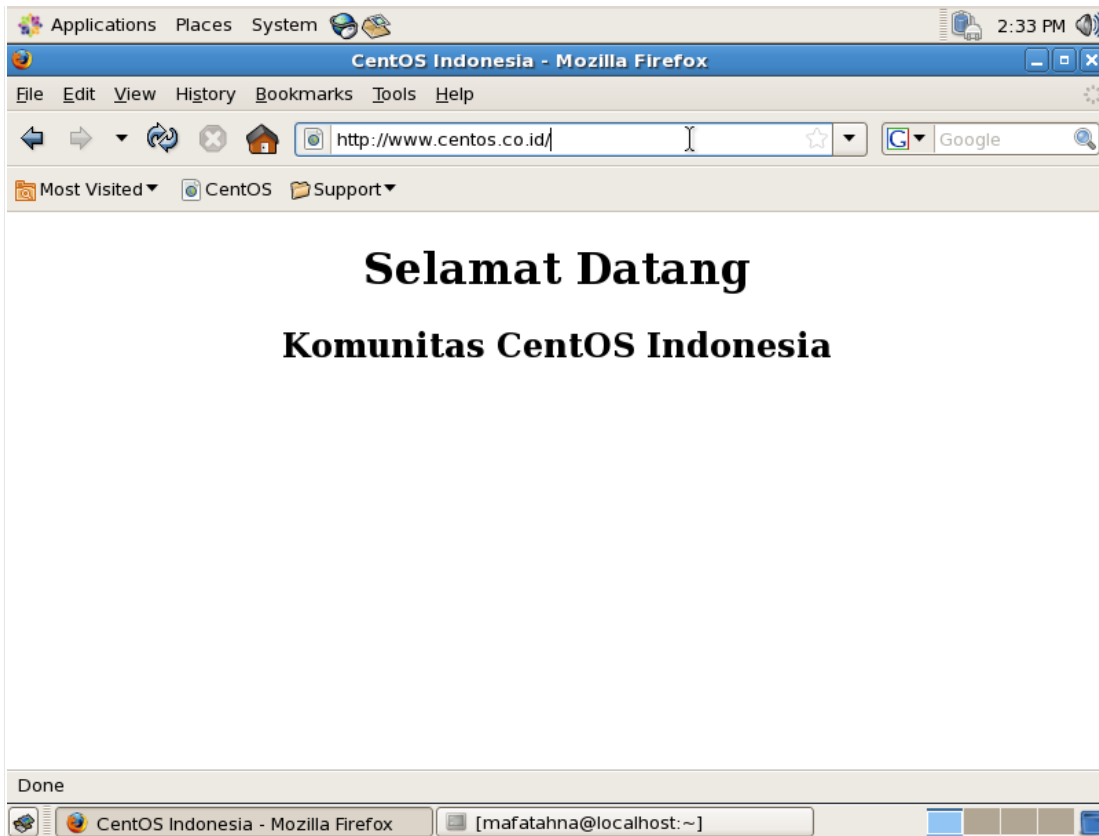
Setelah beberapa file yang tidak dibutuhkan dihapus, buat link agar bahasa perl dikenali server

```
[root@srv2 ~]# ln -s /usr/bin/perl /usr/local/bin/perl
```

Selanjutnya adalah mengedit file index yang terdapat pada default lokasi Web Server, anda dapat memasukkan script html sesuai dengan selera anda, berikut ini contoh script html

```
[root@srv2 ~]# vim /var/www/html/index.html
<html>
<head>
<title>CentOS Indonesia</title>
</head>
<body>
<div style="text-align: center;">
<h1>Selamat Datang</h1>
<h2>Komunitas CentOS Indonesia</h2>
</div>
</body>
</html>
```

Simpan dan keluar dari editor dengan menekann tombol Esc dan ketikkan :wq tekan enter. Jalankan web browser yang sudah terinstall pada PC / Laptop anda. Sebagai bukti bahwa script html tersebut berjalan dengan baik.



Setelah anda menjalankan di browser, maka akan tampil sebuah halaman yang sudah anda edit dengan penambahan html, tetapi jika pada PC / Latop anda masih belum terdapat halaman tersebut maka coba lakukan pengecekan kembali sebab besar kemungkinan konfigurasi yang anda lakukan masih belum benar.

8.2. Multiple Domain

Merupakan salah satu fitur yang dimiliki Web Server yang dipergunakan untuk membuat lebih dari satu domain dalam sebuah server, hal tersebut akan sangat bermanfaat jika anda mempunyai beberapa domain tetapi hanya memiliki sebuah server saja. Misalnya anda memiliki dua domain yaitu centos.co.id dan centos.org, kedua domain tersebut akan diletakkan di sebuah server. Pastikan anda sudah mempelajari bagaimana cara membuat multidomain dalam satu DNS Server, jika anda sudah bisa konfigurasi tersebut anda bisa melanjutkan langkah membuat multidomain di Apache. Test terlebih dahulu apakah domain yang anda miliki sudah berjalan dengan baik.

```
[root@srv2 ~]# nslookup centos.org
Server:          129.93.88.12
Address:        129.93.88.12#53
```

```
Name: centos.org
Address: 129.93.88.12
```

Setelah konfigurasi DNS domain centos.org berjalan dengan baik maka anda bisa melanjutkan

konfigurasi Web Server dengan menambahkan script pada httpd.conf

```
[root@srv2 mafatahna]# vim /etc/httpd/conf/httpd.conf
NameVirtualHost *:80
<VirtualHost *:80>
  ServerAdmin root@centos.co.id
  DocumentRoot "/var/www/html"
  ServerName centos.co.id
  ServerAlias www.centos.co.id
</VirtualHost>

<VirtualHost *:80>
  ServerAdmin root@centos.org
  DocumentRoot "/home/website/centos.org"
  ServerName centos.org.org
  ServerAlias www.centos.org
</VirtualHost>
```

Script yang ditambahkan tersebut digunakan untuk membuat virtualhost pada apache, sehingga bisa diarahkan ke folder lokasi website berada. Domain centos.org diatas belum memiliki direktori sebagai lokasi website, sehingga buatlah terlebih dahulu direktorinya dengan perintah

```
[root@srv2 ~]# mkdir -p /home/website/centos.org
```

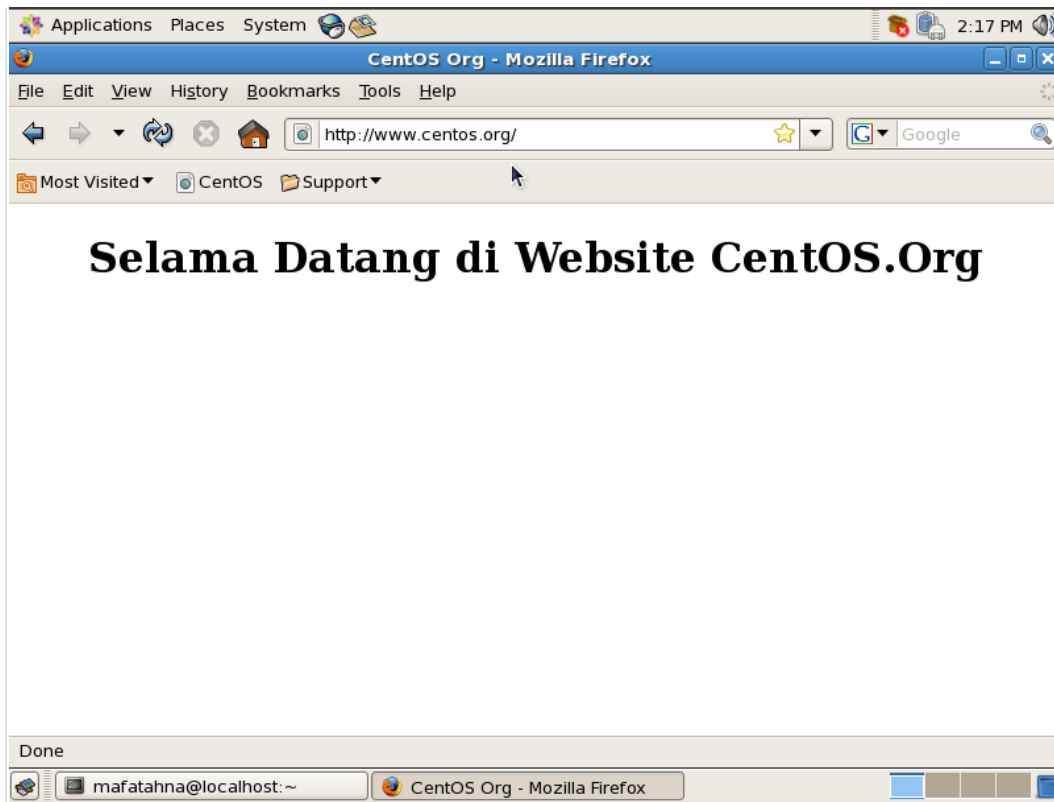
Selanjutnya buatlah file index.html kedalam direktori tersebut

```
[root@srv2 ~]# cd /home/website/centos.org/
[root@srv2 centos.org]# vim index.html
<html>
<head>
<title>CentOS Org</title>
</head>
<body>
<div style="text-align: center;">
<h1>Selama Datang di Website CentOS.Org</h1>
</div>
</body>
</html>
```

Setelah pembuatan file index.html selesai, restart httpd dan pastikan tidak ada error pada proses ini

```
[root@srv2 centos.org]# service httpd restart
Stopping httpd:          [ OK ]
Starting httpd:         [ OK ]
[root@srv2 centos.org]#
```

Jika anda sudah selesai restart apache dengan catatan tidak ada error dalam proses tersebut, maka langkah selanjutnya anda bisa melakukan pengecekan pada web browser dengan mengakses alamat www.centos.org



Anda juga bisa menambahkan beberapa domain lagi di Web Server tersebut dan untuk jumlahnya tidak terbatas, konfigurasi sama dengan sebelumnya yaitu menambahkan domain yang terdapat pada DNS Server dan membuat home page pada Web Server.

8.3. Redirect Domain

Domain yang anda miliki bisa juga dilakukan redirect ketujuan alamat tertentu misalnya jika klien mengakses alamat centos.co.id maka secara otomatis di redirect ke alamat www.centos.co.id, hal tersebut bisa juga ditujukan ke tujuan alamat domain yang lain sesuai keinginan,

Redirect Menggunakan Script

Sebuah website bisa kita lakukan redirect menggunakan script yaitu menggunakan sedikit trik dari pemrograman java script, script ini diletakkan pada file index misalnya pengguna mempunyai domain centos.co.id dan jika terdapat user yang mengakses alamat tersebut maka secara otomatis akan di redirect ke www.centos.co.id, maka buatlah file index.html selanjutnya tambahkan script dibawah ini

```
<META HTTP-EQUIV="REFRESH"  
CONTENT="0; URL='http://www.centos.co.id' ">
```

Simpan konfigurasi tersebut.

Redirect Menggunakan Web Server

Selain menggunakan script Web Server juga bisa digunakan untuk redirect sebuah domain, dalam hal ini penulis mencoba redirect dengan studi khusus sama dengan sebelumnya yaitu dari domain centos.co.id ke domain www.centos.co.id, silahkan edit file httpd.conf yang terdapat di Web Server dan tambahkan beberapa script seperti dibawah ini

```
[root@srv2 ~]# vim /etc/httpd/conf/httpd.conf
NameVirtualHost *:80
```

```
<VirtualHost *:80>
  ServerName centos.co.id
  Redirect permanent / http://www.centos.co.id/
</VirtualHost>
```

```
<VirtualHost *:80>
  ServerAdmin root@centos.co.id
  DocumentRoot "/var/www/html"
  ServerName centos.co.id
  ServerAlias www.centos.co.id
</VirtualHost>
```

```
<VirtualHost *:80>
  ServerAdmin root@centos.org
  DocumentRoot "/home/website/centos.org"
  ServerName centos.org.org
  ServerAlias www.centos.org
</VirtualHost>
```

Tambahkan script sesuai dengan text yang tercetak tebal diatas. Simpan dan keluar dari editor lanjutkan dengan restart apache.

8.4. Autentikasi Web Server

Privasi sebuah halaman website dengan segudang informasi berharga yang diharapkan hanya beberapa orang tertentu saja yang bisa mengakses halaman website tersebut, maka dengan apache anda bisa menggunakan sistem autentikasi password dengan default fitur htpasswd yang dimiliki apache.

Misalnya anda mempunyai direktori yang terletak di webserver, maka dalam hal ini kami memberikan nama yaitu direktori private. Buatlah direktori tersebut didalam domain yang anda inginkan, contoh domain centos.co.id. Langkah-langkah dalam membuat autentikasi password tersebut sebagai berikut

```
[root@srv2 ~]# mkdir /var/www/html/private
[root@srv2 ~]# vim /var/www/html/private/index.html
<html>
<head>
<title>Private</title>
</head>
<body>
<div style="text-align: center;">
<h1>Halaman Rahasia</h1>
</div>
</body>
</html>
```

```
[root@srv2 ~]# htpasswd -c /etc/httpd/htpasswd anggota1
New password:
Re-type new password:
Adding password for user anggota1
[root@srv2 ~]#
```

Setelah password dan direktori selesai dibuat maka langkah selanjutnya adalah menambahkan script terhadap file httpd.conf, untuk memudahkan penulis cetak **tebal** script yang ditambah

```
[root@srv2 ~]# vim /etc/httpd/conf/httpd.conf
NameVirtualHost *:80
<VirtualHost *:80>
  ServerName centos.co.id
  Redirect permanent / http://www.centos.co.id/
</VirtualHost>

<VirtualHost *:80>
  ServerAdmin root@centos.co.id
  DocumentRoot "/var/www/html"
  ServerName centos.co.id
  ServerAlias www.centos.co.id
</VirtualHost>

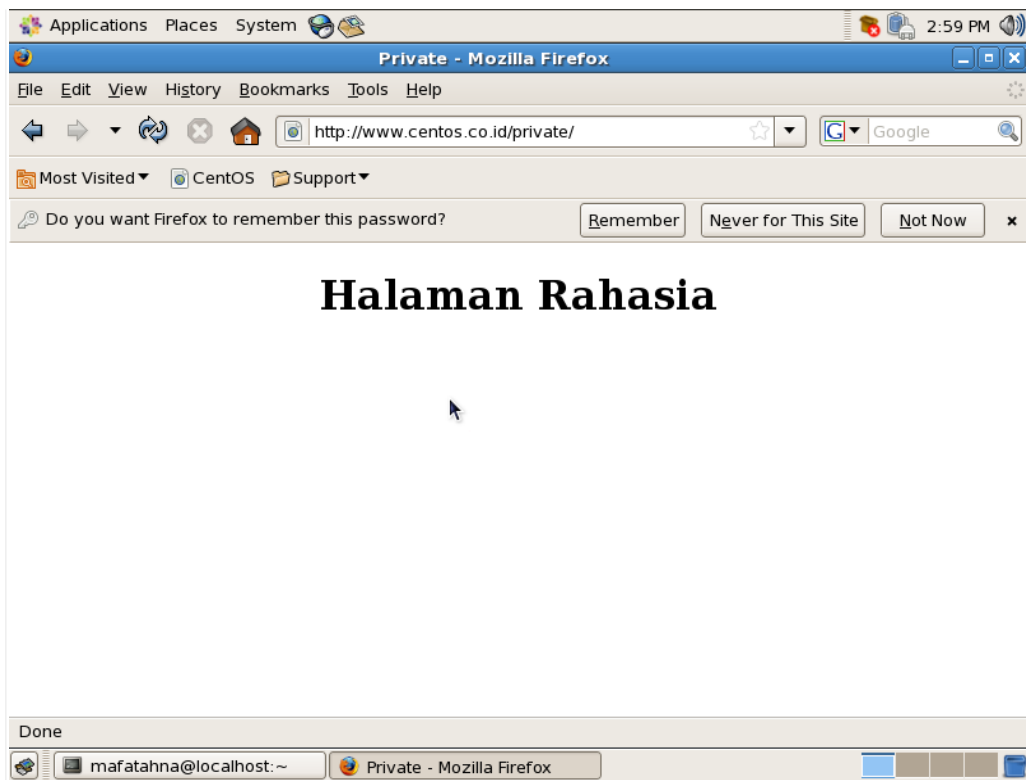
<VirtualHost *:80>
  ServerAdmin root@centos.org
  DocumentRoot "/home/website/centos.org"
  ServerName centos.org.org
  ServerAlias www.centos.org
</VirtualHost>

<Directory "/var/www/html/private/">
  AuthType Basic
  AuthName "Member Access"
  AuthBasicProvider file
  AuthUserFile /etc/httpd/htpasswd
  Require user anggota1
</Directory>
```

Selanjutnya lakukan uji coba dengan masuk ke lokasi folder tersebut yaitu dengan mengaksesnya menggunakan web browser alamat www.centos.co.id/private.



Pada gambar diatas terlihat hasil autentikasi user apache, masukkan user dan password yang sudah anda buat, jika berhasil maka anda bisa memasuki halaman tersebut. Seperti gambar dibawah ini



8.5. Meningkatkan Keamanan Dengan SSL

Sistem keamanan dalam sebuah website memang penting untuk pertimbangan, sama halnya dengan penerapan OpenSSL untuk FTP Server yang terdapat pada bab sebelumnya. Web Server juga bisa diintegrasikan dengan layanan SSL sehingga standart protokol yang digunakan sebelumnya http maka dengan menambahkan fitur SSL protokol yang digunakan adalah https. Dengan menggunakan fitur https maka segala aktifitas yang melibatkan akses halaman website akan dienkripsi, sehingga lebih mengamankan aktifitas browsing ke halaman website tersebut.

Instalasi OpenSSL

Langkah-langkah dalam menambahkan fitur SSL di Web Server adalah membuat terlebih dahulu SSL, sesuai dengan perintah dibawah ini

```
[root@srv2 ~]# cd /etc/pki/tls/certs
[root@srv2 certs]# make centos.key
umask 77 ; \
    /usr/bin/openssl genrsa -des3 1024 > centos.key
Generating RSA private key, 1024 bit long modulus
.....+++++
..+++++
e is 65537 (0x10001)
Enter pass phrase:
Verifying - Enter pass phrase:
[root@srv2 certs]#
```

Ingat, jangan lupa dengan password yang anda pergunakan sebab password tersebut akan digunakan pada tahap selanjutnya

```
[root@srv2 certs]# make centos.csr
umask 77 ; \
    /usr/bin/openssl req -utf8 -new -key centos.key -out centos.csr
Enter pass phrase for centos.key:
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [GB]:ID
State or Province Name (full name) [Berkshire]:mafatahna
Locality Name (eg, city) [Newbury]:Surabaya
Organization Name (eg, company) [My Company Ltd]:CentOS-Indonesia
Organizational Unit Name (eg, section) []:Network Administator
Common Name (eg, your name or your server's hostname) []:centos.co.id
Email Address []:admin@centos.co.id

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:1290
An optional company name []:mafatahna
[root@srv2 certs]#
```

Text yang tercetak tebal harus anda isi secara manual sesuai dengan data valid perusahaan, selanjutnya lanjutkan dengan membuat certificate dengan perintah beriku ini

```
[root@srv2 certs]# openssl x509 -in centos.csr -out centos.crt -req -signkey centos.key -days 3650
Signature ok
subject=/C=ID/ST=mafatahna/L=Surabaya/O=CentOS-Indonesia/OU=Network Administrator/CN=centos.co.id/emailAddress=admin@centos.co.id
Getting Private key
Enter pass phrase for centos.key:
[root@srv2 certs]#
```

Tambahkan permission pada certificate tersebut, dengan hak akses root (write)

```
[root@srv2 certs]# chmod 400 centos.*
[root@srv2 certs]# ls -la
total 492
drwxr-xr-x 2 root root 4096 May 28 15:18 .
drwxr-xr-x 5 root root 4096 May 18 17:22 ..
-rw-r--r-- 1 root root 441017 Mar 27 2010 ca-bundle.crt
-r----- 1 root root 1025 May 28 15:18 centos.crt
-r----- 1 root root 802 May 28 15:14 centos.csr
-r----- 1 root root 963 May 28 15:12 centos.key
-rw----- 1 root root 1468 May 18 17:23 localhost.crt
-rwxr-xr-x 1 root root 610 Mar 27 2010 make-dummy-cert
-rw-r--r-- 1 root root 2240 Mar 27 2010 Makefile
[root@srv2 certs]#
```

Setelah proses pembuatan SSL selesai, langkah selanjutnya adalah integrasikan SSL ke Web Server yaitu dengan install terlebih dahulu paket mod ssl dengan perintah dibawah ini

```
[root@srv2 certs]# yum install mod_ssl -y
[root@srv2 certs]# vim /etc/httpd/conf.d/ssl.conf
DocumentRoot "/var/www/html" # baris 84, Lokasi path default web server
ServerName www.server.world:443 # baris 85, Hilangkan tanda komentar
SSLCertificateFile /etc/pki/tls/certs/server.crt # baris 112, lokasi certificate
SSLCertificateKeyFile /etc/pki/tls/certs/server.key # baris 119, lokasi certificate
```

Selanjutnya restart layanan apache, dalam proses restart anda akan di minta password SSL maka masukkan password tersebut dan tekan enter.

```
[root@srv2 certs]# service httpd restart
Stopping httpd: [ OK ]
Starting httpd: Apache/2.2.3 mod_ssl/2.2.3 (Pass Phrase Dialog)
Some of your private key files are encrypted for security reasons.
In order to read them you have to provide the pass phrases.

Server www.centos.co.id:443 (RSA)
Enter pass phrase:

OK: Pass Phrase Dialog successful. [ OK ]

[root@srv2 certs]#
```

Setelah proses restart tidak ada kesalahan (error) anda bisa melakukan pengecekan dengan menggunakan web browser dengan mengakses alamat <https://www.centos.co.id>, ketika anda membuka alamat

tersebut seharusnya muncul peringatan *“This Connection is Untrusted”* jika hal tersebut terjadi kepada anda berarti proses penggabungan Web Server dan OpenSSL sudah berjalan dengan baik, lanjutkan dengan beberapa petunjuk di web browser tersebut hingga anda bisa masuk di mode https seperti gambar dibawah ini



8.6. OpenSSL dengan Multidomain

SSL yang sudah anda integrasikan pada Web Server bisa juga anda terapkan dengan domain yang berbeda sehingga jika anda memiliki beberapa domain maka anda hanya perlu memiliki 1 certificate, langkah-langkah yang harus dilakukan untuk konfigurasi OpenSSL dengan multidomain yaitu menambahkan VirtualHost pada baris paling bawah dalam file `ssl.conf`, untuk lebih jelasnya penulis tampilkan seluruh konfigurasi dengan memberikan teks tebal pada script yang ditambahkan

```
[root@srv2 ~]# nano /etc/httpd/conf.d/ssl.conf
LoadModule ssl_module modules/mod_ssl.so
Listen 443
AddType application/x-x509-ca-cert .crt
AddType application/x-pkcs7-crl .crl
SSLPassPhraseDialog builtin
SSLSessionCache shmcb:/var/cache/mod_ssl/scache(512000)
SSLSessionCacheTimeout 300
SSLMutex default
SSLRandomSeed startup file:/dev/urandom 256
SSLRandomSeed connect builtin
#SSLRandomSeed startup file:/dev/random 512
#SSLRandomSeed connect file:/dev/random 512
#SSLRandomSeed connect file:/dev/urandom 512
```

```

<VirtualHost centos.co.id:443>
DocumentRoot "/var/www/html"
ServerName centos.co.id:443
ErrorLog logs/ssl_error_log
TransferLog logs/ssl_access_log
LogLevel warn
SSLEngine on
SSLProtocol all -SSLv2
SSLCipherSuite ALL:!ADH:!EXPORT:!SSLv2:RC4+RSA:+HIGH:+MEDIUM:+LOW
SSLCertificateFile /etc/pki/tls/certs/centos.crt
SSLCertificateKeyFile /etc/pki/tls/certs/centos.key
#SSLCertificateChainFile /etc/pki/tls/certs/centos.crt
#SSLCACertificateFile /etc/pki/tls/certs/ca-bundle.crt
<Files ~ "\.(cgi|shtml|phtml|php3?)$" >
    SSLOptions +StdEnvVars
</Files>
<Directory "/var/www/cgi-bin">
    SSLOptions +StdEnvVars
</Directory>
SetEnvIf User-Agent ".*MSIE.*" \
    nokeepalive ssl-unclean-shutdown \
    downgrade-1.0 force-response-1.0
CustomLog logs/ssl_request_log \
    "%t %h %{SSL_PROTOCOL}x %{SSL_CIPHER}x \"%r\" %b"
</VirtualHost>
<VirtualHost centos.org:443>
DocumentRoot "/home/website/centos.org"
ServerName centos.org:443
ErrorLog logs/ssl_error_log
TransferLog logs/ssl_access_log
LogLevel warn
SSLEngine on
SSLProtocol all -SSLv2
SSLCipherSuite ALL:!ADH:!EXPORT:!SSLv2:RC4+RSA:+HIGH:+MEDIUM:+LOW
SSLCertificateFile /etc/pki/tls/certs/centos.crt
SSLCertificateKeyFile /etc/pki/tls/certs/centos.key
#SSLCertificateChainFile /etc/pki/tls/certs/centos.crt
#SSLCACertificateFile /etc/pki/tls/certs/ca-bundle.crt
<Files ~ "\.(cgi|shtml|phtml|php3?)$" >
    SSLOptions +StdEnvVars
</Files>
<Directory "/var/www/cgi-bin">
    SSLOptions +StdEnvVars
</Directory>
SetEnvIf User-Agent ".*MSIE.*" \
    nokeepalive ssl-unclean-shutdown \
    downgrade-1.0 force-response-1.0
CustomLog logs/ssl_request_log \
    "%t %h %{SSL_PROTOCOL}x %{SSL_CIPHER}x \"%r\" %b"
</VirtualHost>

```

Setelah anda menambahkan script pada file ssl.conf langkah selanjutnya adalah restart apache dengan perintah

```
[root@srv2 certs]# service httpd restart
Stopping httpd: [ OK ]
Starting httpd: [Mon May 28 16:10:42 2012] [warn] VirtualHost
centos.co.id:443 overlaps with VirtualHost centos.org:443, the first has
precedence, perhaps you need a NameVirtualHost directive
Apache/2.2.3 mod_ssl/2.2.3 (Pass Phrase Dialog)
Some of your private key files are encrypted for security reasons.
In order to read them you have to provide the pass phrases.

Server centos.org:443 (RSA)
Enter pass phrase:

OK: Pass Phrase Dialog successful.
```

Selanjutnya ketika anda restart httpd pastikan terdapat informasi bahwa Web Server **OK** seperti diatas, jika terdapat informasi “*the first has precedence, perhaps you need a NameVirtualHost directive*” keterangan tersebut menginformasikan bahwa konfigurasi tersebut belum memiliki NameVirtualHost sehingga untuk menambahkan NameVirtualHost anda bisa melakukan penambahan script pada file ssl.conf.

```
[root@srv2 ~]# nano /etc/httpd/conf.d/ssl.conf
NameVirtualHost 129.93.88.12:443
```

IP Address 129.93.88.12 adalah IP Public Web Server anda, sekarang restart lagi

```
[root@srv2 certs]# service httpd restart
Stopping httpd: [ OK ]
Starting httpd: Apache/2.2.3 mod_ssl/2.2.3 (Pass Phrase Dialog)
Some of your private key files are encrypted for security reasons.
In order to read them you have to provide the pass phrases.

Server centos.org:443 (RSA)
Enter pass phrase:

OK: Pass Phrase Dialog successful.

[ OK ]
```

Setelah anda restart service httpd dan tidak terdapat error apapun, maka anda bisa melakukan uji coba dengan menggunakan web browser yaitu dengan akses alamat <https://centos.org>



Kekurangan dari SSL adalah ketika anda mengaktifkan layanan ini dengan merestart httpd diharuskan untuk memasukkan password RSA yang sudah terbuat, sehingga hal tersebut akan mengakibatkan memasukkan password terlebih dahulu ketika booting. Solusinya, anda bisa mematikan layanan httpd dan mengaktifkan kembali ketika proses booting sudah selesai.

8.7. Installasi Mysql-server dan PHP

Server database terutama dalam Sebuah Web Server sangatlah penting, betapa tidak jika anda memiliki sebuah website dan pada website tersebut hanya bisa menampilkan beberapa site static yang anda buat maka hal tersebut tidak akan maksimal sehingga dengan adanya database pada website tersebut akan memiliki kemampuan untuk menyimpan beberapa data yang kita inginkan.

```
[root@srv2 ~]# mysql mysql-server php-pear ruby gettext perl php php-mysql  
php-xml php-imap php-mbstring php-pecl-Fileinfo php-pecl-memcache perl-Net-  
SSLeay php-devel gcc gd php-gd
```

Transaction Summary

```
=====  
Install      24 Package(s)  
Upgrade     11 Package(s)
```

```
Total download size: 74 M  
Is this ok [y/N]:
```

Dalam proses installasi MySQL Server dibutuhkan koneksi internet sehingga ketika anda menjalankan perintah diatas perlu beberapa menit untuk melakukan download paket terlebih dahulu sebelum installasi, perkiraan keseluruhan paket tersebut memiliki kapasitas sebesar 70 MB.

Jika proses instalasi sudah selesai, maka jalankan terlebih dahulu layanan mysql dengan perintah dibawah ini

```
[root@srv2 ~]# service mysqld start
Initializing MySQL database: Installing MySQL system tables...
OK
Filling help tables...
OK
```

To start mysqld at boot time you have to copy support-files/mysql.server to the right place for your system

```
PLEASE REMEMBER TO SET A PASSWORD FOR THE MySQL root USER !
To do so, start the server, then issue the following commands:
/usr/bin/mysqladmin -u root password 'new-password'
/usr/bin/mysqladmin -u root -h srv2.centos.co.id password 'new-password'
```

Alternatively you can run:
/usr/bin/mysql_secure_installation

which will also give you the option of removing the test databases and anonymous user created by default. This is strongly recommended for production servers.

See the manual for more instructions.

You can start the MySQL daemon with:
cd /usr ; /usr/bin/mysqld_safe &

You can test the MySQL daemon with mysql-test-run.pl
cd mysql-test ; perl mysql-test-run.pl

Please report any problems with the /usr/bin/mysqlbug script!

The latest information about MySQL is available on the web at
<http://www.mysql.com>
Support MySQL by buying support/licenses at <http://shop.mysql.com>

```
Starting MySQL: [ OK ]
[root@srv2 ~]# [ OK ]
```

Setelah menjalankan mysql coba anda perhatikan informasi yang dihasilkan dengan perintah tersebut, hal tersebut memberikan informasi kepada pengguna untuk mengamankan server mysql yang sudah terinstall dengan sebuah password, untuk memberika password di mysql anda bisa menjalankan perintah dibawah ini

```
[root@srv2 ~]# mysql -u root
Welcome to the MySQL monitor. Commands end with ; or \g.
Your MySQL connection id is 2
Server version: 5.0.95 Source distribution
```

Copyright (c) 2000, 2011, Oracle and/or its affiliates. All rights reserved.

Oracle is a registered trademark of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

```
mysql> select user,host,password from mysql.user;
```

```
+-----+-----+-----+
| user | host           | password |
+-----+-----+-----+
| root | localhost      |          |
| root | srv2.centos.co.id |          |
| root | 127.0.0.1      |          |
|      | localhost      |          |
|      | srv2.centos.co.id |          |
+-----+-----+-----+
5 rows in set (0.00 sec)
```

```
mysql> set password for root@localhost=password ('password');
Query OK, 0 rows affected (0.01 sec)
```

```
mysql> set password for root@'127.0.0.1'=password ('password');
Query OK, 0 rows affected (0.01 sec)
```

```
mysql> set password for root@'srv2.centos.co.id'=password ('password');
Query OK, 0 rows affected (0.01 sec)
```

```
mysql> select user,host,password from mysql.user;
```

```
+-----+-----+-----+
| user | host           | password          |
+-----+-----+-----+
| root | localhost      | 5d2e19393cc5ef67 |
| root | srv2.centos.co.id | 5d2e19393cc5ef67 |
| root | 127.0.0.1      | 5d2e19393cc5ef67 |
|      | localhost      |                   |
|      | srv2.centos.co.id |                   |
+-----+-----+-----+
5 rows in set (0.00 sec)
```

```
mysql>
```

Setelah anda menambahkan password di mysql lanjutkan dengan melakukan uji coba seperti pada perintah dibawah ini

```
[root@srv2 ~]# mysql -u root -p
Enter password:
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 3
Server version: 5.0.95 Source distribution
```

Copyright (c) 2000, 2011, Oracle and/or its affiliates. All rights reserved.

Oracle is a registered trademark of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

```
mysql>
```

Konfigurasi terakhir pada Mysql-server yaitu mengaktifkan service tersebut ketika awal booting

```
[root@srv2 ~]# chkconfig mysqld on
```

8.8. Instalasi phpMyAdmin

Secara default phpMyAdmin sudah tersedia direpositori CentOS, tetapi tidak ada kepastian bahwa versi yang terdapat pada repository tersebut menggunakan versi terbaru, sehingga jika anda ingin menggunakan versi terbaru dari phpMyAdmin anda bisa mendownload terlebih dahulu disitus resminya yaitu

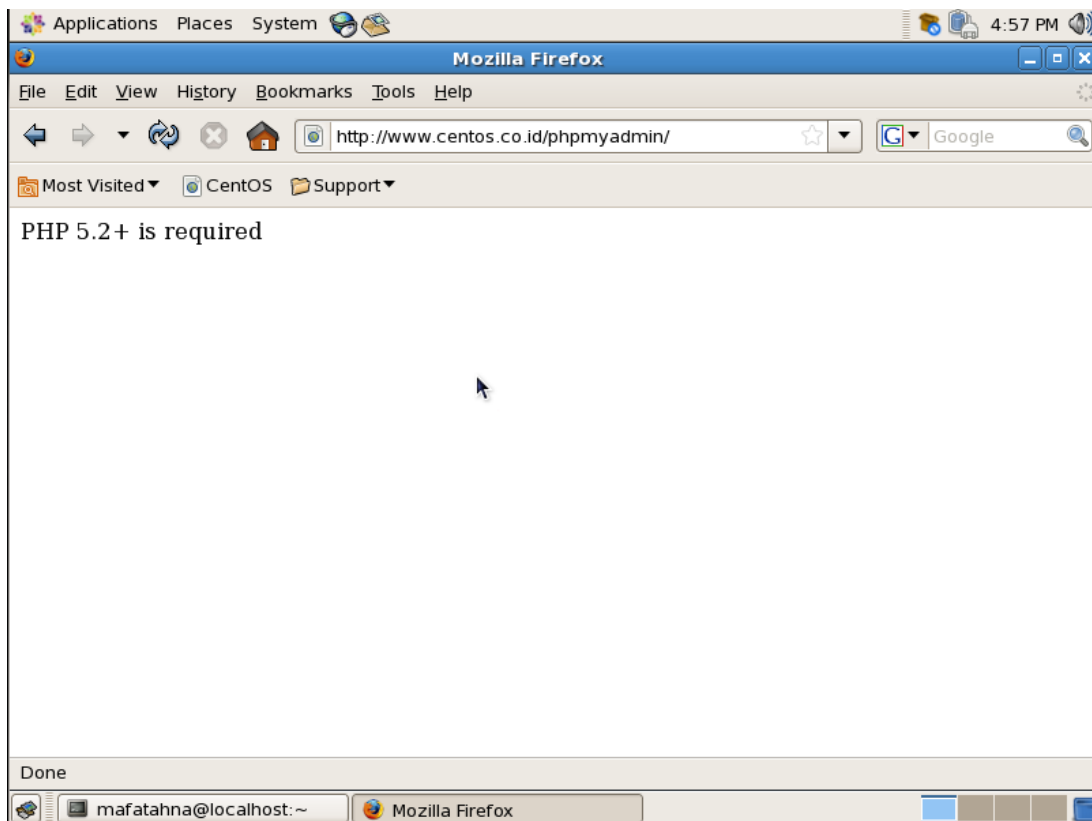
http://www.phpmyadmin.net/home_page/downloads.php

Saat buku ini ditulis versi terbarunya adalah phpMyAdmin-3.5, Jika anda mendownload secara manual disitus resminya anda bisa menggunakan versi terbaru dari phpMyAdmin. Langkah-langkah untuk instalasi phpMyAdmin adalah sebagai berikut

copy file phpMyAdmin yang sudah anda download ke folder /var/www/html, atau anda bisa langsung mendownloadnya dengan perintah wget pada server anda.

```
[root@srv2 ~]# cd /var/www/html/
[root@srv2 html]# ls
index.html  phpMyAdmin-3.5.1-english.tar.gz
[root@srv2 html]# tar zxvf phpMyAdmin-3.5.1-english.tar.gz
[root@srv2 html]# ls
phpMyAdmin-3.5.1-english  phpMyAdmin-3.5.1-english.tar.gz  index.html
[root@srv2 html]# mv phpMyAdmin-3.5.1-english phpmyadmin
```

jika file tersebut sudah anda extract dan direname sesuai dengan perintah diatas maka langkah selanjutnya adalah akses alamat <http://centos.co.id/phpmyadmin> menggunakan web browser seperti pada gambar dibawah ini



Terdapat peringatan “PHP 5.2 + is required” hal tersebut disebabkan CentOS 5.5 masih menggunakan PHP 5.1. Bagaimana cara mengetahui versi PHP yang digunakan saat ini, anda bisa menjalankan perintah dibawah ini

```
[root@srv2 ~]# php -version
PHP 5.1.6 (cli) (built: May 7 2012 15:02:52)
Copyright (c) 1997-2006 The PHP Group
Zend Engine v2.1.0, Copyright (c) 1998-2006 Zend Technologies
[root@srv2 ~]#
```

Langkah selanjutnya adalah update versi PHP menggunakan repo.webtatic.com, silahkan jalankan perintah dibawah ini

```
[root@srv2 ~]# rpm -Uvh http://repo.webtatic.com/yum/centos/5/latest.rpm
Retrieving http://repo.webtatic.com/yum/centos/5/latest.rpm
warning: /var/tmp/rpm-xfer.PmflCj: Header V3 DSA signature: NOKEY, key ID
cf4c4ff9
Preparing... ##### [100%]
 1:webtatic-release ##### [100%]
```

Setelah repo.webtatic.com terinstall, maka update php dengan repositori tersebut dengan perintah

```
[root@srv2 phpmyadmin]# yum --enablerepo=webtatic install php
```

Tunggu beberapa saat hingga proses update selesai, besar paket yang update sekitar 7 MB. Jika proses update sudah selesai maka jalankan perintah dibawah ini untuk mengetahui versi PHP

```
[root@srv2 ~]# php -v
PHP 5.3.13 (cli) (built: May  8 2012 20:24:34)
Copyright (c) 1997-2012 The PHP Group
Zend Engine v2.3.0, Copyright (c) 1998-2012 Zend Technologies
[root@srv2 ~]#
```

Cara kedua yaitu dengan menggunakan repositori CentOS, caranya remove terlebih dahulu paket PHP dengan perintah dibawah ini :

```
[root@mail ~]# yum remove php php-common php-mcrypt
[root@mail ~]# yum install php53 php53-cli php53-devel php53-gd php53-
mbstring php53-mysql php53-pdo php53-xml php53-xmlrpc php-pear php53-mcrypt
php53-imap
```

```
[root@mail ~]# php -v
PHP 5.3.3 (cli) (built: May  7 2012 17:58:01)
Copyright (c) 1997-2010 The PHP Group
Zend Engine v2.3.0, Copyright (c) 1998-2010 Zend Technologies
[root@mail ~]#
```

Setelah paket apache sudah diperbarui, maka buka kembali alamat domain untuk membuka phpmyadmin seperti pada gambar dibawah ini



8.9. Monitoring Log Apache dengan Visitors

Visitors merupakan program aplikasi yang berfungsi sebagai monitoring aktifitas pengunjung di Web Server, sehingga dengan adanya program yang berbasis website ini bisa membantu untuk memantau

siapa saja yang membuka Web Site yang terdapat di Server, berikut cara installasi visitors

Masukkan terlebih dahulu repositori pihak ketiga dag seperti perintah dibawah ini

```
[root@srv2 ~]# wget http://dag.wieers.com/rpm/packages/RPM-GPG-KEY.dag.txt
[root@srv2 ~]# rpm --import RPM-GPG-KEY.dag.txt
[root@srv2 ~]# rm -f RPM-GPG-KEY.dag.txt
[root@srv2 ~]# vi /etc/yum.repos.d/dag.repo
[dag]
name=Dag RPM Repository for Red Hat Enterprise Linux
baseurl=http://apt.sw.be/redhat/el5/en/$basearch/dag/
gpgcheck=1
enabled=0
```

Selanjutnya Install paket graphviz menggunakan repositori dag dengan perintah dibawah ini

```
[root@srv2 ~]# yum --enablerepo=dag -y install graphviz
[root@srv2 ~]# wget http://www.hping.org/visitors/visitors-0.7.tar.gz
[root@srv2 ~]# tar zxvf visitors-0.7.tar.gz
[root@srv2 ~]# cd visitors_0.7
[root@srv2 visitors_0.7]# make
cc -c -O2 -Wall -W -g visitors.c
cc -c -O2 -Wall -W -g aht.c
cc -c -O2 -Wall -W -g antigetopt.c
cc -c -O2 -Wall -W -g tail.c
cc -o visitors -O2 -Wall -W -g visitors.o aht.o antigetopt.o tail.o
[root@srv2 visitors_0.7]# cp visitors /usr/local/bin/
[root@srv2 visitors_0.7]# cd
[root@srv2 ~]# mkdir /var/www/html/visitors
```

Selanjutnya menambahkan IP Network pada jaringan di file /etc/httpd/conf.d/visitors.conf

```
[root@srv2 ~]# vi /etc/httpd/conf.d/visitors.conf
<Location /visitors>
    Order Deny,Allow
    Deny from all
    Allow from 129.93.88.20
</Location>
```

IP Address 129.93.88.20 merupakan IP yang dipergunakan untuk uji coba log apache, anda juga bisa mengantinya dengan IP Address atau IP Network yang ada pada jaringan anda, selanjutnya restart apache dan pastikan tidak ada error

```
[root@srv2 ~]# service httpd restart
```

Jika proses restart apache tidak menemui error atau kendala maka langkah selanjutnya adalah membuat report untuk visitors seperti pada perintah dibawah ini

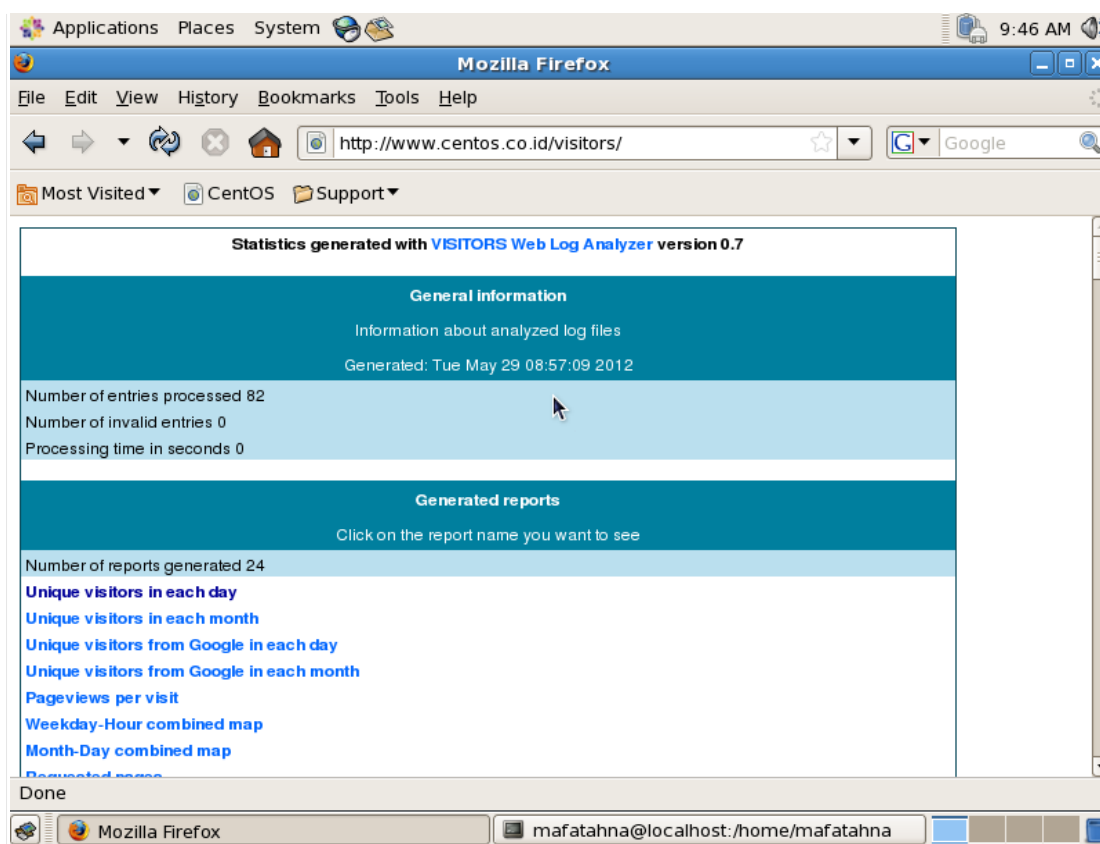
```
[root@srv2 ~]# visitors -A /var/log/httpd/access_log -o html >
/var/www/html/visitors/index.html
--
82 lines processed in 1 seconds
```

```

0 invalid lines, 0 blacklisted referers
[root@srv2 ~]# visitors -A -m 30 /var/log/httpd/access_log -o html --trails
--prefix http://www.centos.co.id > /var/www/html/visitors/trails.html
--
82 lines processed in 1 seconds
0 invalid lines, 0 blacklisted referers
[root@srv2 ~]# visitors /var/log/httpd/access_log --prefix
http://www.centos.co.id -V > /var/www/html/visitors/graph.dot
--
82 lines processed in 1 seconds
0 invalid lines, 0 blacklisted referers
[root@srv2 ~]# dot -Tpng /var/www/html/visitors/graph.dot >
/var/www/html/visitors/graph.png

```

Jika perintah tersebut sudah dijalankan sekarang anda bisa melihat hasilnya dengan mengakses di alamat <http://www.centos.co.id/visitors>



8.10. Monitoring Log Apache dengan Awstats

Awstats sebenarnya memiliki fungsi yang tidak jauh berbeda dengan visitors hanya saja memiliki tampilan yang lebih menarik sehingga bisa menjadikan perbandingan bagi anda untuk menggunakan monitoring mana yang sesuai. Pada proses instalasi kali ini menggunakan repositori dag seperti instalasi visitors. Langkah-langkah instalasi Awstats jalankan perintah dibawah ini

```
[root@srv2 ~]# yum --enablerepo=dag -y install awstats
```

Tunggu beberapa saat hingga instalasi selesai, jika sudah selesai maka copy file berikut ini

```
[root@srv2 ~]# cp /etc/awstats/awstats.model.conf /etc/awstats/awstats.www.centos.co.id.conf
```

Selanjutnya tambahkan beberapa paramater dibawah ini

```
[root@srv2 ~]# vim /etc/awstats/awstats.www.centos.co.id.conf
# Cari baris 122, ganti Log Format = 1
LogFormat=1
# Cari baris 153, ganti dengan alamat domain anda
SiteDomain="www.centos.co.id"
# Cari baris 168, pada baris ini isikan alamat IP yang diperbolehkan akses
HostAliases="localhost 127.0.0.1 REGEX[server\.world$] REGEX[^129\.93\.88\.]"
```

Simpan dan tutup konfigurasi, selanjutnya tambahkan parameter dibawah ini

```
[root@srv2 ~]# vim /etc/httpd/conf.d/awstats.conf
Alias /awstats/icon/ /var/www/awstats/icon/
Alias /report /var/www/awstats/
ScriptAlias /awstats/ /var/www/awstats/
<Directory "/var/www/awstats">
    DirectoryIndex awstats.pl
    Options ExecCGI
    order deny,allow
    deny from all
    allow from 127.0.0.1 129.93.88.12
</Directory>
```

Restart apache dengan perintah

```
[root@srv2 ~]# service httpd restart
[root@srv2 ~]# service httpd restart
Stopping httpd: [ OK ]
Starting httpd: Apache/2.2.3 mod_ssl/2.2.3 (Pass Phrase Dialog)
Some of your private key files are encrypted for security reasons.
In order to read them you have to provide the pass phrases.

Server centos.org:443 (RSA)
Enter pass phrase:

OK: Pass Phrase Dialog successful. [ OK ]

[root@srv2 ~
```

Selanjutnya anda perlu membuat beberapa report seperti dibawah ini

```
[root@srv2 ~]# /var/www/awstats/awstats.pl -config=www.centos.co.id -update
Create/Update database for config
"/etc/awstats/awstats.www.centos.co.id.conf" by AWStats version 7.0 (build
1.971)
From data in log file "/var/log/httpd/access_log"...
Phase 1 : First bypass old records, searching new record...
```

```
Direct access after last parsed record (after line 94)
Jumped lines in file: 94
Found 94 already parsed records.
Parsed lines in file: 0
Found 0 dropped records,
Found 0 comments,
Found 0 blank records,
Found 0 corrupted records,
Found 0 old records,
Found 0 new qualified records.
```

```
[root@srv2 awstats]# /var/www/awstats/awstats.pl -config=www.centos.co.id
-output -staticlink > /var/www/awstats/index.html
```

Buatlah crontab agar perintah tersebut dijalankan perjam, caranya adalah

```
[root@srv2 ~]# vi /etc/cron.hourly/00awstats
#!/bin/bash
if [ -f /var/log/httpd/access_log ] ; then

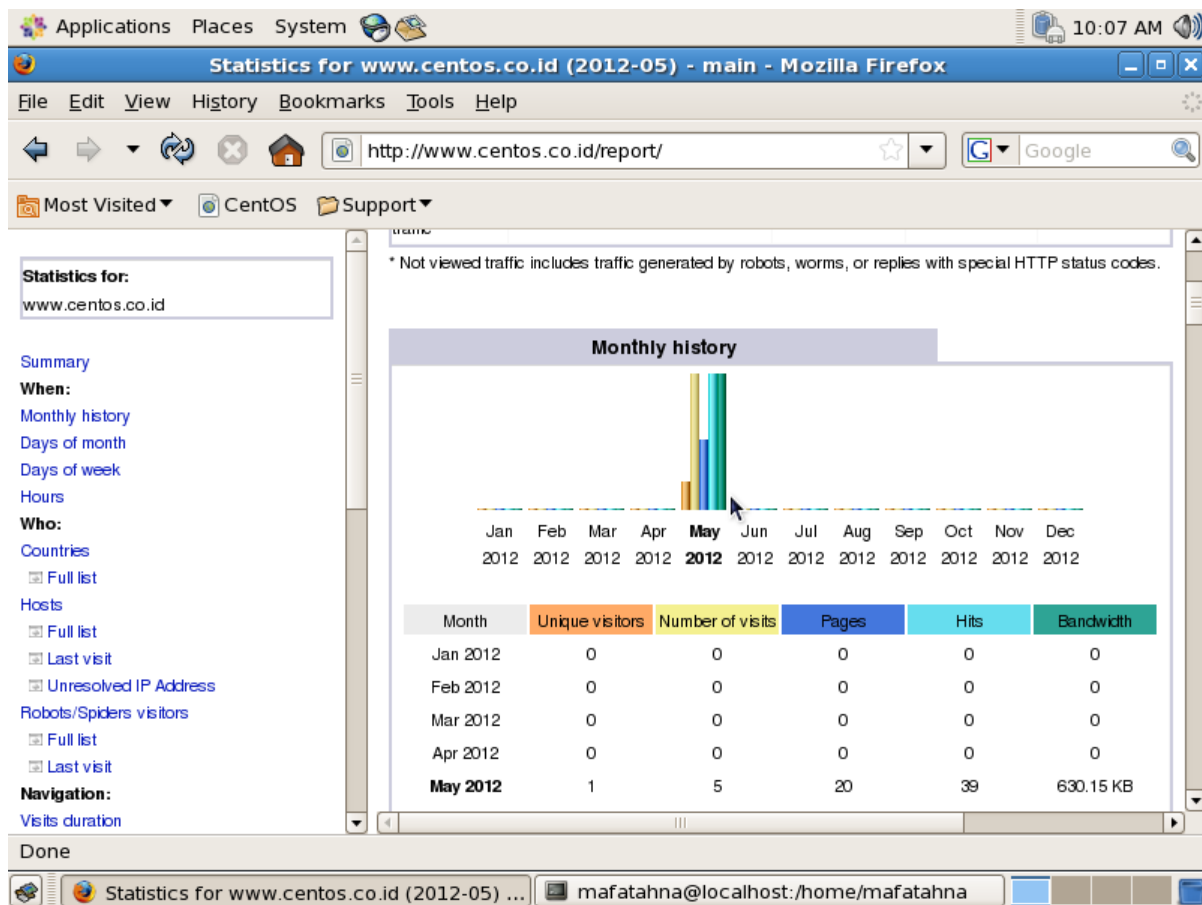
# Tutup perintah ini
#exec /usr/bin/awstats_updateall.pl now -configdir="/etc/awstats"
-awstatsprog="/var/www/awstats/awstats.pl" > /dev/null

# Tambahkan perintah ini
/var/www/awstats/awstats.pl -config=www.server.world -update > /dev/null

/var/www/awstats/awstats.pl -config=www.server.world -output -staticlink
> /var/www/awstats/index.html

fi
exit 0
```

Simpan dan tutup editor anda, sekarang silahkan buka web browser dan akses alamat <http://www.centos.co.id/report/>



8.11. Monitoring Log Apache dengan Piwik

Banyak sekali software yang digunakan untuk monitoring aktifitas Web Server seperti visitors dan awstats. Piwik berbeda dengan visitors dan awstats, piwik merupakan aplikasi monitoring menggunakan java script dan untuk mengaksesnya membutuhkan PHP dan MySQL, sehingga jika anda ingin menggunakan aplikasi ini diharapkan sudah selesai melakukan installasi untuk PHP dan MySQL sehingga ketika installasi piwik tidak menemui beberapa kendala. Sebelum installasi piwik terlebih dahulu install beberapa paket dependensi piwik seperti pada perintah dibawah ini

```
[root@srv2 ~]# yum -y install php-pdo php-gd php-xml
[root@srv2 ~]# vim /etc/php.ini
memory_limit = 512M # baris 314
```

Setelah installasi paket selesai maka langkah selanjutnya adalah download aplikasi piwik di situs resminya menggunakan wget,

```
[root@srv2 ~]# cd /var/www/html
[root@srv2 html]# wget http://piwik.org/latest.zip
[root@srv2 html]# unzip latest.zip
[root@srv2 html]# chmod 777 ./piwik/tmp
[root@srv2 html]# chmod 777 ./piwik/config
```

Piwik selain membutuhkan PHP juga membutuhkan sebuah database MySQL sehingga masuk terlebih dahulu di MySQL pada Server

```
[root@srv2 ~]# mysql -u root -p
Enter password:
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 2
Server version: 5.0.95 Source distribution

Copyright (c) 2000, 2011, Oracle and/or its affiliates. All rights reserved.

Oracle is a registered trademark of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.
```

```
mysql>
```

Selanjutnya setelah masuk di MySQL langkah selanjutnya adalah membuat sebuah database, kali ini penulis menggunakan database dengan nama piwik

```
mysql> create database piwik character set utf8 collate utf8_bin;
Query OK, 1 row affected (0.00 sec)

mysql> grant all privileges on piwik.* to piwik@'localhost' identified by 'password';
Query OK, 0 rows affected (0.00 sec)

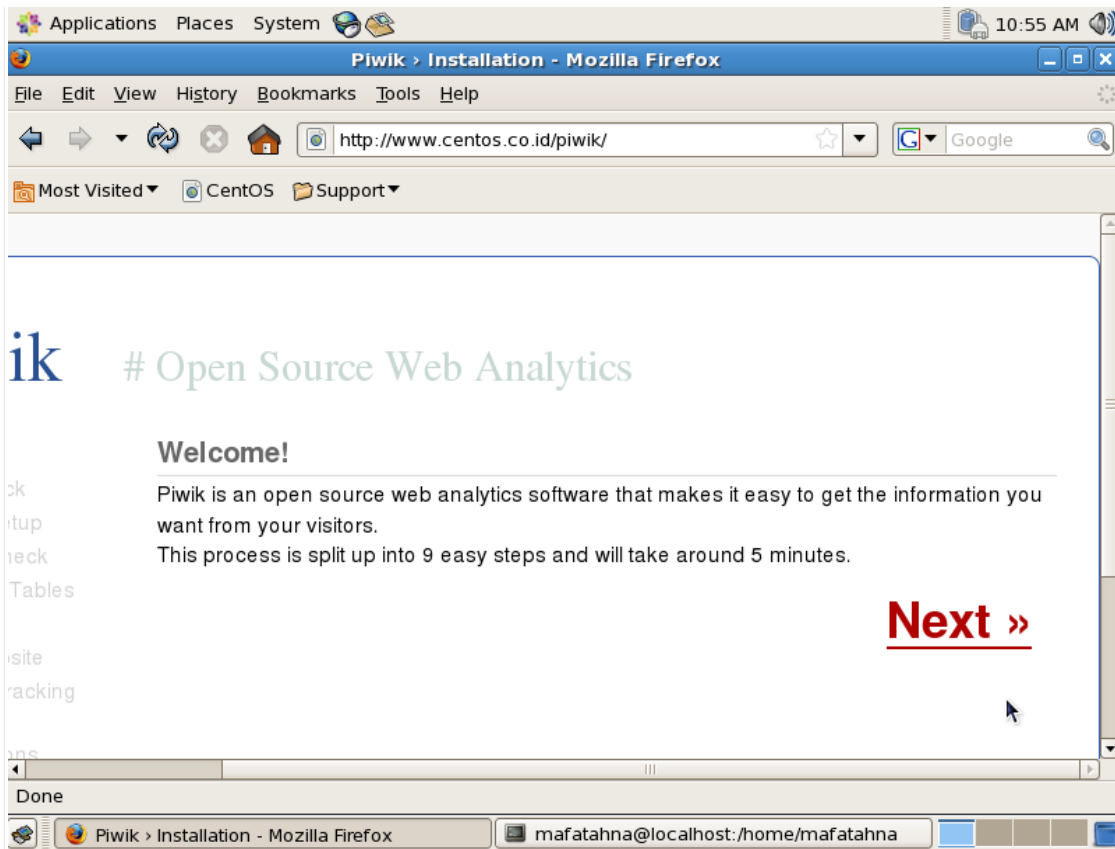
mysql> flush privileges;
Query OK, 0 rows affected (0.00 sec)

mysql> exit
Bye
[root@srv2 ~]#
```

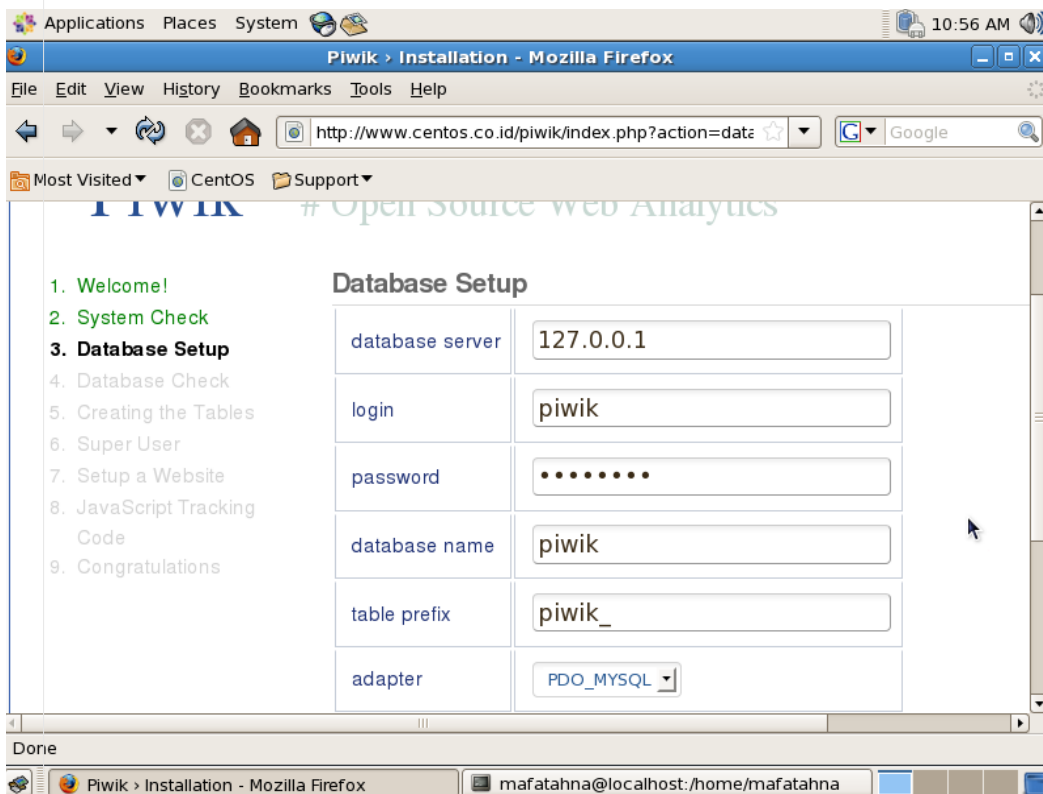
Instalasi Piwik

Seperti halnya web paket yang lain piwik sendiri proses instalasi tidak jauh berbeda dengan paket web yang lain seperti wordpress, drupal, joomla, phpbb dll. Proses instalasi piwik secara prosedural sama persis dengan beberapa paket web yang sudah penulis sebutkan. Sehingga sengaja penulis tidak memberikan contoh bagaimana instalasi web paket seperti wordpress, drupal, joomla, phpbb dll. Tapi penulis hanya memberikan contoh bagaimana cara instalasi piwik, sebab jika anda memperhatikan proses ini maka secara tidak langsung ketika anda install paket web yang lain tidak akan mengalami kendala, berikut ini adalah proses instalasi paket web piwik yang digunakan untuk monitor log apache. Berhubung hasil capture terlalu banyak maka penulis lampirkan hanya beberapa capture yang dirasa penting untuk diketahui

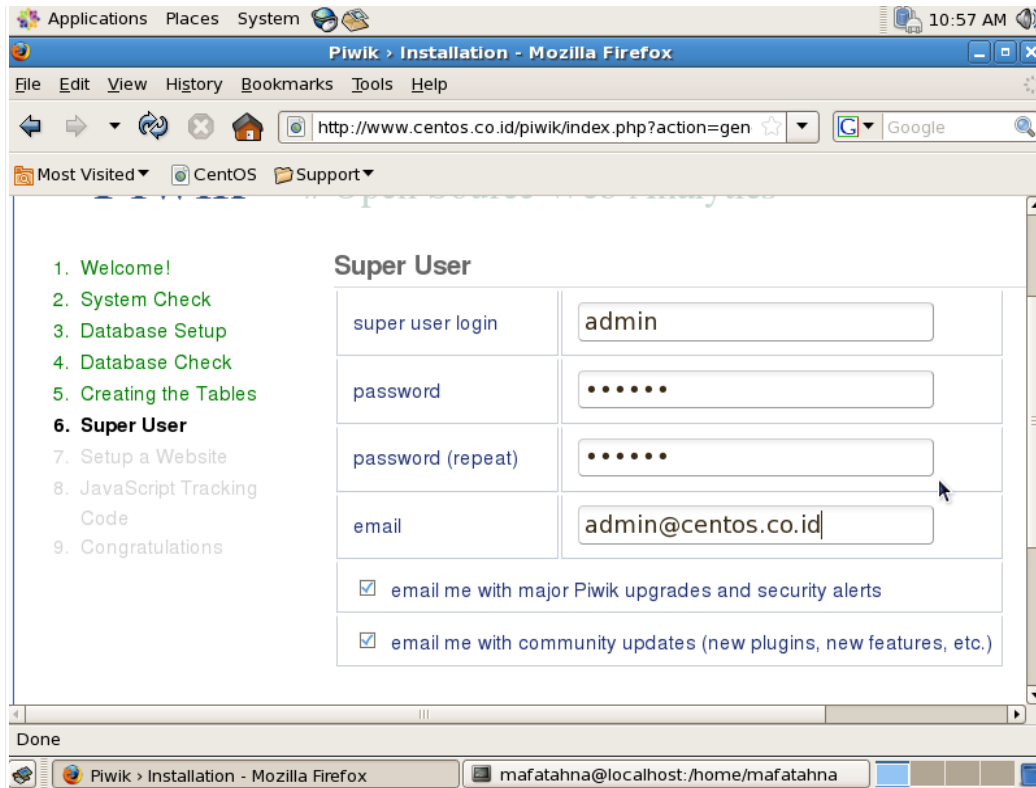
Langkah awal instalasi piwik yaitu dengan mengakses alamat <http://www.centos.co.id/piwik>, selanjutnya untuk memulainya tekan tombol Next



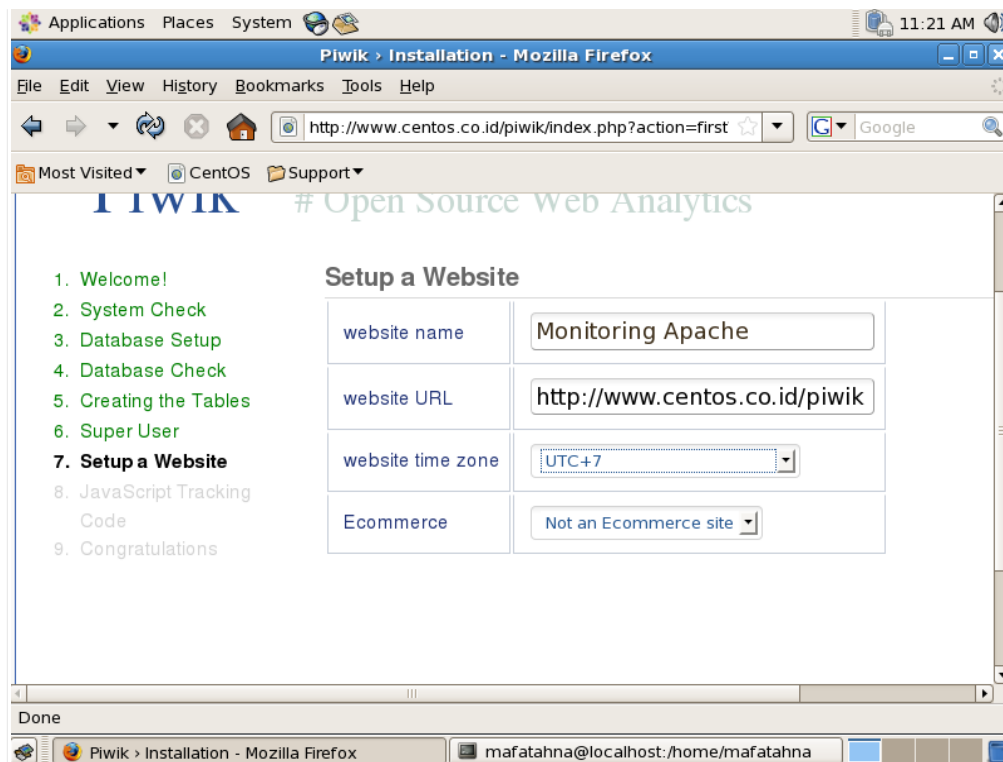
Selanjutnya akan keluar dialog pengecekan sistem, jika anda sudah install beberapa dependensi yang sudah dijelaskan pada Bab pada buku ini kemungkinan kurangnya dependensi tidak ada, sehingga anda bisa lanjutkan dengan klik tombol next



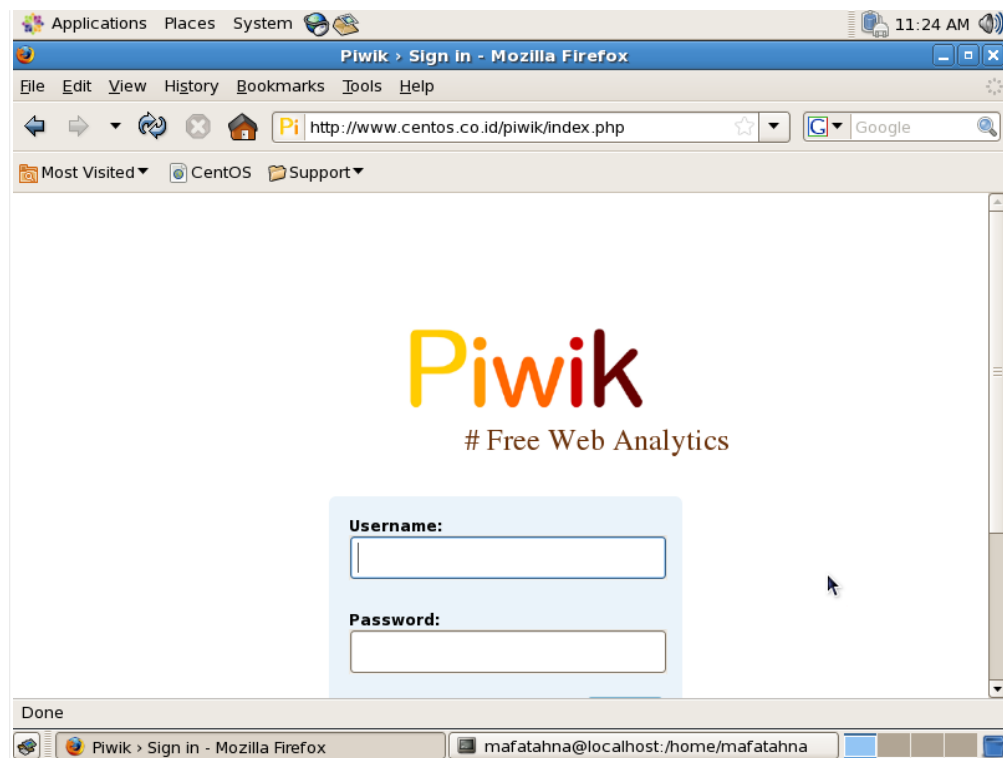
Setelah anda melengkapi beberapa database pada gambar diatas tekan tombol Nxt untuk melanjutkan, selanjutnya terdapat beberapa dialog klik Next saja hingga muncul tampilan pada gambar dibawah ini



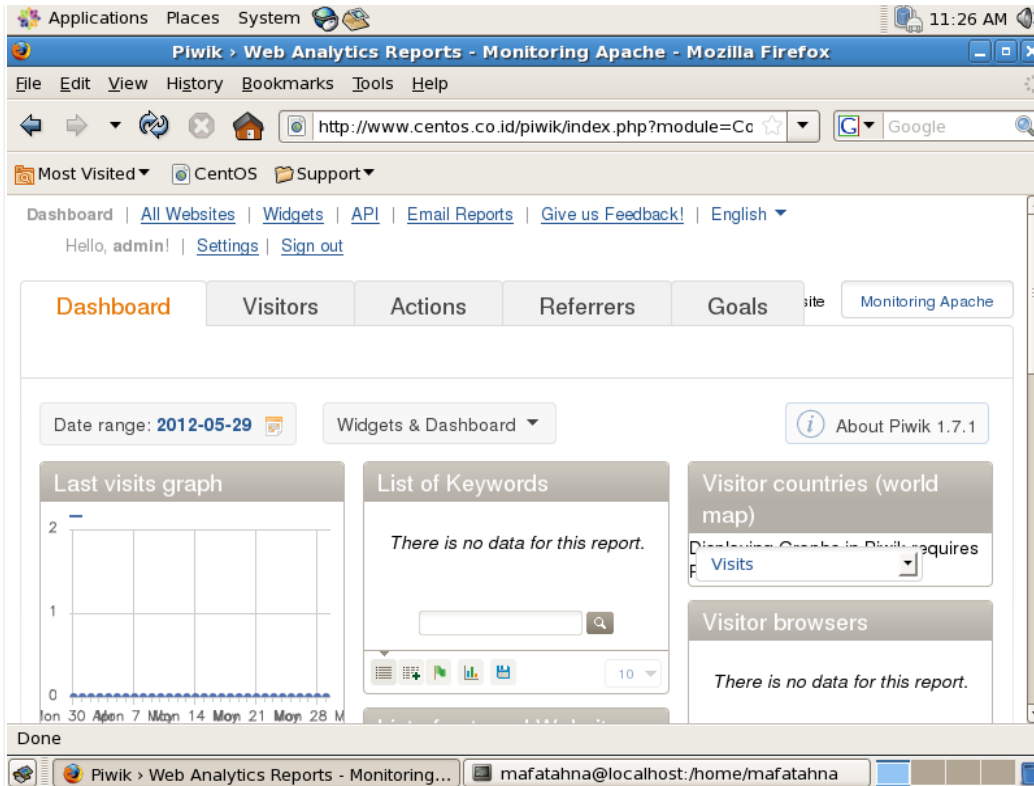
Klik Next untuk melanjutkan instalasi, selanjutnya terdapat dialog “*Setup a Website*” isi dengan nama Website dan pada website URL isi dengan nama domain dan nama folder (lokasi file piwik), pilih juga pada website time zone UTC +7 jika sudah selesai maka klik Next untuk melanjutkan proses instalasi



Tekan tombol Next untuk melanjutkan Installasi Piwik, setelah proses installasi anda diminta memasukkan user dan password sesuai yang anda masukkan ketika proses installasi berlangsung.



Masukkan username dan password yang sudah anda buat, selanjutnya klik Sign In. Jika berhasil maka akan tampil sebuah web seperti pada gambar dibawah ini.



Terdapat beberapa tools untuk monitoring website sehingga penulis tidak bisa menjelaskan satu persatu maka diharapkan anda mencoba sendiri beberapa tools yang sudah disediakan.

Proxy Server

Proxy Server adalah protokol yang digunakan untuk menjembatani koneksi internet dari klien ke server, dengan menggunakan proxy maka secara tidak langsung klien dipaksa mengikuti semua aturan yang sudah ditetapkan proxy. Beberapa aturan yang bisa ditetapkan meliputi hak akses, filtering konten, limiter download dan autentikasi password.

Squid adalah salah satu piranti lunak yang digunakan untuk menerapkan beberapa rule tersebut. Beberapa fitur yang dimiliki squid meliputi beberapa fungsi parameter untuk meningkatkan kinerja dan optimasi secara maksimal tidak penulis jelaskan di buku ini, sebab secara teknik ukuran dalam kinerja squid berbeda-beda dari setiap individu.

Beberapa persiapan yang perlu diperhatikan dalam membangun squid adalah cache. Cache merupakan media penyimpanan khusus untuk menampung cache aktifitas browsing, sehingga cache sendiri perlu dikelompokkan dalam partisi sendiri, misalnya sebuah server dengan Harddisk ukuran 40GB akan dibagi menjadi beberapa partisi yaitu sebagai sistem utama, swap sebagai cadangan memori dan cache sebagai penyimpanan cache browsing, maka anda bisa membuatnya seperti ini :

1. Membuat partisi root (/) kapasitas harddisk 15 GB
2. Membuat partisi swap kapasitas harddisk 4 GB atau 2 kali besar memori
3. Membuat 3 partisi masing-masing 4 GB dengan direktori /cache01, /cache02 dan /cache03

Cara membuat partisi dengan metode penambahan partisi cache bisa anda lihat di bab yang menjelaskan instalasi pada buku ini.

9.1. Instalasi Squid

Selanjutnya jika persiapan tersebut sudah siap maka anda bisa memulai proses instalasi proxy server menggunakan squid yaitu dengan menjalankan perintah dibawah ini :

```
[root@proxy ~]# yum install squid
```

Ketika proses instalasi squid membutuhkan waktu sekitar 5 menit untuk download paket, jika proses instalasi sudah selesai, silahkan membuka editor file utama squid.conf dengan perintah dibawah ini

```
[root@proxy ~]# vim /etc/squid/squid.conf
```

Cari baris 572 dan tambahkan alamat network anda seperti dibawah ini

```
acl my-network src 192.168.10.0/24  
#Recommended minimum configuration:
```

Baris 628 tambahkan rule http_access seperti contoh berikut

```
http_access allow my-network  
# INSERT YOUR OWN RULE(S) HERE TO ALLOW ACCESS FROM YOUR CLIENTS
```

Baris 3008 tambahkan nama hostname yang digunakan, penulis menggunakan proxy.centos.co.id

```
visible_hostname proxy.centos.co.id
```

Baris 4280 setting menjadi OFF berfungsi menyembunyikan IP Address

```
forwarded_for off
```

Konfigurasi tersebut merupakan beberapa parameter standart yang digunakan proxy server, jika sudah selesai simpan konfigurasi anda dan restart service squid

```
[root@proxy ~]# service squid restart
Stopping squid: ..... [ OK ]
Starting squid: . [ OK ]
[root@proxy ~]#
[root@proxy ~]# chkconfig squid on
```

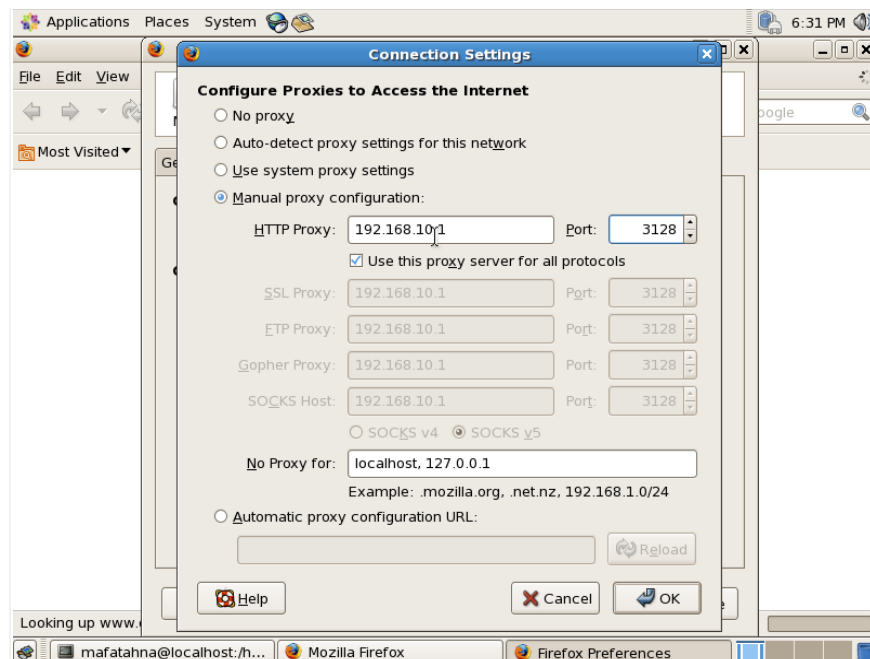
Selanjutnya aktifkan mode forwarding dengan mengubah default 0 menjadi 1 seperti dibawah ini

```
[root@proxy ~]# vim /etc/sysctl.conf
net.ipv4.ip_forward = 1
```

Simpan dan keluar dari editor tersebut, jalankan perintah dibawah ini

```
[root@proxy ~]# sysctl -p
net.ipv4.ip_forward = 1
net.ipv4.conf.default.rp_filter = 1
net.ipv4.conf.default.accept_source_route = 0
[root@proxy ~]#
```

Setelah mode forwarding sudah anda aktifkan, maka coba lakukan akses internet dari klien yaitu menambahkan proxy seperti dibawah ini



Jangan lupa untuk mengarahkan gateway ke IP Address router yaitu 192.168.10.1 sedangkan default port menggunakan 3128 sebab port squid tidak dirubah. Jika dari klien bisa akses internet maka proxy server anda sudah berhasil.

9.2. Autentikasi Password

Secara umum, klien yang terhubung dengan proxy server pasti bisa melakukan koneksi internet, dengan catatan mengetahui network, gateway dan DNS yang digunakan. Namun jika internet tersebut digunakan hanya untuk orang tertentu maka sistem tersebut kurang aman, sebab setiap orang bisa terkoneksi dengan internet. Autentikasi password digunakan solusi dari masalah tersebut.

Sistem ini biasa digunakan lingkup Universitas, sebab batasan dalam hak akses yang digunakan tidak lagi bersifat IP Address yang digunakan klien, tetapi menggunakan user dan password sehingga aktifitas internet lebih aman dan hanya orang-orang yang memiliki user dan password saja yang bisa menggunakan fasilitas internet.

Htpasswd merupakan sistem autentikasi dari apache, namun bisa di integrasikan dengan squid. Dalam penggunaannya juga relatif mudah sebab squid sudah support dengan htpasswd. Sebelum menambahkan beberapa parameter yang digunakan di file squid.conf, buatlah user yang digunakan untuk akses internet menggunakan htpasswd dengan perintah dibawah ini :

```
[root@proxy ~]# touch /etc/squid/password
[root@proxy ~]# htpasswd /etc/squid/passwd user1
New password:
Re-type new password:
Adding password for user user1
[root@proxy ~]#
```

Setelah user ditambahkan menggunakan htpasswd, langkah selanjutnya menambahkan beberapa parameter yang terdapat di file squid.conf, edit file tersebut seperti berikut ini :

```
[root@proxy ~]# vim /etc/squid/squid.conf
```

Hilangkan tanda komentar [#] pada parameter dibawah ini :

```
auth_param basic program /usr/lib/squid/ncsa_auth /etc/squid/passwd
auth_param basic children 5
auth_param basic realm Squid proxy-caching web server
auth_param basic credentialsttl 2 hours
auth_param basic casesensitive off
```

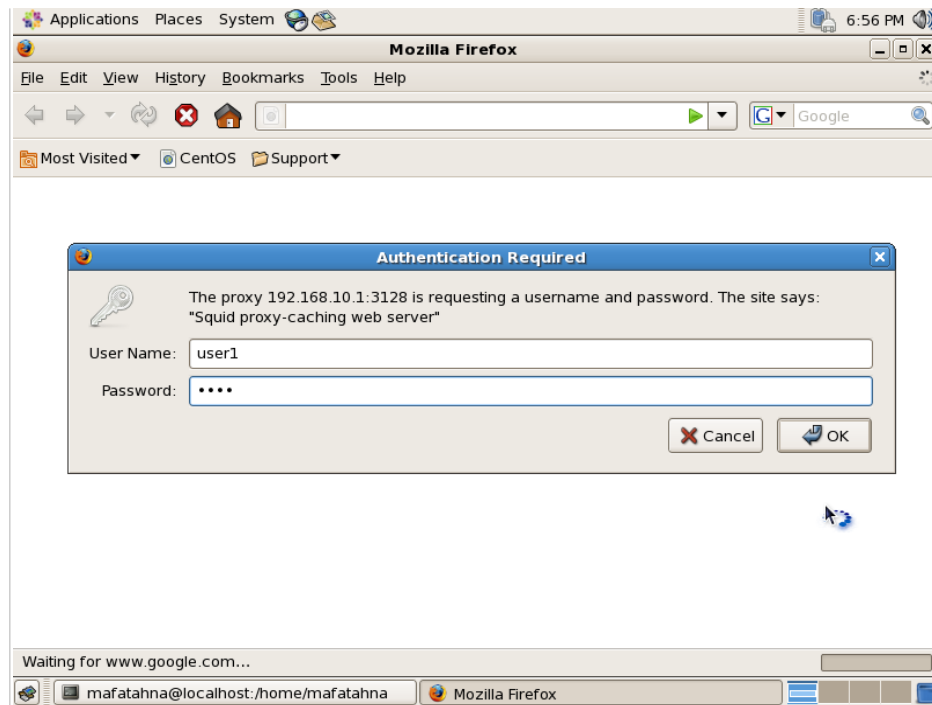
Tambahkan ncsa network dibawah acl network

```
acl my_network src 192.168.10.0/24
acl ncsa_network proxy_auth REQUIRED
```

Tambahkan juga hak akses dibawah acl network

```
http_access allow ncsa_network
http_access allow my_network
```

Simpan konfigurasi tersebut, keluar dari editor dan terakhir restart squid. Lakukan uji coba menggunakan web browser, jika dalam akses alamat situs meminta password dan user maka integrasikan htpassword dengan squid sudah berhasil.



Permintaan autentikasi tersebut digunakan sebagai kunci koneksi ke internet, sehingga jika terdapat user memasukkan user name dan password salah, maka secara otomatis akan ditolak oleh server proxy.

9.3. Filtering Content

Internet merupakan pintu untuk mengetahui semua informasi di dunia, banyak sekali kemudahan yang dihasilkan dari teknologi internet, namun informasi yang terdapat di internet tidak semuanya berdampak positif bagi kebanyakan orang, sehingga perlu adanya pemilihan content apa saja yang perlu dan tidak untuk diakses.

Penerapan fitur ini biasanya digunakan di beberapa Universitas yaitu dengan harapan fasilitas internet yang diberikan kampus hanya ditujukan terhadap situs-situs yang berhubungan dengan kampus, sehingga mahasiswa bisa lebih memaksimalkan dalam aktifitas mencari informasi dan mewujudkan internet sehat di Universitas tersebut.

Parameter yang digunakan dalam `acl url_regex`, sehingga jika anda memiliki list alamat situs yang di blok bisa dimasukkan terlebih dahulu pada sebuah file sehingga script yang ditambahkan di `squid.conf` lebih singkat. Dalam penerapannya anda bisa melihat contoh berikut ini :

Membuat file sebagai lokasi penulisan website yang di block

```
[root@proxy ~]# mkdir /etc/squid/block/  
[root@proxy ~]# touch /etc/squid/block/acl_jejaring sosial  
[root@proxy ~]# touch /etc/squid/block/acl_terlarang
```

Terdapat 2 file yang digunakan sebagai block content yaitu `acl_jejaring sosial` dan `acl_terlarang`, fungsi

dari file tersebut akan digunakan sebagai pengelompokan alamat website seperti jejaring sosial (facebook, twitter dll) sedangkan acl_terlarang digunakan sebagai pengelompokan situs-situs yang tidak diperbolehkan, misalnya situs torrent dan situs porno.

Tambahkan beberapa alamat situs di kedua file tersebut dengan editor vim seperti dibawah ini :

```
[root@proxy ~]# vim /etc/squid/block/acl_jejaringsosial
.facebook.com
.twitter.com
```

```
[root@proxy ~]# touch /etc/squid/block/acl_terlarang
.youtube.com
```

Anda juga bisa menambahkan alamat situs yang lain sesuai kebutuhan, setelah file sudah tersedia maka anda tinggal memasukkan parameter dibawah ini ke dalam file squid.conf

```
acl blokir1 url_regex -i "/etc/squid/block/acl_jejaringsosial"
acl blokir2 url_regex -i "/etc/squid/block/acl_terlarang"

http_access deny blokir1
http_access deny blokir2
```

Nama blokir1 hanya sebuah pendefinisian sehingga bisa anda ganti sesuai kebutuhan,

9.4. Limit Berdasarkan Waktu

Batasan akses internet akan lebih flexibel jika diterapkan terhadap beberapa waktu yang memang diharapkan sebagai user tidak jenuh yang hanya bisa mengakses beberapa situs yang sudah ditunjuk. Namun bisa juga digunakan sebagai (hiburan) ketika semua aktifitas sudah selesai. Misalnya sebuah Universitas menerapkan filtering content dengan aturan sebagai berikut

Block seluruh situs jejaring sosial pada jam praktikum yaitu
Jam 08:00 s.d 12:00 dan 13:00 s.d 16:00 hari Senin s.d Jum'at
Jam 08:00 s.d 12:00 hari Sabtu dan Minggu

Sedangkan situs terlarang di block permanen (setiap hari). Maka anda bisa menerapkan aturan tersebut dengan rule berikut ini :

```
acl waktu_pagi time MTWHF 08:00-12:00
acl waktu_siang time MTWHF 13:00-16:00
acl hari_libur time AS 08:00-14:00

acl blokir_situs url_regex -i "/etc/squid/block/acl_jejaringsosial"
acl blokir_terlarang url_regex -i "/etc/squid/block/acl_terlarang"

http_access deny blokir_situs waktu_pagi
http_access deny blokir_situs sabtu_siang
http_access deny blokir_situs hari_libur
http_access deny blokir_terlarang
```

Keterangan :

S – Sunday, M – Monday, T – Tuesday, W – Wednesday, H – Thursday, F – Friday, A – Saturday

9.5. Partisi Cache di Squid

Sebelumnya sudah dijelaskan cara membuat partisi cache di bab instalasi pada buku ini. Cache digunakan sebagai tempat penyimpanan cache sementara, sehingga kecepatan dalam penyimpanan cache juga perlu diperhatikan sehingga perlu adanya partisi tersendiri sebagai media penyimpanan cache. Berikut ini langkah-langkah yang digunakan untuk menambahkan cache di squid.

Cek terlebih dahulu partisi di root (/) apakah sudah terdapat partisi cache atau belum, dengan perintah

```
[root@proxy ~]# ls /
bin          cache02     etc         lost+found  mnt         proc        selinux     tmp
boot        cache03     home        media        net         root        srv         usr
cache01     dev         lib         misc         opt         sbin        sys         var
[root@proxy ~]#
```

Selanjutnya ganti hak kepemilikan cache tersebut menjadi squid (sebelumnya root), dengan perintah `chown` seperti berikut ini :

```
[root@proxy ~]# chown squid.squid /cache01
[root@proxy ~]# chown squid.squid /cache02
[root@proxy ~]# chown squid.squid /cache03
```

Secara default cache sudah diarahkan ke direktori `/var/spool/squid` edit pengaturan cache berikut ini :

```
#Default:
# cache_dir ufs /var/spool/squid 100 16 256
```

Menjadi

```
cache_dir ufs /cache01 3000 16 256
cache_dir ufs /cache02 3000 16 256
cache_dir ufs /cache03 3000 16 256
```

Simpan dan tutup file `squid.conf`, selanjutnya restart squid

9.6. Transparent Proxy

Layanan free akses internet yang disediakan di beberapa cafe, hotel dan restaurant biasanya tidak menggunakan password. Namun, jangan kira free hotspot tersebut tidak memiliki proxy yang digunakan untuk memonitoring aktifitas anda di internet, biasanya koneksi internet yang digunakan menggunakan salah satu fungsi dari squid yaitu proxy transparent.

Proxy transparent memungkinkan penggunaan bebas melakukan koneksi internet tanpa memasukkan alamat proxy dan port yang digunakan. Namun klien akan dipaksa untuk masuk kedalam sistem squid terlebih dahulu sebelum terkoneksi dengan internet. Adapun langkah-langkah untuk membuat proxy transparent adalah sebagai berikut.

Aktifkan forwarding dengan memberikan angka 1 (aktif)

```
[root@proxy ~]# vim /etc/sysctl.conf
net.ipv4.ip_forward = 1
```

Selanjutnya aktifkan fitur tersebut dengan perintah berikut ini :

```
[root@proxy ~]# sysctl -p
net.ipv4.ip_forward = 1
net.ipv4.conf.default.rp_filter = 1
net.ipv4.conf.default.accept_source_route = 0
[root@proxy ~]#
```

Tambahkan default port yang terdapat di /etc/squid/squid.conf menjadi

```
http_port 3128 transparent
```

Simpan konfigurasi squid.conf, kemudian jalankan iptables untuk mengalihkan default port http (80) menuju port yang digunakan squid yaitu 3128. perintahnya adalah sebagai berikut ini :

```
[root@proxy ~]# iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE
[root@proxy ~]# iptables -A PREROUTING -t nat -p tcp --dport 80 -j REDIRECT
--to-port 3128
```

Agar perintahnya tersebut dijalankan secara otomatis ketika komputer restart maka save rule tersebut ke file /etc/rc.local

```
[root@proxy ~]# vim /etc/rc.local

#!/bin/sh
#
# This script will be executed *after* all the other init scripts.
# You can put your own initialization stuff in here if you don't
# want to do the full Sys V style init stuff.

iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE
iptables -A PREROUTING -t nat -p tcp --dport 80 -j REDIRECT

touch /var/lock/subsys/local
```

Simpan konfigurasi tersebut dan restart PC Router anda, lakukan uji coba dengan menghapus konfigurasi proxy di web browser klien.

9.7. Membatasi Bandwidth Dengan Delay Pools

Fitur-fitur yang dimiliki squid selain memiliki beberapa parameter yang digunakan sebagai batasan hak akses dan filter content, namun juga memiliki fitur yang digunakan sebagainya limit bandwidth yaitu delay pools. Delay pools sendiri memiliki beberapa struktur tambahan meliputi :

Delay_pools

Parameter ini digunakan sebagai dasar dalam manajemen bandwidth yaitu menentukan berapa jumlah pools yang akan digunakan, parameter ini nantinya akan berhubungan dengan parameter yang lain seperti delay_class, delay_parameters dan delay_access, kode yang digunakan yaitu :

```
delay_pools 3
```

Artinya dalam parameter delay pools menerapkan 3 pengelompokan manajemen bandwidth

Delay_class

Merupakan parameter yang digunakan untuk menentukan jumlah class dalam delay pools, squid pada dasarnya hanya mendukung 3 class saja yaitu

- Class 1 : berfungsi untuk membatasi bandwidth dalam jaringan dengan single bucket, opsi ini nanti juga bisa digunakan sebagai parent dari class sesudahnya yaitu class 2 dan class 3
- Class 2 : batasan jika menggunakan opsi ini akan dibatasi oleh single bucket (class 1) tetapi class 2 juga bisa memberikan batasan tersendiri dibawah parent (class 1) yaitu disetiap host.
- Class 3 : merupakan opsi class yang paling spesifik sebab class ini dibatas single bucket (class 1) dan batasan per host (class 2). Namun biasanya class 3 digunakan untuk membatasi file multimedia, document dan beberapa extension lain, misalnya mp3, odt, avi dan lain sebagainya.

Kode yang digunakan yaitu :

```
delay_class 1 3
```

Delay_parameters

Parameter yang digunakan untuk menentukan nilai yang digunakan sebagai limit bandwidth, misalnya :

```
delay_parameters 1 64000/64000 10000/320000 1000/1000
```

Dari contoh parameter tersebut dijelaskan bawah bandwidth total yang diberikan adalah 64000 bps, jika anda ingin mengubahnya kesatuan Kbps (Kilo Bit) silahkan dibagi 8, untuk lebih jelasnya perhatikan contoh berikut ini :

$64000 \text{ bps (Bit)} = 512 \text{ Kbps (Kilo Bit)} = 64\text{KBps (Kilo Byte)}$

Sehingga kecepatan real yang akan didapatkan adalah 64 KBps, dari penjelasan diatas merupakan hasil dari besar jumlah bandwidth yang diberikan dalam class 1 (single bucket). Delay class 2 terdapat 10000 dan 32000, artinya secara normal bandwidth yang didapatkan setiap host dalam jaringan adalah 80 Kbps dan 256 Kbps adalah nilai bandwidth maksimum dalam bucket. Delay class 3 lebih spesifik dengan batasan segment di jaringan seperti extension file dan multimedia.

Delay_access

Parameter yang terakhir di delay pools ini digunakan sebagai menentukan acl mana saja yang di ijinan dalam mengikuti prosedur yang sudah ditetapkan dalam struktur delay pools. Misalnya anda memiliki acl yang di alokasikan untuk admin dan office, yang anda inginkan admin tidak melalui delay pools, namun office masuk dalam prosedur delay pools, maka parameter yang digunakan adalah :

```
delay_access 1 allow office  
delay_access 2 deny admin
```

9.8. File Squid.conf

Berikut ini contoh parameter yang digunakan di squid sekaligus catatan singkat sebagai penjelasan, anda juga bisa copas ke server proxy anda tetapi dengan catatan file-file yang terdapat di konfigurasi tersebut juga harus ada misalnya acl_jejaringsosial, web, file, multimedia dan lain sebagainya.

```
# Mengaktifkan fitur autentikasi password
auth_param basic program /usr/lib/squid/ncsa_auth /etc/squid/password
auth_param basic children 5
auth_param basic realm Squid proxy-caching web server
auth_param basic credentialsttl 2 hours
auth_param basic casesensitive off

acl ncsa_network proxy_auth REQUIRED
acl waktu time MTWHF 08:00-16:00
acl sabtu time AS 08:00-14:00

# Redirect ke situs google.com jika mengakses situs jejaring sosial
# dalam jam kerja
acl blokir url_regex -i "/etc/squid/block/acl_jejaringsosial"
deny_info http://www.google.com blokir

# rule block situs website
acl blokir1 url_regex -i "/etc/squid/block/acl_terlarang"
acl blokir2 url_regex -i "/etc/squid/block/web"

# limitasi bandwidth berdasarkan extension
acl limit_download url_regex -i "/etc/squid/download/file"
acl limit_download url_regex -i "/etc/squid/download/multimedia"
acl limit_download url_regex -i "/etc/squid/download/software"

# acl user dalam groups
acl unlimited proxy_auth "/etc/squid/groups/unlimited"
acl standart proxy_auth "/etc/squid/groups/standart"
acl limit proxy_auth "/etc/squid/groups/limit"
acl nointernet proxy_auth "/etc/squid/groups/nointernet"

acl all src 0.0.0.0/0.0.0.0
acl manager proto cache_object
acl localhost src 127.0.0.1/255.255.255.255
acl to_localhost dst 127.0.0.0/8
acl SSL_ports port 443
acl Safe_ports port 80          # http
acl Safe_ports port 21         # ftp
acl Safe_ports port 443       # https
acl Safe_ports port 70        # gopher
acl Safe_ports port 210       # wais
acl Safe_ports port 1025-65535 # unregistered ports
acl Safe_ports port 280       # http-mgmt
acl Safe_ports port 488       # gss-http
acl Safe_ports port 591       # filemaker
acl Safe_ports port 777       # multiling http
acl CONNECT method CONNECT
```

```

# block situs berdasarkan waktu yang sudah ditentukan
http_access deny blokir waktu
http_access deny blokir sabtu

# block situs pada rule blokir1
http_access deny blokir1

# user kelompok groups nointernet hanya bisa mengakses situs yang terdaftar
# di file blokir2 = /etc/squid/block/web
http_access allow blokir2
http_access deny nointernet

http_access allow unlimited
http_access allow standart
http_access allow limit

# Mengaktifkan fitur autentikasi
http_access allow ncsa_network

http_access deny manager localhost
http_access deny manager
http_access deny !Safe_ports
http_access deny CONNECT !SSL_ports
http_access deny localhost
http_access deny all

icp_access allow all
http_port 3128
hierarchy_stoplist cgi-bin ?

cache_mem 8 MB
maximum_object_size_in_memory 8 KB
memory_replacement_policy lru
cache_replacement_policy lru

# partisi cache
cache_dir ufs /cache01 3000 16 256
cache_dir ufs /cache02 3000 16 256
cache_dir ufs /cache03 3000 16 256

minimum_object_size 0 KB
maximum_object_size 4096 KB
cache_swap_low 90
cache_swap_high 95
access_log /var/log/squid/access.log squid
cache_log /var/log/squid/cache.log
cache_store_log /var/log/squid/store.log
logfile_rotate 0
mime_table /etc/squid/mime.conf

```

```

acl QUERY urlpath_regex cgi-bin \?
cache deny QUERY
refresh_pattern ^ftp:          1440      20%      10080
refresh_pattern ^gopher:       1440      0%       1440
refresh_pattern .               0         20%      4320
quick_abort_min 16 KB
quick_abort_max 16 KB
quick_abort_pct 95
positive_dns_ttl 1 hours
negative_dns_ttl 1 minute
request_header_max_size 20 KB
reply_header_max_size 20 KB
request_body_max_size 0 KB
acl apache rep_header Server ^Apache
broken_vary_encoding allow apache
cache_mgr root
forwarded_for on
coredump_dir /var/spool/squid

header_access Referer deny all
header_access X-Forwarded-For deny all
header_access Via deny all
header_access Cache-Control deny all

delay_pools 4

# Membatas download di file ekstensi yang sudah diregistrasikan
# dengan bandwidth penuh 256 kbps, perhost 80kbps sedangkan
# per extension 8kbps
delay_class 1 3
delay_parameters 1 32000/32000 10000/10000 1000/1000
delay_access 1 allow limit limit_download
delay_access 1 deny all

# Bandwidth yang disediakan 256kbps sedangkan untuk perhost 80kbps
delay_class 2 2
delay_parameters 2 32000/32000 10000/10000
delay_access 2 allow limit
delay_access 2 deny all

# Bandwidth yang disediakan 512kbps sedangkan untuk perhost 256kbps
delay_class 3 2
delay_parameters 3 64000/64000 32000/32000
delay_access 3 allow standart
delay_access 3 deny all

# Bandwidth yang disediakan unlimited
delay_class 4 1
delay_parameters 4 -1/-1
delay_access 4 allow unlimited
delay_access 4 deny all

```