Network Technologies

Information and Communication Technology

Training Institute, Union of Myanmar

[Linux Server]

Document History

Date	Version	By	Remarks
24 Aug. 2007	1.00	T. Sasahara	First version
7 Jan. 2008	1.01-1	T. D. Win K. Z. Z. Phyu	Supporting openSUSE10.3
9 Jan. 2008	1.01-2	T. D. Phyu E. E. Khin	Supporting openSUSE10.3
11 Jan. 2008	1.01-3	T. D. Phyu Sabei Ko	Supporting openSUSE10.3
14 Jan. 2008	1.01-4	Sabei Ko K. M. San	Supporting openSUSE10.3
17 Jan. 2008	1.01-5	E. E. Khin T. D. Win	Supporting openSUSE10.3
20 Jul. 2008	1.02	K. P. Thant K. M. San	Supporting openSUSE10.3
11 Jan. 2009	1.03	T. D. Phyu K. M. San S.B.Ko T.D.Win T.Naing	Supporting openSUSE11.1
8 Jul. 2010	1.04	K.M.San K.P.Thant E.C.Htoon K.Z.Z.Phyu	Supporting openSUSE11.2
20 Dec. 2010	1.05	K.P.Thant K.Z.Z.Phyu T.Naing K. M. San	Supporting openSUSE11.3
20 Jul. 2010	1.06	K.P. Thant T.Naing	Editing Mail Server (openSUSE11.3)
8 Jan. 2012	1.07	K.M.San T.Naing	Supporting openSUSE11.4

Copyright Information

SUSE®, openSUSE®, the openSUSE® logo, Novell®, the Novell® logo, the N® logo, are registered trademarks of Novell, Inc. in the United States and other countries. Linux is a registered trademark of Linus Torvalds.

The example companies, organizations, products, domain names, e-mail address, logos, people, places, and events depicted herein are fictitious. No association with any real company, organization product, domain name, e-mail address, logo, person, place, or event is intended or should be inferred.

All other products and company names are the trademarks, registered trademarks, and service marks of the respective owners. Throughout this manual, ICTTI and JICA have used its best efforts to distinguish proprietary trademarks from descriptive names by following the capitalization styles used by the manufacturer.

Contents at a Glance

Table of Contents

1. DNS Server (BIND) <Day 1>

1.1. DNS Introduction

The Domain Name System (DNS) is a system that stores information about host names and domain names on networks, such as the Internet. Most importantly, it provides an IP address for each host name, and lists the mail exchange servers accepting e-mail for each domain.

The DNS forms a vital part of the Internet, because hardware requires IP addresses to perform routing, but humans use host names and domain names, for example in URLs and e-mail addresses.

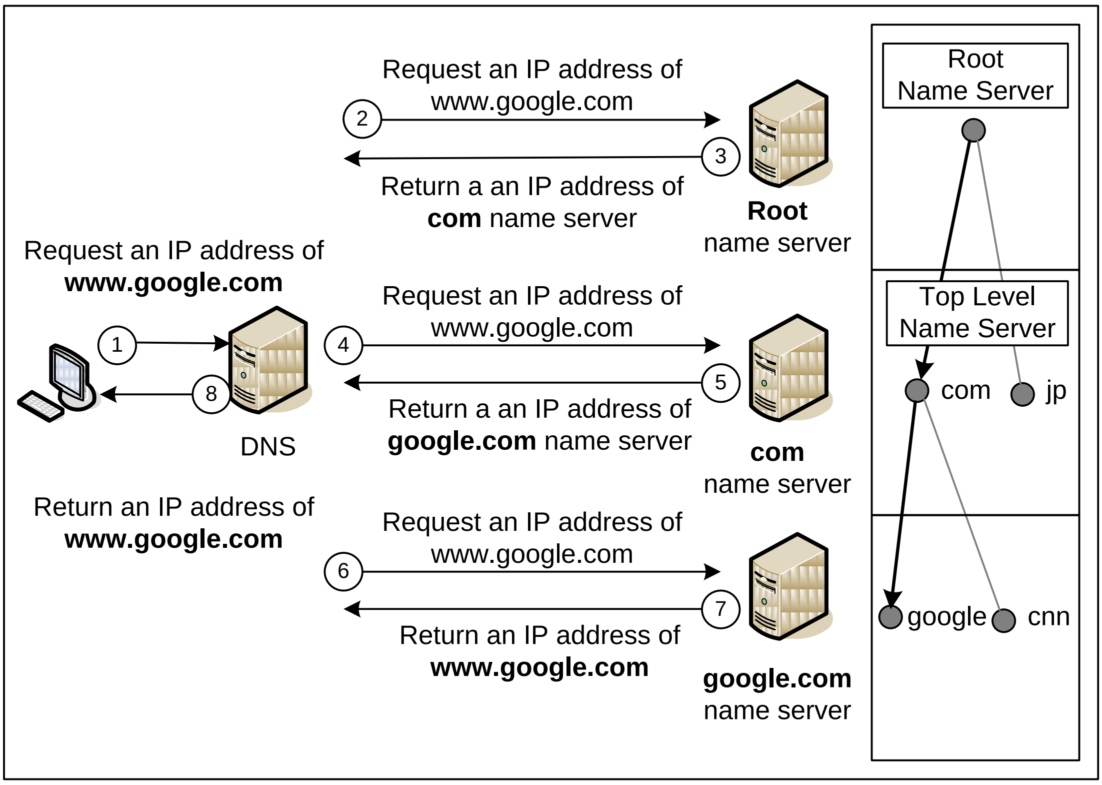


Figure 1 – How the DNS works

A domain name usually consists of two or more parts (technically labels) separated by dots. The rightmost label conveys the top-level domain (for example, the address www.google.com has the top-level domain com). Each label to the left specifies a subdivision or subdomain (for example, google.com is a subdomain of com and www.google.com is a subdomain of google.com).

BIND (Berkeley Internet Name Domain, previously: Berkeley Internet Name Daemon) is the most commonly used DNS server on the Internet, especially on Unix-like systems, where it is a de facto standard.

1.2. BIND Configuration

1.2.1. BIND Installation

Install the following packages.

- `bind`
- `bind-chrootenv`
- `bind-doc`
- `bind-libs`
- `bind-utils`

Start BIND automatically

```
# chkconfig --list | grep named
named                 0:off  1:off  2:off  3:off  4:off  5:off  6:off
# chkconfig named on
# chkconfig --list | grep named
named                 0:off  1:off  2:off  3:on   4:off  5:on   6:off
```

Location of setting files

Table 1 – BIND setting files

Path	
/etc/named.conf	Main configuration file
/var/lib/named/master/	Directory for master zone and reverse zone file
/var/lib/named/slave/	Directory for slave zone and reverse zone file
/etc/resolv.conf	DNS local resolver configuration

1.2.2. Forward Zone

Forward zone configuration is basically to resolve the IP address by FQDN.

If you do not add any zone, this is a caching-only server that is not authoritative for any zone. This type of server’s function is to answer queries by storing in its memory data from authoritative servers.

First, we must introduce the zone to `/etc/named.conf`

```
…
zone "domain1.site" in {
       file "master/domain1.zone";
       type master;
};
```

Next, create the zone file `/var/lib/named/master/domain1.zone`

```
$TTL 2D
@                          IN  SOA                srv1.domain1.site.
root.srv1.domain1.site. (
                            2009071401     ; serial
                            3H            ; refresh
                            1H            ; retry
                            1W            ; expiry
                            1D )           ; minimum
              IN MX 10       srv1.domain1.site.
              IN NS          srv1.domain1.site.
              IN A           192.168.0.10
srv1           IN A           192.168.0.10
pop3           IN CNAME        srv1
smtp           IN CNAME        srv1
www            IN CNAME        srv1
proxy          IN CNAME        srv1
mail           IN CNAME        srv1
admin           IN CNAME        srv1
```

These types of DNS records are stored in DNS as Table 2.

Table 2 – Types of DNS records

Record	Description
A	An A record or address record maps a host name to its 32-bit IPv4 address.

CNAME	A CNAME record or canonical name record makes one domain name an alias of another. The aliased domain gets all the subdomains and DNS records of the original.
MX	An MX record or mail exchange record maps a domain name to a list of mail exchange servers for that domain.
PTR	A PTR record or pointer record maps a host name to the canonical name for that host. Setting up a PTR record for a host name in the in-addr.arpa domain that corresponds to an IP address implements reverse DNS lookup for that address. For example (at the time of writing), www.icann.net has the IP address 192.0.34.164, but a PTR record maps 164.34.0.192.in-addr.arpa to its canonical name, referrals.icann.org.
NS	An NS record or name server record maps a domain name to a list of DNS servers for that domain and are used to create delegations.
SOA	A Start of Authority (SOA) record or start of authority record specifies the DNS server providing authoritative information about an Internet domain.
.	A free standing dot is used to refer to the current domain name.
@	A free standing @ is used to denote the current origin.
()	Parentheses are used to group data that crosses a line boundary. In effect, line terminations are not recognized within parentheses.
;	Semicolon is used to start a comment; the remainder of the line is ignored.

The Start of Authority (SOA) record specifies the time to live. The SOA record has the parameters as Table 3.

Table 3 – SOA records

Record	Description
Serial	The zone serial number, incremented when the zone file is modified, so the slave and secondary name servers know when the zone has been changed and should be reloaded.
Refresh	The number of seconds between update requests from secondary and slave name servers.
Retry	The number of seconds the secondary or slave will wait before retrying when the last attempt has failed.
Expire	The number of seconds a master or slave will wait before considering the data stale if it cannot reach the primary name server.

`Minimum`	Previously used to determine the minimum TTL, this offers negative caching.

1.2.3. Reverse Zone

Reverse zone configuration is to resolve the hostname by IP address. We must introduce the zone to `/etc/named.conf.` The zone name is the opposite order of the network address (or IP address)

```
…
zone "10.0.168.192.in-addr.arpa" in {
       file "master/192.168.0.10.zone";
       type master;
};
```

Next, create the reverse zone file
`/var/lib/named/master/192.168.0.10.zone`

```
$TTL 2D
@                          IN  SOA                srv1.domain1.site.
root.srv1.domain1.site. (
                           2009071401     ; serial
                           3H             ; refresh
                           1H             ; retry
                           1W             ; expiry
                           1D )           ; minimum

              IN      NS      srv1.domainl.site.
              IN      PTR     domain1.site.
10            IN      PTR     srv1.domain1.site.
```

Whenever you changed the configuration, you must restart the service to enable to configuration.

```
# /etc/init.d/named restart
```

Note: If a DNS service is dead, update the update profile wizard in Novell AppArmor.
In [YaST] [Novell AppArmor] [Update Profile Wizard] [Enable repository] [Finish].

1.2.4. Resolver Configuration

The last thing we need to do before running BIND is to set up the local resolver software.

/etc/resolv.conf

```
nameserver 192.168.0.10
search domain1.site
```

If you configure DNS server by DHCP, you also need to reconfigure DHCP server for its clients.

1.2.5. DNS Forwarder

To use the name server of the provider or one already running on your network as the forwarder, enter the corresponding IP address or addresses in the options section under forwarders. The addresses in the followings are just examples. Change these entries according to your own setup.

```
options {
   directory "/var/lib/named";
   forwarders { 10.11.12.13; 10.11.12.14; 192.168.0.1; };
   listen-on port 53 { 127.0.0.1; 192.168.0.10; };
   allow-query { 127/8; 192.168.0.0/24; };
   notify no;
};
```

The options entry is followed by entries for the zone, for localhost, 0.0.127.in-addr.arpa, and the type hint entry under “.”, which should always be present. The corresponding files do not need to be modified and should work as is. Also make sure that each entry is closed with a “;” and that the curly braces are in the correct places. After changing the configuration file `/etc/named.conf` or the zone files, tell BIND to reread them.

1.2.6. DNS Slave

DNS slave servers load zone data from the master server and at intervals specified in the start of authority (SOA) record for each zone. When a zone file is changed, the changes are automatically propagated to the slave servers.

This example is acting as a slave for the `domain2.site`.

```
zone "domain2.site" {
      type slave;
      file "slave/domain2.zone";
      masters {192.168.0.11;};
};
```

After restarting the DNS at slave server, you will find a slave zone file under `/var/lib/named/slave` directory.

1.2.7. Configuration Options

In the master configuration file (`/etc/named.conf`), following options are available at the first part of this file as,

```
options {
        …
}
```

A `directory` specifies the directory where BIND can find the files containing the zone data.

```
directory "/var/lib/named";
```

A `forwarders` specifies the name servers (mostly of the provider) to which DNS requests should forwarded if they cannot be resolved directly.

```
forwarders { 192.0.2.1; 192.0.2.2; };
```

A `forward first` causes DNS requests to be forwarded before an attempt is made to resolve them via the root name servers.

```
forward first;
```

Instead of `forward first`, `forward only` can be written to have all requests forwarded and none sent to the root name servers. This makes sense for firewall configurations.

```
forward only;
```

A listen-on port tells BIND to which network interface and port to listen. The port 53 specification can be left out, as 53 is the default port. If this entry is completely omitted, BIND accepts requests on all interfaces.

```
listen-on port 53 { 127.0.0.1; 192.168.0.1; };
```

A `query-source address` is necessary if a firewall is blocking outgoing DNS requests. This tells BIND to post requests externally from port 53 and not from any of the high ports above 1024.

```
query-source address * port 53;
```

An `allow-query` defines the networks from which clients can post DNS requests. The /24 at the end is an abbreviated expression for the netmask, in this case, 255.255.255.0.

```
allow-query { 127.0.0.1; 192.168.0.0/24; };
```

An `allow-transfer` controls which hosts can request zone transfers. In the example, such requests are completely denied with `!*`. Without this entry, zone transfers can be requested from anywhere without restrictions.

```
allow-transfer { !*; };
```

If `notify` is set to yes (default), notify messages are sent to other name servers when the zone data is changed. Instead of setting a global 'notify' statement in the 'options' section, a separate 'notify' can be added to each zone definition.

```
notify no;
```

1.2.8. Round Robin

A load balancing technique in which balance power is placed in the DNS server instead of a strictly dedicated machine as other load techniques do.

Round robin works on a rotating basis in that one server IP address is handed out, then moves to the back of the list; the next server IP address is handed out, and then it moves to the end of the list; and so on, depending on the number of servers being used. This works in a looping fashion.

Round robin DNS is usually used for balancing the load of geographically distributed Web servers. For example, a company has one domain name and three identical home pages residing on three servers with three different IP addresses. When one user accesses the home page it will be sent to the first IP address. The second user who accesses the home page will be sent to the next IP address, and the third user will be sent to the third IP address. In each case, once the IP address is given out, it goes to the end of the list. The fourth user, therefore, will be sent to the first IP address, and so forth.

Although very easy to implement, round robin DNS has important drawbacks, such as those inherited from the DNS hierarchy itself and TTL times, which causes undesired address caching to be very difficult to manage. Moreover, its simplicity makes those remote servers that go unpredictably down inconsistent in the DNS tables. However, this technique, together with other load balancing and clustering methods, can produce good solutions for some situations.

For example, www.microsoft.com is running at seven web servers.

```
# dig www.microsoft.com +short
toggle.www.ms.akadns.net.
g.www.ms.akadns.net.
lb1.www.ms.akadns.net.
207.46.19.190
207.46.19.254
207.46.192.254
207.46.193.254
```

This is an exmple of making a round robin.

```
; Round Robin
www         IN     A      192.168.0.10
www         IN     A      192.168.0.11
```

1.2.9. Troubleshooting

Check `/var/log/messages` for any error messages as

```
# less /var/log/messages
```

Press “G” to move the bottom of this file. You might search the string “named”

This command always shows the bottom of the file, and then you can monitor.

```
# tail -f /var/log/messages
```

1.3. How to check DNS

1.3.1. Nslookup command

`nslookup` means `name server lookup`, is a network administration command-line tool available for many computer operating systems for querying the Domain Name System (DNS) to obtain domain name or IP address mapping or for any other specific DNS record. It is configured automatically by the contents of the operating system file `resolv.conf`.

`nslookup` operates in interactive or non-interactive mode. If you only want to lookup one record for one domain name, use the noninteractive form. If you plan on doing something more extensive, such as changing name servers or options, use an interactive session.

To start an interactive session, just type nslookup command:

```
# nslookup
> srv1
Server:         192.168.0.10
Address:        192.168.0.10#53

Name:   srv1.domain1.site
Address: 192.168.0.10
> www
Server:         192.168.0.10
Address:        192.168.0.10#53

www.domain1.site canonical name = srv1.domain1.site.
Name:   srv1.domain1.site
Address: 192.168.0.10
> www.domain1.site
Server:         192.168.0.10
Address:        192.168.0.10#53

www.domain1.site canonical name = srv1.domain1.site.
Name:   srv1.domain1.site
Address: 192.168.0.10
> 192.168.0.10
Server:         192.168.0.10
Address:        192.168.0.10#53

10.0.168.192.in-addr.arpa     name = domain1.site.
```

An MX record is used for a mail server. To check the MX record,

```
> set type=mx
> domain1.site
Server:         192.168.0.10
Address:        192.168.0.10#53

domain1.site    mail exchanger = 10 srv1.domain1.site.
> exit
```

For a noninteractive lookup, include the name you are looking up on the command line:

```
# nslookup www.domain1.site
Server:         192.168.0.10
Address:        192.168.0.10#53

www.domain1.site canonical name = srv1.domain1.site.
Name:   srv1.domain1.site
Address: 192.168.0.10
```

1.3.2. Dig command

Dig command is to perform DNS name lookups. Dig is similar to Nslookup but does not have that interactive mode as nslookup.

This output shows the global options that are set.

```
# dig domain1.site

; <<>> DiG 9.3.2 <<>> domain1.site
;; global options:  printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 44439
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 0

;; QUESTION SECTION:
;domain1.site.                IN      A

;; AUTHORITY SECTION:
domain1.site.           86400   IN      SOA     srv1.domain1.site.
 root.srv1.domain1.site. 2007062001 10800 3600 604800 86400

;; Query time: 1 msec
;; SERVER: 192.168.0.10#53(192.168.0.10)
;; WHEN: Sat Jun 16 16:01:01 2007
;; MSG SIZE  rcvd: 76
```

This option shows a list of A records.

```
# dig domain1.site A +answer

; <<>> DiG 9.3.2 <<>> domain1.site A +answer
;; global options:  printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 64462
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 0

;; QUESTION SECTION:
;domain1.site.                  IN      A

;; AUTHORITY SECTION:
domain1.site.          86400   IN      SOA     srv1.domain1.site.
 root.srv1.domain1.site. 2007062001 10800 3600 604800 86400

;; Query time: 0 msec
;; SERVER: 192.168.0.10#53(192.168.0.10)
;; WHEN: Sat Jun 16 16:23:43 2007
;; MSG SIZE  rcvd: 76
```

This option shows MX (mail exchanges) records.

```
# dig domain1.site MX +answer

; <<>> DiG 9.3.2 <<>> domain1.site MX +answer
;; global options:  printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 61516
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 1

;; QUESTION SECTION:
;domain1.site.                  IN      MX

;; ANSWER SECTION:
domain1.site.          172800  IN      MX      10 srv1.domain1.site.

;; AUTHORITY SECTION:
```

```
domain1.site.           172800  IN      NS      srv1.domain1.site.

;; ADDITIONAL SECTION:
srv1.domain1.site.      172800  IN      A       192.168.0.10

;; Query time: 0 msec
;; SERVER: 192.168.0.10#53(192.168.0.10)
;; WHEN: Sat Jun 16 16:23:51 2007
;; MSG SIZE  rcvd: 81
```

This option shows a list of DNS servers authoritative for the domain.

```
# dig domain1.site NS +answer

; <<>> DiG 9.3.2 <<>> domain1.site NS +answer
;; global options:  printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 22413
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; QUESTION SECTION:
;domain1.site.                  IN      NS

;; ANSWER SECTION:
domain1.site.           172800  IN      NS      srv1.domain1.site.

;; ADDITIONAL SECTION:
srv1.domain1.site.      172800  IN      A       192.168.0.10

;; Query time: 1 msec
;; SERVER: 192.168.0.10#53(192.168.0.10)
;; WHEN: Sat Jun 16 16:23:59 2007
;; MSG SIZE  rcvd: 65
```

This option shows all of the above.

```
# dig domain1.site ANY +answer
```

```
; <<>> DiG 9.3.2 <<>> domain1.site ANY +answer
;; global options:  printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 30352
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 0, ADDITIONAL: 1

;; QUESTION SECTION:
;domain1.site.                IN      ANY

;; ANSWER SECTION:
domain1.site.             172800   IN       SOA      srv1.domain1.site.
root.srv1.domain1.site. 2007062001 10800 3600 604800 86400
domain1.site.           172800  IN      MX      10 srv1.domain1.site.
domain1.site.           172800  IN      NS      srv1.domain1.site.

;; ADDITIONAL SECTION:
srv1.domain1.site.      172800  IN      A       192.168.0.10

;; Query time: 1 msec
;; SERVER: 192.168.0.10#53(192.168.0.10)
;; WHEN: Sat Jun 16 16:24:09 2007
;; MSG SIZE  rcvd: 122
```

If you want a quick answer, the +short option can be used.

```
# dig www.domain1.site +short
srv1.domain1.site.
192.168.0.10
```

If you want an answer with “the SOA records in a verbose multi-line format with human-readable comments”, the `+multiline` option can be used.

```
# dig domain1.site +multiline

; <<>> DiG 9.4.1-P1 <<>> domain1.site +multiline
;; global options:  printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 38931
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL:
0

;; QUESTION SECTION:
;domain1.site.       IN A

;; AUTHORITY SECTION:
Domain1.site.       86400 IN SOA srv1.domain1.site.
root.srv1.domain1.site. (
                          2008010202 ; serial
                          10800     ; refresh (3 hours)
                          3600      ; retry (1 hour)
                          604800    ; expire (1 week)
                          86400     ; minimum (1 day)
                          )

;; Query time: 0 msec
;; SERVER: 192.168.0.10#53(192.168.0.10)
;; WHEN: Wed Jan  2 18:22:03 2008
;; MSG SIZE  rcvd: 81
```

Use –x option to lookup the hostname associated with an IP address.

```
# dig -x 192.168.0.10 +short
domain1.site.
```

To use a different nameserver, use @nameserver as,

```
# dig @192.168.0.1 www.google.com
```

To use the search list in `/etc/resolv.conf`, there is a host utility. It uses the search list in `/etc/resolv.conf` file.

```
# host www
www.domain1.site is an alias for srv1.domain1.site.
srv1.domain1.site has address 192.168.0.10
www.domain1.site is an alias for srv1.domain1.site.
www.domain1.site is an alias for srv1.domain1.site.
```

If you want to use the hostname instead of FQDN, use the `+search` option.

```
# dig www +search +short
srv1.domain1.site.
192.168.0.10
```

Exercise 1 – BIND

1. Configure DNS master and slave servers.
2. Configure round robin DNS for web (www) server.

2. NFS Server <Day 2>

2.1. NFS Introduction

The Network File System (NFS) is introduced by Sun Microsystems in 1985. Though NFS was originally implemented as a surrogate file system, it was well designed, stable, and useful as a general file-sharing solution. As a result, most UNIX supplier, Linux distributions have at least minimal support for NFS.

NFS allows computers to mount a disk partition on a remote computer as though it were on a local hard drive. Adopting client/server architecture, NFS enables a fast, seamless sharing of files across a network.

NFS Characteristics are as follows,

- Transport protocol

NFS runs on top of Sun's RPC (Remote Procedure Call) protocol, which defines a system-independent way for processes to communicate over a network. NFS originally used UDP, but now current NFS systems (version 3) supports Linux distributions use TCP as transport layer protocol in addition to the UDP.

- Stateless mounting

A NFS client must explicitly mount an NFS file system before using it, just as a client must mount a file system stored on a local disk. However, because NFS is stateless, the server does not keep track of which clients have mounted each file system. Instead, the server sends to a client a secret “cookie” after a successful mount. It is then sent every time the client makes an NFS request.

- UID, GID

NFS servers rely on the UID &GID given by the NFS client to determine file permission. No password authentication is performed as an authentication. It means that users who can change their UID 0 (root), or whatever UID they want. The server gives the access to the corresponding file. To address this security caution, mount command support **root_squash** option so as to prohibit the access as **root**.

- Daemons

NFS relies on three daemons.

- `portmap`: The RPC port mapper service. It allows NFS client to discover RPC services running on the server. From here it allows the client to find out NFS service.
- `rpc.mountd`: It processes client's mount requests, and validate it.
- `rpc.nfsd`: It is responsible for the file service.

The `rpc.mountd` validates a client's request. Then the client can request file system operations. The `nfsd` handles these requests on the server side. Both `mountd` and `nfsd` should start when the system boots, and remain running.

2.2. NFS Server Configuration

Following RPM packages are required for NFS server. Install by RPM command or YaST.

- `nfsidmap`
- `nfs-kernel-server`

Edit `/etc/exports` file to export file systems. An export simply means the server's filesystem that to make available to clients. Table 4 shows common export options.

Table 4 – NFS export options in the /etc/exports

Option	Description
`ro`	Exports read-only
`rw`	Exports for reading and writing (the default)
`sync`	It ensures that any file updates have been committed to stable storage. This is the default and is safes; that is, least likely to result in data loss in the evento of a server crash.
`async`	User of this option may increase some performance on writing, but is less safe.
`root_squash`	This option prevents super-user identity from propagating from an NFS. The root user usually becomes `nobody`.
`no_root_squash`	The opposite of root_squash. Using this option, root on the client remains as root on the server. Use this option with caution, and offer it only to trusted clients.
`anonuid=xxx`	Specifies the UID to which remote roots should be squashed.

	(default: UID of `nobody`)
`anongid=xxx`	Specifies the GID to which remote roots should be squashed. (default: GID of `nobody`)
`all_squash`	It causes all users to be squashed down to `nobody/nogroup`. You might use this if you are providing a communal export to many users.
`subtree_check`	A filesystem which is readonly, and does not see many file renames should be `subtree_check` option.
`no_subtree_check`	A filesystem which is has lots of file rename, should be exported with `no_subtree_check`.

Check RPC registerd service

```
# rpcinfo -p
```

In the `/etc/exports` file, the clients that may access a given file system are presented in a white space-separated list. Each client is followed immediately by a parenthesized list of comma-separated options. Below is a sample

```
/srv/ftp/           *(ro,root_squash)
/home                192.168.0.0/24(ro,root_squash)
/home/everyone       *(rw,no_root_squash,sync)
```

Restart NFS daemon, and automatically start at boot time.

```
# /etc/init.d/nfsserver restart
# chkconfig nfsserver on
```

The `portmap` is configured to start at boot time at the installation by default.

The `rpcinfo` command shows running RPC-registered service

```
# rpcinfo -p
```

NFS server needs to get three daemons started.

- `portmap`
- `rpc.mountd`
- `rpc.nfsd`

`/etc/init.d/nfsserver` shell script launches **`rpc.mountd`** as well as **`rpc.nfsd`**, so you can execute two shell scripts listed above with ‘start’ argument.

2.2.1. Troubleshooting

Check `/var/log/messages` for any error messages as

```
# less /var/log/messages
```

Press “G” to move the bottom of this file. You might search the string “`nfsd`”

This command always shows the bottom of the file, and then you can monitor.

```
# tail -f /var/log/messages
```

2.3. NFS Client Configuration

Make sure **`portmap`** is running

```
# ps ax | grep portmap
```

By default open SUSE Linux installation, `portmap` daemon starts at boot. It is unlikely that you have to start this daemon by hand.

A `showmount` queries the `rpc.mountd` daemon on a NFS server for information about the state of it. With no options, `showmount` lists the set of clients who are mounting from that host. With option `-e` (`--exports`) shows NFS server’s export list.

```
# showmount -e 192.168.0.10
Export list for 192.168.0.10:
/home/everyone   *
/opt/project         *.subdomain.mydomain.com
/home               192.168.0.0/24
/srv/ftp              *
```

A `mount` command maps the remote directory on the remote host into a directory within local file tree. After mounting, an NFS-mounted filesystem is accessed in the same way as a local file. Below is the example of mount usage.

```
# mount -o ro,rsize=8192 192.168.0.14:/srv/ftp  /mnt/ftp
```

Options specified by `-o` flag, and separated by comma “,”. Table 5 is more details of NFS mount options. For more options, check by `man exports`

Table 5 – NFS mount options

Option	Description
`rw`	Mount the file system read-write (must be exported that way)

`ro`	Mount the file system read-only
`hard`	This is the default option. If the NFS server disconnects or goes down while a process is waiting to access it, the process will hang until the server comes back up.
`soft`	If the NFS server disconnects or goes down, a process trying to access data from the server will time out after a set period of time when this option is on.
`rsize`	The number of bytes of data read at a time from an NFS server. The default is 1024. Using a larger number (such as 8192) will get you better performance on a network that is fast.
`wsize`	The number of bytes of data written at a time to an NFS server. The default is 1024.
`bg`	If the first mount attempt times out, try all subsequent mounts in the background. This option is valuable if you are mounting a slow or sporadically available NFS file system.
`timeo=#`	Sets the time (in tenths of a second) the NFS client will wait for a request to complete. The default value is 7 (0.7 seconds). What happens after a timeout depends on whether you use the hard or soft option.
`retrans=#`	Sets the number of minor timeouts and retransmissions that need to happen before a major timeout occurs.
`retry=#`	Sets how many minutes to continue to retry failed mount requests, where # is replaced by the number of minutes to retry. The default is 10,000 minutes (which is about a week).

Mount at boot time. By placing mount commands in `/etc/fstab`, a remote exported directory is mounted at boot time. The following mount entries mount the file system /srv/ftp from the hosts “192.168.0.1”

```
# filesystem       mountpoint fstype flags              dump fsck
192.168.0.1:/srv/ftp  /mnt/ftp  nfs  soft,rsize=8192,bg  0  0
```

This `mount -a` command mounts all file systems in /etc/fstab, and then `df` command confirm the mount points.

```
# mount -a
# df
```

Exercise 2 – NFS

Configure NFS server, and NFS client, following the textbook.

3. FTP Server (Vsftp) <Day 2-3>

3.1. FTP Introduction

The File Transfer Protocol (FTP) is a software standard for transferring computer files between machines with widely different operating systems. It belongs to the application layer of the Internet protocol suite.

FTP is an 8-bit client-server protocol, capable of handling any type of file without further processing, such as MIME or Uuencode. However, FTP has extremely high latency; that is, the time between beginning the request and starting to receive the required data can be quite long, and a sometimes-lengthy login procedure is required.

FTP runs over TCP. FTP servers by default listen on port 21 for incoming connections from FTP clients. Depending on the transfer mode, the process of setting up the data stream is different.

- **Active mode**: the FTP client opens a random port (> 1023), sends the FTP server the random port number on which it is listening over the control stream and waits for a connection from the FTP server. When the **FTP server initiates the data connection** to the FTP client it binds the source port to port 20 on the FTP server. To use active mode, the client sends a **PORT** command.
- **Passive mode**: The FTP server opens a random port (> 1023), sends the FTP client the server's IP address to connect to and the port on which it is listening over the control stream and **waits for a connection from the FTP client**. In this case the FTP client binds the source port of the connection to a random port greater than 1023. To use passive mode, the client sends the **PASV** command.

While transferring data over the network, several data representations can be used. The two most common transfer modes are:

- ASCII mode
- Binary mode

The two types differ in the way they send the data. When a file is sent using an ASCII-type transfer, the individual letters, numbers, and characters are sent using their ASCII character codes. The receiving machine saves these in a text file in the appropriate format (for example, a Unix machine saves it in a Unix format, a Windows machine saves it in a Windows format). Hence if an ASCII transfer is used it can be assumed plain text is sent, which is stored by the receiving computer in its own format. Translating between text formats entails substituting the end of line and end of file characters used on the source platform with those on the destination platform, e.g. a Windows machine receiving a file from a UNIX machine will replace the line feeds with carriage return-line feed pairs.

The objectives of FTP are:

1. To promote sharing of files (computer programs and/or data).
2. To encourage indirect or implicit use of remote computers.
3. To shield a user from variations in file storage systems among different hosts.
4. To transfer data reliably and efficiently.

Disadvantages are:

1. Passwords and file contents are sent in clear text, allowing eavesdropping which may be unwanted.
2. It is hard to filter active mode FTP traffic on the client side by using a firewall, since the client must open a random port in order to make the connection. This problem is largely resolved by using passive mode FTP.
3. It is possible to tell a server to send to an arbitrary port of a third computer.

Vsftpd is an FTP server, or daemon. The "vs" stands for Very Secure. Recent evidence suggests that vsftpd is also extremely fast (and this is before any explicit performance tuning). In tests against wu-ftpd, vsftpd was always faster, supporting over twice as many users in some tests.

3.2. Vsftpd Configuration

Install vsftpd by YaST, or by RPM command.

Enable the runlevel of vsftpd and start. Make sure that vsftpd starts automatically at boot time.

```
# chkconfig vsftpd on
# /etc/init.d/vsftpd restart
```

To enable writing of file on server, uncomment `/etc/vsftpd.conf` as,

```
write_enable=YES
```

However, anonymous user can not write to the server anyway.

To allow local system users to log in, uncomment,

```
local_enable=YES
```

To set YES, a user can not look outside h(er|is) home directory. To disable this function, it can be NO. However, if there is no reason, keep it YES for security reason.

```
chroot_local_user=YES
```

The `chroot_list_enable` make the specific users to have access to the entire system tree. To all other users their home directory will be shown as root directory (chroot). To enable this, uncomment following lines.

```
chroot_list_enable=YES
chroot_list_file=/etc/vsftpd.chroot_list
```

The file `vsftpd.chroot_list` describes the names of the users that have access to the entire system tree. The file would look like,

```
user1
user2
```

The file `/etc/ftpusers` describes the names of the users that will not log into the system via the FTP server. This usually include as `root`, `uucp`, `news`, and so on, because those users have too much power to be allowed to do as FTP.

3.3. FTP Client

3.3.1. FTP Command

FTP command is available on both Linux and Windows. To login as an anonymous user,

```
# ftp 192.168.250.10
Connected to 192.168.250.10.
220 (vsFTPd 2.0.5)
Name (192.168.250.10:root): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
```

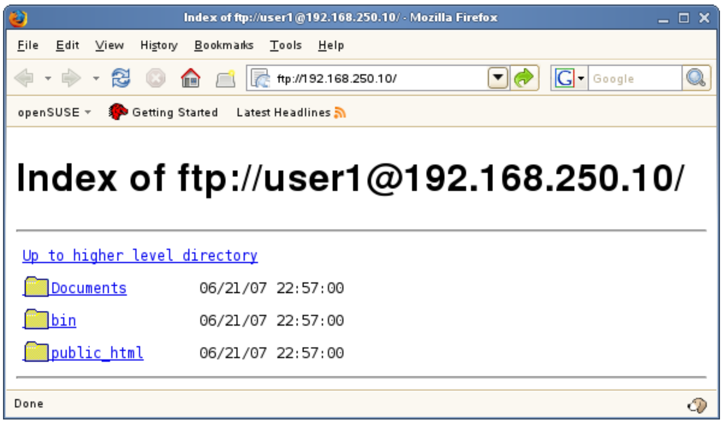
```
ftp>
```

Table 6 – FTP Commands

Command	Description
`> open` *`hostname`*	Connects to the host
`> quit`	Terminates the FTP session
`> dir`	Directory listing on the remote machine
`> ls`	Directory listing on the remote machine
`> pwd`	Print the current remote directory
`> lpwd`	Print the current local directory
`> cd`	Change directory on remote directory
`> lcd`	Change directory on local host
`> binary`	Set binary transfer mode
`> ascii`	Set ascii transfer mode
`> get` *`filename`*	Download a file to local
`> mget *`	Download multiple files to local. [anpqy] stands for “all”, “no”, “prompt off”, “quit”, “yes”
`> put filename`	Upload a file to remote
`> mput *`	Upload multiple files to remote
`> prompt`	Switch the interactice mode on or off.
`> help`	Show help

3.3.2. FTP GUI applications for Linux

- Firefox: Open as `ftp://ftphost.` To log-on by a specific user, use URL as `ftp://user@ftphost.` However, you cannot upload files.

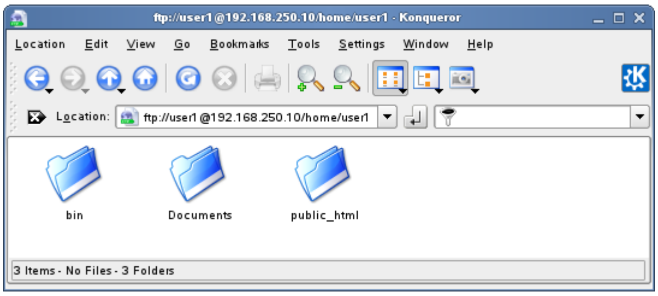


Index of ftp://user1@192.168.250.10/

Up to higher level directory

Documents	06/21/07 22:57:00
bin	06/21/07 22:57:00
public_html	06/21/07 22:57:00

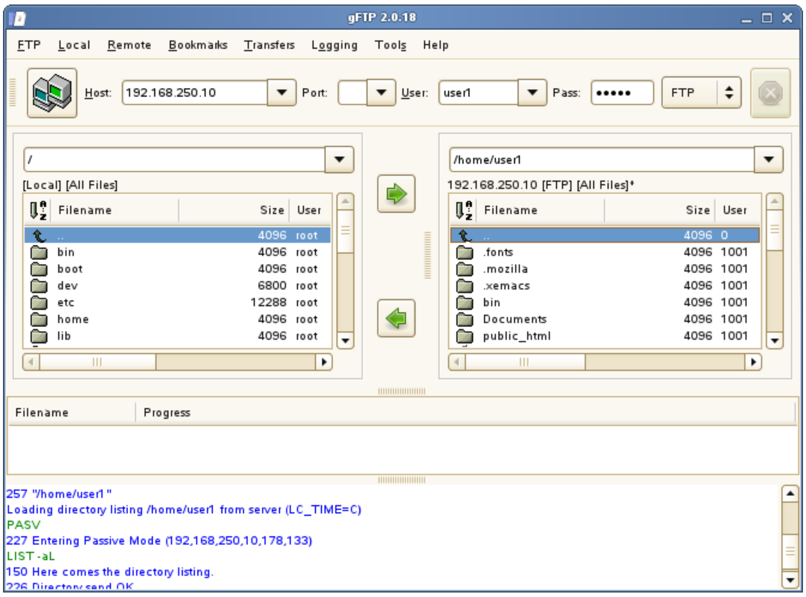
- Konquerror: Open as `ftp://ftphost`. To log-on by a specific user, use URL as `ftp://user@ftphost`. You can upload files by Konquerror.



Location: ftp://user1@192.168.250.10/home/user1

3 Items - No Files - 3 Folders

- Gftp: A tool for Mirroring FTP and FTP servers.



Host: 192.168.250.10 Port: User: user1 Pass: •••••

/

[Local] [All Files]

Filename	Size	User
..	4096	root
bin	4096	root
boot	4096	root
dev	6800	root
etc	12288	root
home	4096	root
lib	4096	root

/home/user1

192.168.250.10 [FTP] [All Files]*

Filename	Size	User
..	4096	0
.fonts	4096	1001
.mozilla	4096	1001
.xemacs	4096	1001
bin	4096	1001
Documents	4096	1001
public_html	4096	1001

Filename	Progress

```
257 "/home/user1 "
Loading directory listing /home/user1 from server (LC_TIME=C)
PASV
227 Entering Passive Mode (192,168,250,10,178,133)
LIST -aL
150 Here comes the directory listing.
226 Directory send OK
```

3.3.3. Wget Command

Wget is a non-interactive download of files from FTP, HTTP, HTTPS protocols. Wget can follow links in HTML pages and create local version of remote web sites, recreating the directory structure of the original site. This is referred to as “recursive downloading”.

Wget has been designed for over slow or unstable network connections. If a download fails due to a network problem, it will keep retrying until the whole file has been retrieved.

Download a single file

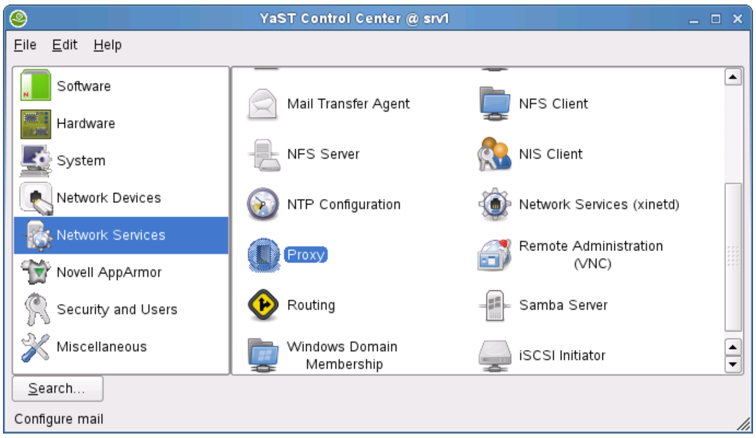
```
$ wget http://www.example.com/program.tar.gz
$ wget ftp://ftp.example.com/program.tar.gz
```

To use wget with a proxy, you must set up an environment variable before using wget. You can set a proxy, by using export command:

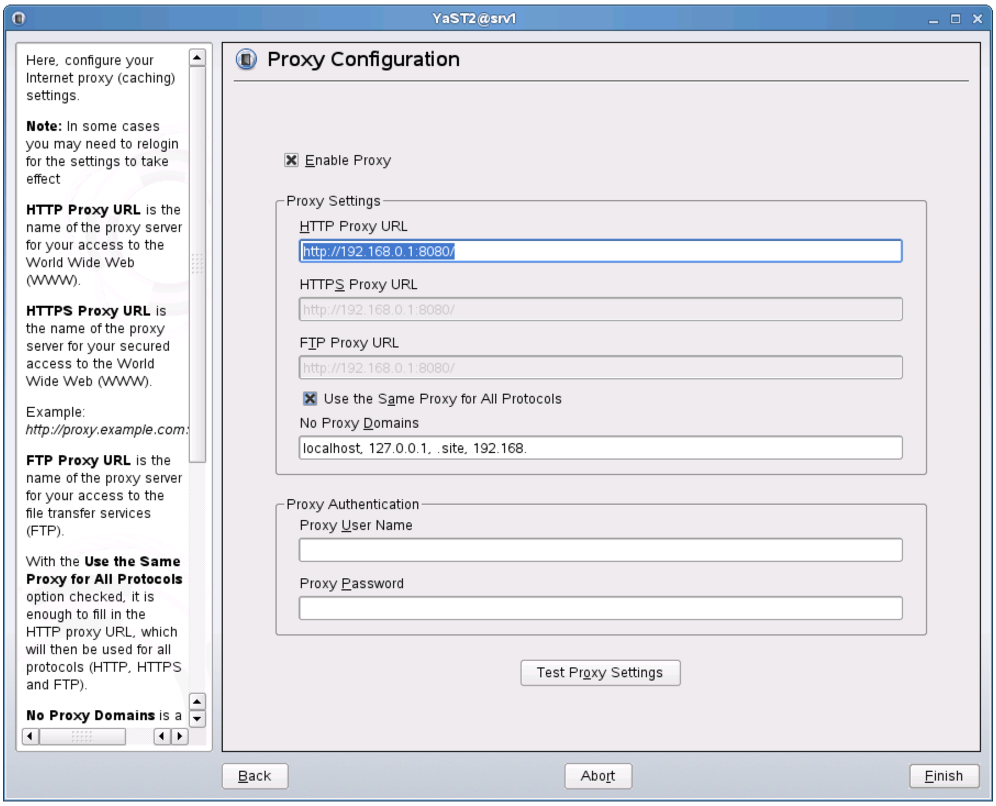
```
export http_proxy="192.168.0.1:8080"
```

You can similarly use *ftp_proxy* to proxy ftp requests and *https_proxy* to proxy https requests.

And also you can set proxy for an environment variable form YaST.



You can specify http, https and ftp proxy for an environment variable from YaST



Here, configure your Internet proxy (caching) settings.

Note: In some cases you may need to relogin for the settings to take effect

HTTP Proxy URL is the name of the proxy server for your access to the World Wide Web (WWW).

HTTPS Proxy URL is the name of the proxy server for your secured access to the World Wide Web (WWW).

Example: *http://proxy.example.com:*

FTP Proxy URL is the name of the proxy server for your access to the file transfer services (FTP).

With the **Use the Same Proxy for All Protocols** option checked, it is enough to fill in the HTTP proxy URL, which will then be used for all protocols (HTTP, HTTPS and FTP).

No Proxy Domains is a

Proxy Configuration

☒ Enable Proxy

Proxy Settings

HTTP Proxy URL: http://192.168.0.1:8080/

HTTPS Proxy URL: http://192.168.0.1:8080/

FTP Proxy URL: http://192.168.0.1:8080/

☒ Use the Same Proxy for All Protocols

No Proxy Domains: localhost, 127.0.0.1, .site, 192.168.

Proxy Authentication

Proxy User Name:

Proxy Password:

The `--no-proxy` option disable to use proxies, even if there is appropriate environment is defined.

```
$ wget --no-proxy ftp://ftp.example.com/program.tar.gz
```

Force wget to resume download. You can use -c option to wget. This is useful when you want to finish up a download started by a previous instance of wget and the net connection was lost.

```
$ wget -c ftp://ftp.example.com/dvd.iso
```

Force wget to download all files in background, and log the activity in a file. `nohup` runs the given command (in this example wget) with hangup signals ignored, so that the command can continue running in the background after you log out.

```
$ nohup wget -c -o /tmp/download.log ftp://ftp.example.com/dvd.iso &
```

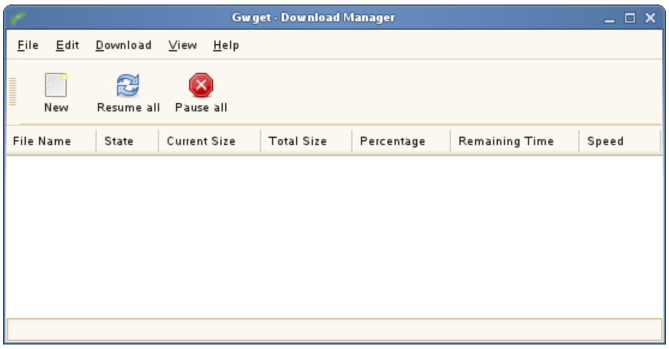
Download all pdf files from the remote FTP server

```
$ wget ftp://ftp.example.com/downloads/*.pdf
```

Download the entire contents of www.example.com

```
$ wget -r -l 0 http://www.example.com/
```

- Gwget: Front-end for wget. This is also called Download Manager at GNOME.



Exercise 3 – Vsftp

1. Install Vsftp, and make chroot configuration enabled as instructed in the text.

2. Allow local users to upload web contents under public_html folder, and verify the updated contents browsing from the other computer.

4. Web Server (Apache) <Day 3-4>

4.1. Apache Introduction

The World Wide Web (the "Web" or "WWW" for short) is a distributed hypertext system that operates over the Internet. Hypertext is viewed using a program called a web browser which retrieves pieces of information, called "documents" or "web pages", from web servers and displays them, typically on a computer monitor. One can then follow hyperlinks on each page to other documents or even send information back to the server to interact with it. The act of following hyperlinks is often called "surfing" or "browsing" the web. Web pages are often arranged in collections of related material called "web sites."

Apache came from the term "A PAtCHy server". It was based on some existing code and a serious of “patch files”. Apache began as the NCSA (National Centre for Supercomputing Applications) HTTP server. After NCSA’s active development stopped, a small group of Web who have ever been involved the HTTP server development, gathered together and made a group ‘Apache group’, then in April 1995 this group released the Apache 0.62. In December 1995, Apache group release version 1.0, which lead the Apache as number 1 HTTP server. Nowadays, Apache is prominent in terms of robustness and stability, in deed; in August 2005 Apache was running on 69% of HTTP servers.

Apache is easily extensive using Dynamic Shared Objects (DSO), which is commonly known as *modules*. Modules extends Apache’s new feature, without recompile. Modules can be loaded or unloaded dynamically.

4.2. Apache Configuration

Make sure that the following requirements are met before trying to set up the Apache Web server:

- The machine's network is configured properly.
- The machine's exact system time is maintained by synchronizing with a time server. This is necessary because parts of the HTTP protocol depend on the correct time.
- The default Web server port (port 80) is opened in the firewall.

[YaST] [Security and Users] [Firewall] [Allow Services] [External Zone] [Service to allow]

[HTTP Server and HTTPs Server]

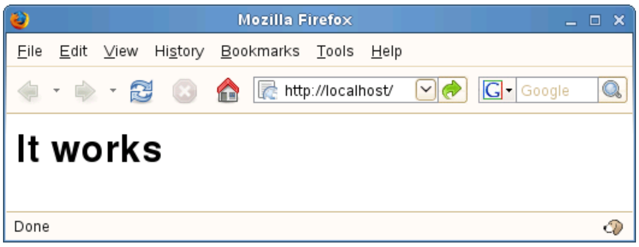
Install apache package as follow if it is not installed,

- `apache2`
- `apache2-example-pages`

Start Apache daemon, and make sure that it is automatically started at boot time.

```
# /etc/init.d/apache2 restart
# chkconfig apache2 on
```

If you have not received error messages when starting Apache, the Web server should be running now. Start a browser and open `http://localhost/`. You should see an Apache test page.



It works

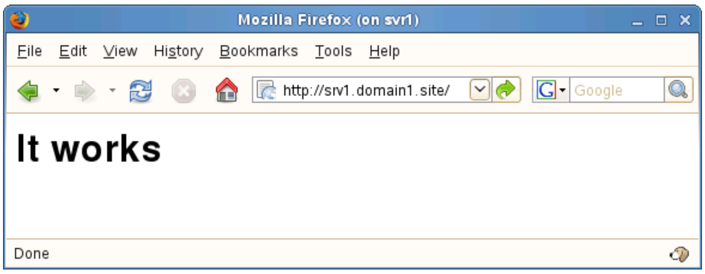
Done

To access the web server from the client with server's domain name, check at Client PC's `/etc/reslov.conf` file.

```
nameserver 192.168.0.10
search domain1.site
```

In client PC's browser, Add your network address and domain name. [Edit] [Preferences] [Advanced] [Network] [Settings] [No Proxy for] [192.168.0.0/16, .site].

Open at `http://srv1.domain1.site.`


Mozilla Firefox (on svr1)
File Edit View History Bookmarks Tools Help
http://srv1.domain1.site/
Google

It works

Done

Apache configuration files can be found in two different locations:

- /etc/sysconfig/apache2
- /etc/apache2/

/etc/sysconfig/apache2 controls some global settings of Apache, like modules to load, additional configuration files to include, flags with which the server should be started, and flags that should be added to the command line. For a general-purpose Web server, the settings in /etc/sysconfig/apache2 should be sufficient for any configuration needs.

/etc/apache2/ hosts all configuration files for Apache. In the following, the purpose of each file is explained. Each file includes several configuration options (also referred to as *directives*).

Table 7 – Overview of Apache2 Configuration Files

File /etc/apache2/	Description
uid.conf	UserID/GroupID to run under
server-tuning.conf	sizing of the server (how many processes to start, ...)
sysconfig.d/loadmodule.conf	load these modules
listen.conf	IP adresses / ports to listen on
mod_log_config.conf	define logging formats
sysconfig.d/global.conf	server-wide general settings
Mod_status.conf	restrict access to mod_status (server monitoring)
mod_info.conf	restrict access to mod_info
mod_usertrack.conf	defaults for cookie-based user tracking
mod_autoindex-defaults.conf	restrict access to mod_info
mod_mime-defaults.conf	defaults for cookie-based user tracking
errors.conf	customize error responses
ssl-global.conf	SSL conf that applies to default server _and all_ virtual hosts
default-server.conf	set up the default server that replies to non-virtual-host requests
mod_userdir.conf	Enable UserDir (if mod_userdir is loaded)
conf.d/apache2-manual.conf	add the docs (if installed)
sysconfig.d/include.conf	your include files (for each file to be included here, put its name into APACHE_INCLUDE_* in /etc/sysconfig/apache2)

`vhosts.d/*.conf`	for each virtual host, place one file here (*.conf is automatically included)

4.2.1. httpd.conf

- DirectoryIndex

It determines for which files Apache should search to complete a URL lacking a file specification. For example, if the client requests the URL http://www.xyz.com/foo/bar and the directory foo/bar containing a file called index.html exists under the `DocumentRoot`, Apache returns this page to the client.

4.2.2. default-server.conf

- DocumentRoot

One basic setting is the DocumentRoot — the directory under which Apache expects web pages the server should deliver. For the default virtual host, it is set to `/srv/www/htdocs`. Normally, this setting does not need to be changed.

- Directory

This directive can be used to set the access permissions and other permissions for a directory. A directive of this kind also exists for the DocumentRoot. The directory name specified here must be changed whenever the DocumentRoot is changed.

- Options

The Options directive controls which server features are available in a particular directory.

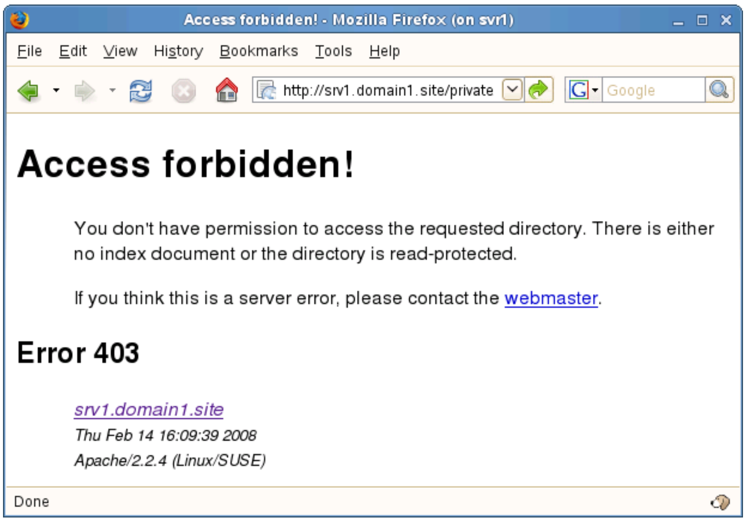
Table 8 – Apache Directory Options

Options	Description
`All`	All options except for MultiViews. This is the default setting.
`ExecCGI`	Execution of CGI scripts using `mod_cgi` is permitted.
`FollowSymLinks`	The server will follow symbolic links in this directory.
`Indexes`	If a URL which maps to a directory is requested, and there is no DirectoryIndex (e.g., index.html) in that directory, then mod_autoindex will return a formatted listing of the directory.
`SymLinksIfOwnerMatch`	The server will only follow symbolic links for which the target file or directory is owned by the same user id as the link.

Example

```
# mkdir /srv/www/htdocs/private
# cd /srv/www/htdocs/private
# echo "My Private Data" > private
```

Open at "`http://srv1.domain1.site/private`"


Access forbidden! - Mozilla Firefox (on svr1)
File Edit View History Bookmarks Tools Help
http://srv1.domain1.site/private
Google
Done

Access forbidden!

You don't have permission to access the requested directory. There is either no index document or the directory is read-protected.

If you think this is a server error, please contact the webmaster.

Error 403

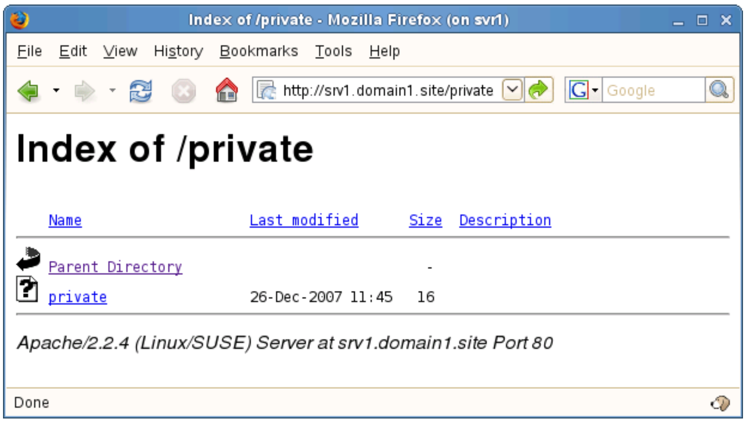
srv1.domain1.site
Thu Feb 14 16:09:39 2008
Apache/2.2.4 (Linux/SUSE)

Edit `/etc/apache2/default-server.conf` as below,

```
…
<Directory "/srv/www/htdocs">
       # Options None
       Options Indexes FollowSymLinks
</Directory>
```

The options indexes will give the directory listing under that directory. Then you need to restart the apache after you have changed your configuration.

Open at `http://srv1.domain1.site/private`.


Index of /private - Mozilla Firefox (on svr1)
File Edit View History Bookmarks Tools Help
http://srv1.domain1.site/private
Google
Done

Index of /private

```
Name                Last modified      Size  Description
Parent Directory                         -
private             26-Dec-2007 11:45   16
```

Apache/2.2.4 (Linux/SUSE) Server at srv1.domain1.site Port 80

- AllowOverride

Every directory Apache delivers documents may contain a file that can override the global access permissions and other settings for this directory. These settings are applied recursively to the current directory and its subdirectories until they are overridden by another such file in a subdirectory. Accordingly, settings specified in such a file are applied globally if it is located in the `DocumentRoot`. Such files normally have the name .htaccess.

Use AllowOverride to determine if the settings specified in local files may override the global settings. Possible values are None, All, and any combination of Options, FileInfo, AuthConfig, and Limit. The meanings of these values are described in detail in the Apache documentation. The (safe) default setting is None.

For example, you can create the file `/srv/www/htdocs/private/.htaccess`

```
Options Indexes
```

And then we need to edit the file `/etc/apache2/default-server.conf` as below.

```
Options None
AllowOverride All
```

Open at "`http://srv1.domain1.site/private`"

- Order

This option determines the order in which the settings for Allow and Deny access permissions are applied. The default setting is:

```
Order allow,deny
```

Accordingly, the access permissions for allowed accesses are applied first, followed by the access permissions for denied accesses. The underlying approach is based on one of the following:

```
allow all
```

Allow every access and define exceptions

```
deny all
```

Deny every access and define exceptions

Example for deny all:

```
Order deny,allow
Deny from all
Allow from example.com
Allow from 10.1.0.0/255.255.0.0
```

Edit the configuration file `/etc/apache2/default-server.conf` to make deny permission to all and allow permission to 192.168.10.0 network.

```
...
<Directory "/srv/www/htdocs/private">
        Options None
        AllowOverride All
        Order deny,allow
        Deny from all
        Allow from 192.168.10.0/255.255.255.0
</Directory>
```

Only client PC's can open the private link, "`http://srv1.domain1.site/private`".

4.2.3. Troubleshooting

Check `/var/log/apache2/error_log` for error messages as

```
# less /var/log/apache2/error_log
```

Press “G” to move the bottom of this file.

This command always shows the bottom of the file, and then you can monitor.

```
# tail -f /var/log/apache2/error_log
```

4.3. Name-based Virtual Host

The term Virtual Host refers to the practice of running more than one web site (such as www.test1.com and www.test2.com) on a single machine. Virtual hosts can be "IP-based", meaning that you have a different IP address for every web site, or "name-based", meaning that you have multiple names running on each IP address. The fact that they are running on the same physical server is not apparent to the end user.

Name-based virtual hosting is usually simpler, since you need only configure your DNS server to map each hostname to the correct IP address and then configure the Apache HTTP Server to recognize the different hostnames. Name-based virtual hosting also eases the demand for scarce IP addresses. Therefore you should use name-based virtual hosting unless there is a specific reason to choose IP-based virtual hosting.

4.3.1. Configuration

Uncomment this line at `listen.conf` to enable the name-based virtul hosting.

```
# NameVirtualHost *:80
NameVirtualHost *:80
```

Create the index files `/srv/www/vhosts/www/index.html`

```
<html><body><h1>Welcome To My Website</h1></body></html>
```

Create index files `/srv/www/vhosts/mail/index.html`

```
<html><body><h1>Welcome To My Email System</h1></body></html>
```

You can copy `vhost.template` and edit for your configuration. The extension should be “`.conf`”. In this example creates two virtual hosts of www and mail to one server. The DNS server of this domain should be configured to map each hostname to the machine.

```
# cd /etc/apache2/vhosts.d
# cp vhost.template www.conf
# cp vhost.template mail.conf
```

`www.conf`

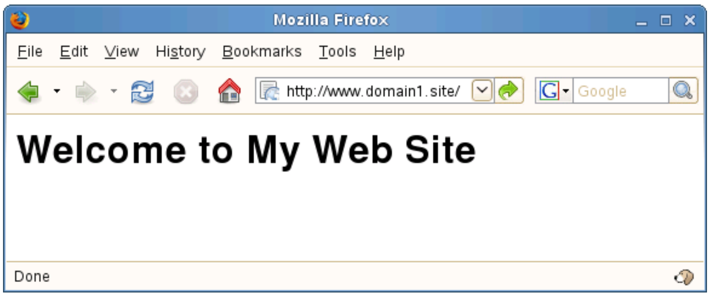
```
<VirtualHost *:80>
    ServerName www.domain1.site
    DocumentRoot /srv/www/vhosts/www

    <Directory "/srv/www/vhosts/www">
        AllowOverride None
        Options Indexes FollowSymLinks
        Order allow,deny
        Allow from all
    </Directory>
</VirtualHost>
```

mail.conf

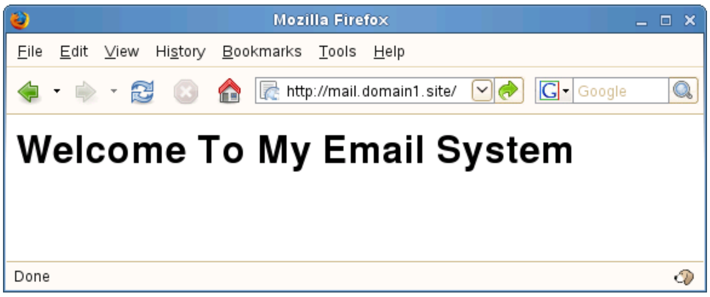
```
<VirtualHost *:80>
    ServerName mail.domain1.site
    DocumentRoot /srv/www/vhosts/mail
    <Directory "/srv/www/vhosts/mail">
        Options Indexes FollowSymLinks
        Order allow,deny
        Allow from all
    </Directory>
</VirtualHost>
```

Note: If you create separate log file for each virtual hosts, you need to rotate log files editing `/etc/logrotate.d/apache2`

Open at `http://www.domain1.site` and `http://mail.doamin1.site` from your client PC and then you can see the content of the index files from each virtual host.



Welcome to My Web Site


Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://mail.domain1.site/
Google
Done

Welcome To My Email System

4.4. User Directory

The user directory is that the client is requesting for data from a user's home directory.

This configuration enables user directories to publish. If a user1 creates a `public_html` at their home directory as `/home/user1/public_html`, the directory is published at `http://host/~user1/`, and then each user can publish their own contents.

For example:

```
# useradd user1 -m -g users
# su - user1
> cd public_html
> echo "This is User1 web page" > index.html
> exit
```

Edit the file `/etc/apache2/vhost.d/www.conf`

```
    <IfModule mod_userdir.c>
        UserDir public_html
        Include /etc/apache2/mod_userdir.conf
        # AliasMatch ^/users/([a-zA-Z0-9-_.]*)/?(.*) /home/$1/public_html/$2
    </IfModule>
```

Open at "`http://www.domain1.site/~user1`"

If you use this directive, the user directory is accessible by `http://host/users/user1/`

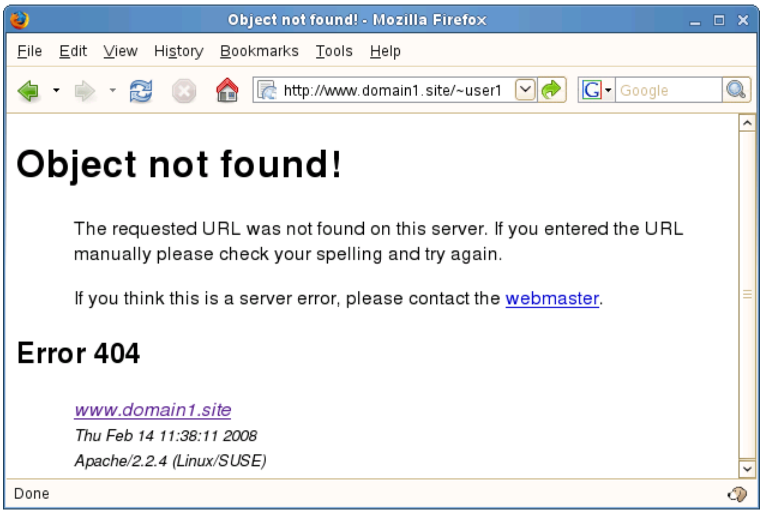
```
        AliasMatch ^/users/([a-zA-Z0-9-_.]*)/?(.*) /home/$1/public_html/$2
```

Open at "`http://www.domain1.site/users/user1`"

Keyword `UserDir disabled` turns off all username directories.

Example:

```
    <IfModule mod_userdir.c>
        UserDir Disabled
        Include /etc/apache2/mod_userdir.conf
        # AliasMatch ^/users/([a-zA-Z0-9-_.]*)/?(.*) /home/$1/public_html/$2
    </IfModule>
```


Object not found! - Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://www.domain1.site/~user1
Google
Done

Object not found!

The requested URL was not found on this server. If you entered the URL manually please check your spelling and try again.

If you think this is a server error, please contact the webmaster.

Error 404

www.domain1.site
Thu Feb 14 11:38:11 2008
Apache/2.2.4 (Linux/SUSE)

4.5. SSI

SSI (Server-side includes) directives are placed in HTML pages, and evaluated on the server while the pages are being served. They let you add dynamically generated content to an existing HTML page, without having to serve the entire page via a CGI program, or other dynamic technology.

Uncomment following lines at `/etc/apache2/mod_mime-defaults.conf`

```
AddType text/html .shtml
AddOutputFilter INCLUDES .shtml
```

This lines control the SSI file extensions.

These options control SSI features.

Table 9 – Apache SSI Directory Options

Options	Description
`Includes`	Server-side includes (SSI) provided by `mod_include` are permitted.
`IncludesNOEXEC`	Server-side includes are permitted, but the `#exec cmd` and

	#exec cgi are disabled. It is still possible to #include virtual CGI scripts from ScriptAliased directories.

We first create the index file under admin if there is no matching virtual host exist this file will be displayed.

Create the file /srv/www/vhosts/admin/index.html for admin user.

```
<html><body>This is Admin Page</body></html>
```

For example, this will enable the SSI to a directory.

Create the file /etc/apache2/vhosts.d/admin.conf.

```
<VirtualHost *:80>
   ServerName admin.domain1.site
   DocumentRoot /srv/www/vhosts/admin

   <Directory "/srv/www/vhosts/admin">
      AllowOverride None
      Options Indexes FollowSymLinks
      Options +Includes
      Order allow,deny
      Allow from all
   </Directory>
</VirtualHost>
```

This is an example of html file with SSI. The file extension should be .shtml

Create the file /srv/www/vhosts/admin/ssi.shtml as below.

```
<html>
<head><title>SSI</title></head>
<body>
<!--#include virtual="header.html" -->
<p>Contents</p>
<hr></hr>
<!--#include virtual="footer.html" -->
</body>
</html>
```

You need to create header.html and footer.html as below.

Create the file `/srv/www/vhosts/admin/header.html`

```
<html><body>SSL Header "Admin Page"</body></html>
```

Create the file `/srv/www/vhosts/admin/footer.html`

```
<html><body>SSL Footer "admin@domain1.site"</body></html>
```

This html will include both `header.html` and `footer.html`.

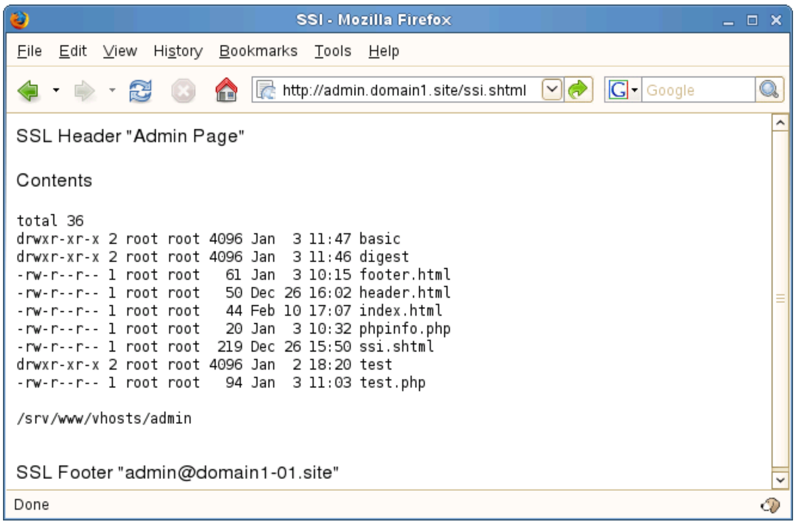
Table 10 – SSI commands

SSI command	Description
`<!--#include virtual="file.html" -->`	Inserts the file.
`<!--#exec cmd="command" -->`	Executes a shell or command
`<!--#exec cgi="command" -->`	Executes a CGI script
`<!--#printenv -->`	Display all current variables.

This example is to execute commands in a HTML.

```
<pre>
<!--#exec cmd="ls -l" -->
<!--#exec cmd="pwd" -->
</pre>
```

Open at http://admin.domain1.site/ssi.shtml.



SSI - Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://admin.domain1.site/ssi.shtml
Google
Done

SSL Header "Admin Page"

Contents

```
total 36
drwxr-xr-x 2 root root 4096 Jan  3 11:47 basic
drwxr-xr-x 2 root root 4096 Jan  3 11:46 digest
-rw-r--r-- 1 root root   61 Jan  3 10:15 footer.html
-rw-r--r-- 1 root root   50 Dec 26 16:02 header.html
-rw-r--r-- 1 root root   44 Feb 10 17:07 index.html
-rw-r--r-- 1 root root   20 Jan  3 10:32 phpinfo.php
-rw-r--r-- 1 root root  219 Dec 26 15:50 ssi.shtml
drwxr-xr-x 2 root root 4096 Jan  2 18:20 test
-rw-r--r-- 1 root root   94 Jan  3 11:03 test.php

/srv/www/vhosts/admin
```

SSL Footer "admin@domain1-01.site"

4.6. CGI

Common Gateway Interface (CGI) is an important World Wide Web technology that enables a client web browser to request data from a program executed on the Web server. CGI specifies a standard for passing data between the client and the program.

The programming language Perl is well known as a language used for CGI, but one of the points of CGI is to be language-neutral. The Web server does not need to know anything about the language in question.

FastCGI applications are very fast because they're persistent. There is no per-request startup and initialization overhead.

Install the following modules by YaST.

- `apache2-mod_perl`
- `apache2-mod_fcgid by YaST.`

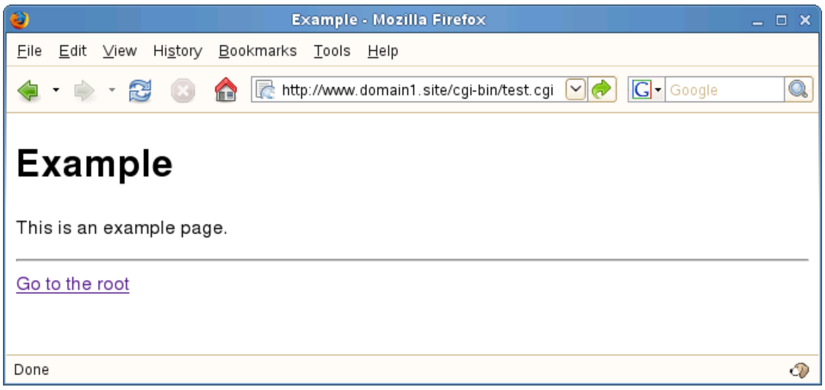
This is a simple example of CGI made by Perl. Creat as `/srv/www/cgi-bin/test.cgi`

```
#!/usr/bin/perl
use CGI ':standard';
print header;
print start_html('Example'),
    h1('Example'),
    p,
    "This is an example page.",
    p,
    hr;
print a({href=>'/'},'Go to the root');
print end_html;
```

Change the file permission to be executed by the users.

```
# chmod 755 test.cgi
```

Open at `http://www.domain1.site/cgi-bin/test.cgi.`


Example - Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://www.domain1.site/cgi-bin/test.cgi
Google
Done

Example

This is an example page.

Go to the root

CGI script works at `ScriptAliased` as `/srv/www/cgi-bin` directory. For using cgi extension outside of the directory, you need to modify `mod_mime-defaults.conf` and add following lines.

```
…
AddHandler cgi-script .cgi .pl
```

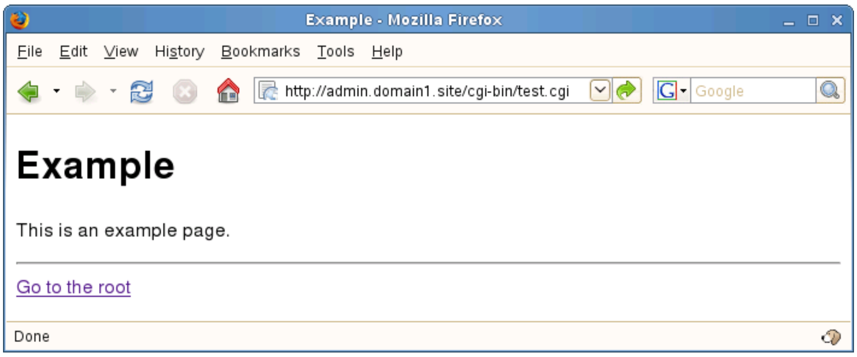
You will also need to add "ExecCGI" to the "Options" directive. For example,

Edit `/etc/apache2/vhosts.d/admin.conf`

```
ScriptAlias /cgi-bin/ "/srv/www/vhosts/admin/test/"

<Directory "/srv/www/vhosts/admin/test">
      AllowOverride None
      Options Indexes FollowSymLinks
      Options +ExecCGI
      Order allow,deny
      Allow from all
   </Directory>
</Directory>
```

```
# mkdir /srv/www/vhosts/admin/test
# cp /srv/www/cgi-bin/test.cgi /srv/www/vhosts/admin/test/
# rcapache2 restart
```

`Open at http://admin.domain1.site/test/test.cgi.`


Example - Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://admin.domain1.site/cgi-bin/test.cgi
Google
Done

Example

This is an example page.

Go to the root

4.7. PHP

PHP (a recursive acronym for "PHP: Hypertext Preprocessor") is a widely-used open-source programming language primarily for server-side applications and developing dynamic web content. The PHP model can be seen as an alternative to Microsoft's ASP/VBScript/JScript system, Macromedia's ColdFusion system, Sun Microsystems' JSP/Java system, and to the CGI/Perl system.

PHP's ease of use and similarity with the most common structured programming languages – most notably C and Perl (and from version 5, Java) – allows most experienced programmers to start developing complex applications with a minimal learning curve. It also enables experienced developers to get involved with dynamic web content applications without having to learn a whole new set of functions and practices.

The Linux, Apache, MySQL, PHP (LAMP) architecture has become very popular in the Web industry as a way of deploying inexpensive, reliable, scalable, secure web applications.

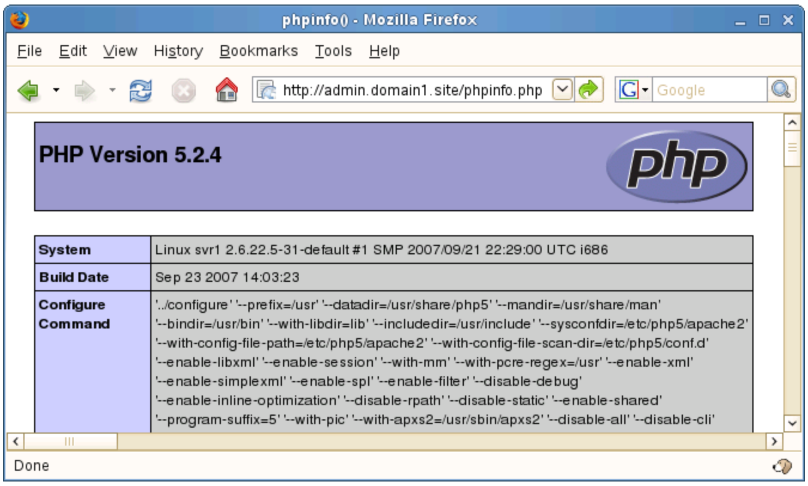
For PHP to work, install `php5` and, `apache2-mod_php5` for Apache. You may install other php modules for your necessity as database connectivity. Install the following package by YaST

- php5
- apache2-mod_php5

To test PHP, create a file named as `/srv/www/vhosts/admin/phpinfo.php` as,

```
<?php phpinfo(); ?>
```

You should see a page full of information about your Apache and PHP installation. If you are prompted to download the file, check the appropriate PHP installation.


phpinfo() - Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://admin.domain1.site/phpinfo.php
Google
php
Done

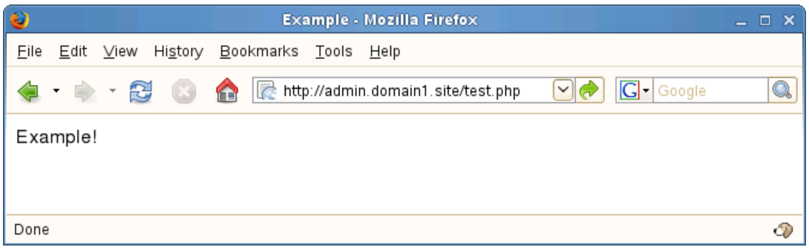
PHP Version 5.2.4

System	Linux svr1 2.6.22.5-31-default #1 SMP 2007/09/21 22:29:00 UTC i686
Build Date	Sep 23 2007 14:03:23
Configure Command	'./configure' '--prefix=/usr' '--datadir=/usr/share/php5' '--mandir=/usr/share/man' '--bindir=/usr/bin' '--with-libdir=lib' '--includedir=/usr/include' '--sysconfdir=/etc/php5/apache2' '--with-config-file-path=/etc/php5/apache2' '--with-config-file-scan-dir=/etc/php5/conf.d' '--enable-libxml' '--enable-session' '--with-mm' '--with-pcre-regex=/usr' '--enable-xml' '--enable-simplexml' '--enable-spl' '--enable-filter' '--disable-debug' '--enable-inline-optimization' '--disable-rpath' '--disable-static' '--enable-shared' '--program-suffix=5' '--with-pic' '--with-apxs2=/usr/sbin/apxs2' '--disable-all' '--disable-cli'

Create `/srv/www/vhosts/admin/test.php` and this is an example of PHP .

```
<html>
<head><title>Example</title></head>
<body>
<?php
echo "Example!";
?>
</body>
</html>
```

Open at `http://admin.doamin1.site/test.php`.


Example - Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://admin.domain1.site/test.php
Google
Done

Example!

4.8. Basic Authentication

As the name implies, basic authentication is the simplest method of authentication and for a long time was the most common authentication method used. However, other methods of authentication have recently passed basic in common usage. The issue of using basic authentication is that your password is sent across the network in the clear.

There are two configuration steps which you must complete in order to protect a resource using basic authentication.

- Create a password file
- Set the configuration to use this password file

Create the index file for Basic Authentication

```
# mkdir /srv/www/vhosts/admin/basic
# cd /srv/www/vhosts/admin/basic
# echo "Basic Authentication Succeed" > index.html
```

Edit the configuration file.

```
<Directory /srv/www/vhosts/admin/basic/>
      AuthType Basic
      AuthUserFile /srv/www/.htpasswd
      AuthName "Private1"
      require valid-user
      Order deny,allow
      Deny from all
      Allow from 127.0.0.1 192.168.0.10 192.168.10.0/24
</Directory>
```

Create `.htpasswd` file, and then add a users.

```
# touch /srv/www/.htpasswd
# htpasswd2 /srv/www/.htpasswd user1
New password: user1
Re-type new password: user1
Adding password for user user1
```

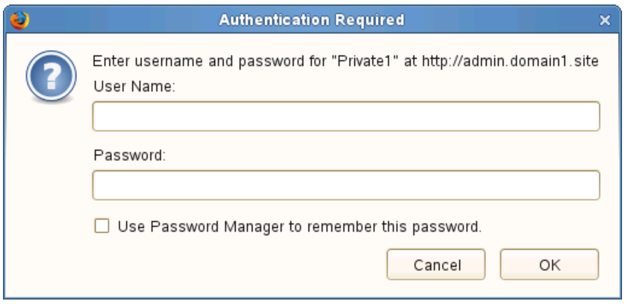
```
# htpasswd2 /srv/www/.htpasswd user2
New password: user2
Re-type new password: user2
Adding password for user user2
```

You can check your created user name and password in `.htpasswd` files.

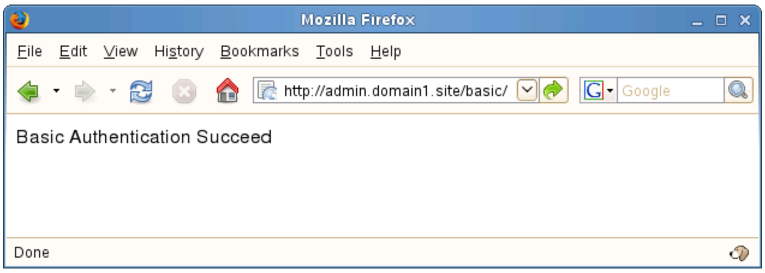
```
# cat /srv/www/.htpasswd
```

```
user1:IpNr/u8ySg1FI
user2:koSBj8dTBQkyI
```

Open at `http://admin.domain1.site/basic/`


Authentication Required
Enter username and password for "Private1" at http://admin.domain1.site
User Name:
Password:
□ Use Password Manager to remember this password.
Cancel
OK

The phrase "Private1" will be displayed in the password pop-up box, where the user will have to type their credentials.


Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://admin.domain1.site/basic/
Google
Done

Basic Authentication Succeed

4.9. Digest Authentication

Addressing one of the security issue of basic authentication, digest authentication provides an alternate method for protecting your web content.

Using digest authentication, your password is never sent across the network in the clear, but is always transmitted as an MD5 digest of the user's password. In this way, the password cannot be determined by sniffing network traffic.

The steps for configuring your server for digest authentication are very similar for those for basic authentication.

- Add auth_digest module
- Set the configuration to use this password file
- Create the password file

To add a module called auth_digest, use `a2enmod` command, as

```
# a2enmod auth_digest
# a2enmod -l
actions  alias  auth_basic  authn_file  authz_host  authz_groupfile
authz_default authz_user authn_dbm autoindex cgi dir env expires include
log_config mime negotiation setenvif ssl suexec userdir php5 fcgid perl
auth_digest
```

This command actually edits `/etc/sysconfig/apache2`

Create the index file for digest authentication:

```
# cd /srv/www/vhosts/admin
# mkdir digest
# cd digest
# echo "Digest Authentication Succeed" > index.html
```

The following example defines an authentication realm called "Private1". The password file will be used to verify the user's identity.

```
<Directory /srv/www/vhosts/admin/digest/>
        AuthType Digest
        AuthName "Private1"
        AuthUserFile /srv/www/.htdigest
        Require valid-user
        Order deny,allow
        Deny from all
        Allow from 127.0.0.1 192.168.0.10 192.168.10.0/24
</Directory>
```

Create .htdigest file, and then add users.

```
# touch /srv/www/.htdigest
# htdigest2 /srv/www/.htdigest "Private1" user1
Adding password for user1 in realm Private1.
New password:user1
Re-type new password:user1
```

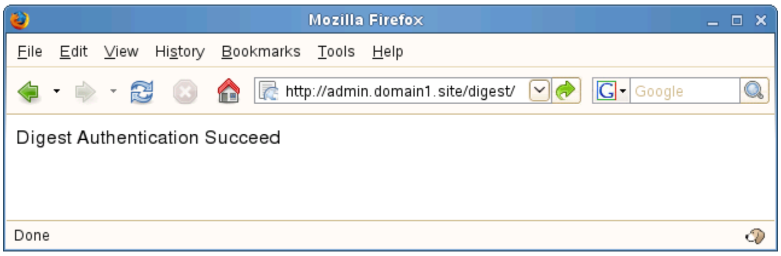
```
# htdigest2 /srv/www/.htdigest "Private1" user2
Adding user user2 in realm Private1
New password: user2
```

```
Re-type new password: user2
```

You can check the user and password as follow.

```
# cat /srv/www/.htdigest
user1:Private1:703b7a15109fd140da8609f9cf2caa3b
user2:Private1:b6a938aff0b49bdbded1463b0e389b8d
```

Open with `http://admin.domain1.site/digest/`


Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://admin.domain1.site/digest/
Google
Done

Digest Authentication Succeed

4.10. SSL/TLS

Secure Sockets Layer (SSL) is a cryptographic protocol to provide secure communications on the Internet. These protocols provide endpoint authentication and communications privacy over the Internet using cryptography. In typical use, only the server is authenticated (i.e. its identity is ensured) while the client remains unauthenticated; mutual authentication requires PKI deployment to clients. The protocols allow client/server applications to communicate in a way designed to prevent eavesdropping, tampering, and message forgery.

The key to this system is the SSL/TLS protocol. It operates between the TCP layer and the HTTP application layer. TLSv1 is the IETF standard implementation, based on SSLv3. TLS stands for Transport Layer Security.

To enabling SSL on Apache, edit

SSL does not run with Apache at openSUSE. So you need to change the option of Apache at `/etc/sysconfig/apache2`.

```
APACHE_SERVER_FLAGS=" -D SSL"
```

Make sure that you also have ssl module loaded. Depending on the environment, you might not have ssl here.

```
APACHE_MODULES="actions alias auth_basic authn_file authz_host authz_groupfile authz_defau
```

```
lt authz_user authn_dbm autoindex cgi dir env expires include log_config mime negotiation
setenvif ssl suexec userdir php5 fcgid perl auth_digest"
```

You also need following openssl packages.

- libopenssl-devel
- openssl
- openssl-doc

4.10.1. Setup your own CA (Certificate Authority)

First, your DNS configuration must be correct (hostname=FQDN, PTR records, etc.)

In order to run a secure (SSL/TLS encrypted) web server, you have to have a private key and a certificate for the server. For a commercial web site, you will probably want to purchase a certificate signed by a well-known root CA. For Intranet or special-purpose uses like this, you can be your own CA. This is done with the OpenSSL tools.

We will make a directory for the certs and keys:

```
# mkdir /usr/local/ca
# chmod 770 /usr/local/ca
# cd /usr/local/ca
```

We will make a private CA key and a private CA X.509 certificate.

```
# openssl genrsa -des3 -out my-ca.key 2048
Enter pass phrase for my-ca.key:mycakey
Verifying - Enter pass phrase for my-ca.key:mycakey
# openssl req -new -x509 -days 3650 -key my-ca.key -out my-ca.crt
Enter pass phrase for my-ca.key:mycakey
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) [AU]:MM
```

```
State or Province Name (full name) [Some-State]:Yangon
Locality Name (eg, city) []:Hlaing
Organization Name (eg, company) [Internet Widgits Pty Ltd]:ICTTI
Organizational Unit Name (eg, section) []:Certificate Authority
Common Name (eg, YOUR name) []:ICTTI CA
Email Address []:root@domain1.site
# openssl x509 -in my-ca.crt -text -noout
```

The first OpenSSL command makes the key. The second command makes the X.509 certificate with a 10 years lifetime. The third command lets you view the completed certificate.

4.10.2. Make a key and a certificate for the web server

We have to make an X.509 certificate and corresponding private key for the web server. Rather than creating a certificate directly, we will create a key and a certificate request, and then sign the certificate request with the CA key we made previously. You can make keys for multiple web servers this way. One thing to note is that SSL/TLS private keys for web servers need to be either 512 or 1024 bits. Any other key size may be incompatible with certain browsers.

```
# openssl genrsa -des3 -out server.key 1024
Generating RSA private key, 1024 bit long modulus
…
e is 65537 (0x10001)
Enter pass phrase for server.key:serverkey
Verifying - Enter pass phrase for server.key:serverkey
# openssl req -new -key server.key -out server.csr
Enter pass phrase for server.key:serverkey
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) [AU]:MM
```

```
State or Province Name (full name) [Some-State]:Yangon
Locality Name (eg, city) []:Hlaing
Organization Name (eg, company) [Internet Widgits Pty Ltd]:ICTTI
Organizational Unit Name (eg, section) []:Certificate Authority
Common Name (eg, YOUR name) []:www.domain1.site
Email Address []:root@domain1.site

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
```

Make sure that your common name is the same as the FQDN that your clients will use when connecting to your site.

As above configuration, you need to type pass phrase every time starting SSL. Moveover SSL does not start automatically in a case of a power failure. So remove pass phrase from server.key to avoid such a problem.

```
# cp server.key server.key.bak
# openssl rsa -in server.key.bak -out server.key
Enter pass phrase for server.key.bak:serverkey
writing RSA key
```

Create a Server Certificate (server.crt)

```
# openssl x509 -req -in server.csr -out server.crt -sha1 -CA my-ca.crt
-CAkey my-ca.key -CAcreateserial -days 365
Signature ok
subject=/C=MM/ST=Yangon/L=Hlaing/O=ICTTI/OU=Certificate
Authority/CN=www.domain1.site/emailAddress=root@domain1.site
Getting CA Private Key
Enter pass phrase for my-ca.key:mycakey
# openssl x509 -in server.crt -text -noout
…
```

We need to move the new keys and certs into the proper directories

```
# chmod 400 *.key
# cp server.crt /etc/apache2/ssl.crt/server.crt
# cp server.key /etc/apache2/ssl.key/server.key
```

4.10.3. Apache SSL Configuration

SSL configuration files are under `/etc/apache2/vhosts.d` for openSUSE. You need to create `vhost_ssl.conf`

```
# cd /etc/apache2/vhosts.d/
# cp vhost-ssl.template www-ssl.conf
```

Modify the `DocumentRoot`, `ServerName`, and `Directory` directives to work for the virtual host.

```
<IfDefine SSL>
<IfDefine !NOSSL>
<VirtualHost *:443>
        ServerName www.domain1.site:443
        DocumentRoot /srv/www/vhosts/www
        <Directory "/srv/www/vhosts/www">
            AllowOverride None
            Options all
            Order allow,deny
            Allow from all
        </Directory>
        SSLEngine on
        SSLCipherSuite ALL:!ADH:!EXPORT56:RC4+RSA:+HIGH:+MEDIUM:+LOW:+SSLv2:+EXP:+eNULL
        SSLCertificateFile /etc/apache2/ssl.crt/server.crt
        SSLCertificateKeyFile /etc/apache2/ssl.key/server.key
        <Files ~ "\.(cgi|shtml|phtml|php3?)$">
            SSLOptions +StdEnvVars
        </Files>
        SetEnvIf User-Agent ".*MSIE.*" \
                 nokeepalive ssl-unclean-shutdown \
                 downgrade-1.0 force-response-1.0
</VirtualHost>
</IfDefine>
</IfDefine>
```

Note that name-based virtual hosts should not be used with SSL. You will get error.

Restart the Apache

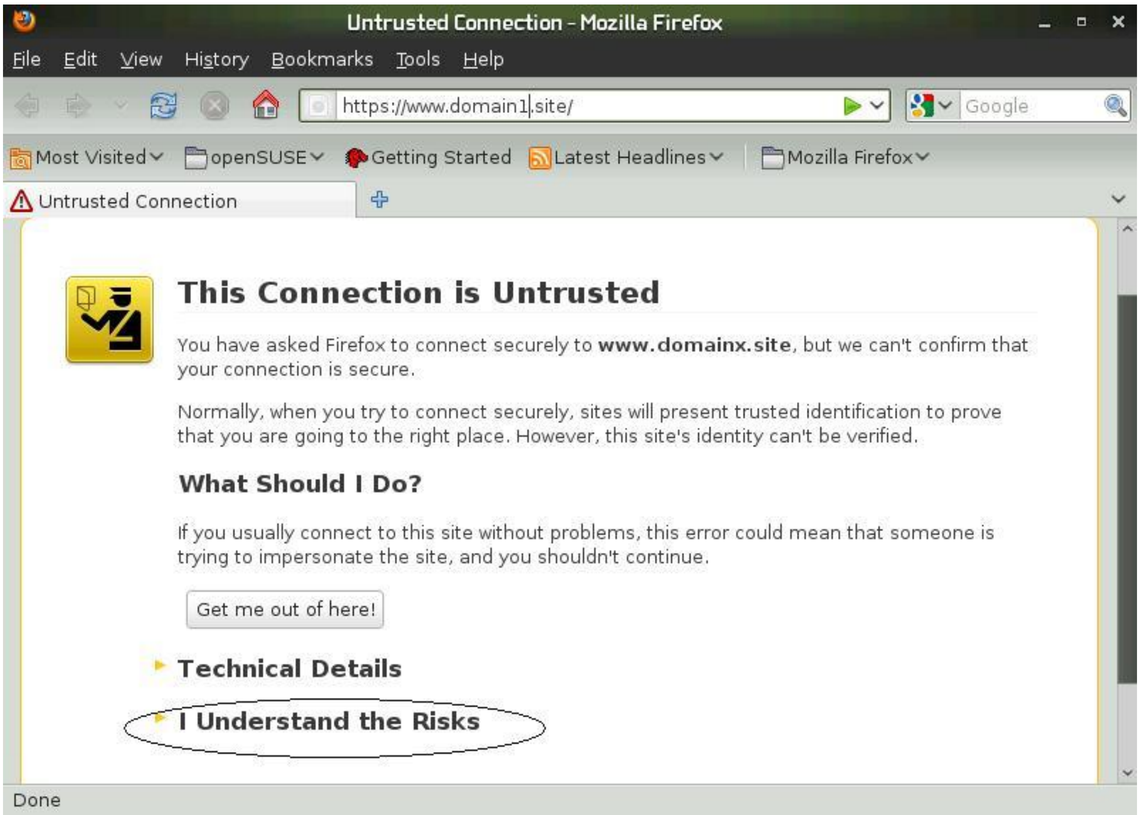
```
# /etc/init.d/apache2 restart
```

Make sure that the web server is now listening on the SSL/TLS port, TCP port 443:

```
# netstat -tna
tcp   0    0 :::443              :::*                LISTEN
```

Now you are able to access `https://www.domain1.site/`.

At the first time, you will see the screen as below. You can examine the certificate by “I Understand the Risks” button, and then select “Add Exception” and then select “Confirm Security Exception” button and click “OK”.



This Connection is Untrusted

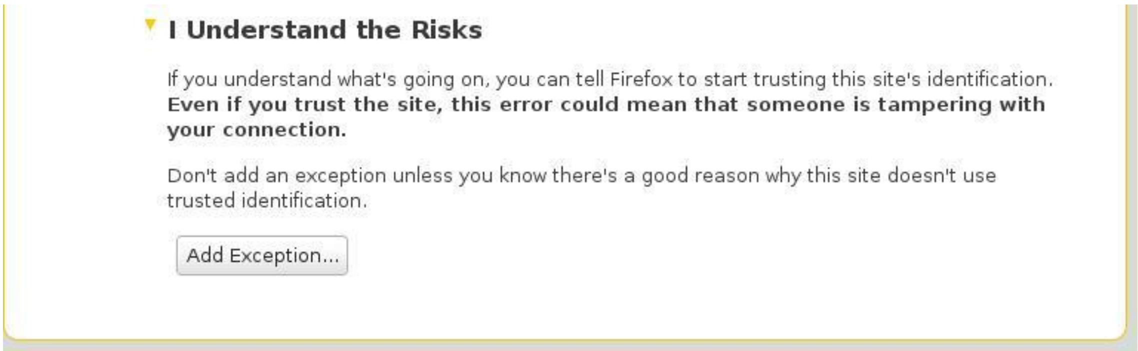
You have asked Firefox to connect securely to **www.domainx.site**, but we can't confirm that your connection is secure.

Normally, when you try to connect securely, sites will present trusted identification to prove that you are going to the right place. However, this site's identity can't be verified.

What Should I Do?

If you usually connect to this site without problems, this error could mean that someone is trying to impersonate the site, and you shouldn't continue.

Select “I Understand the Risks” and “Add Exception”.

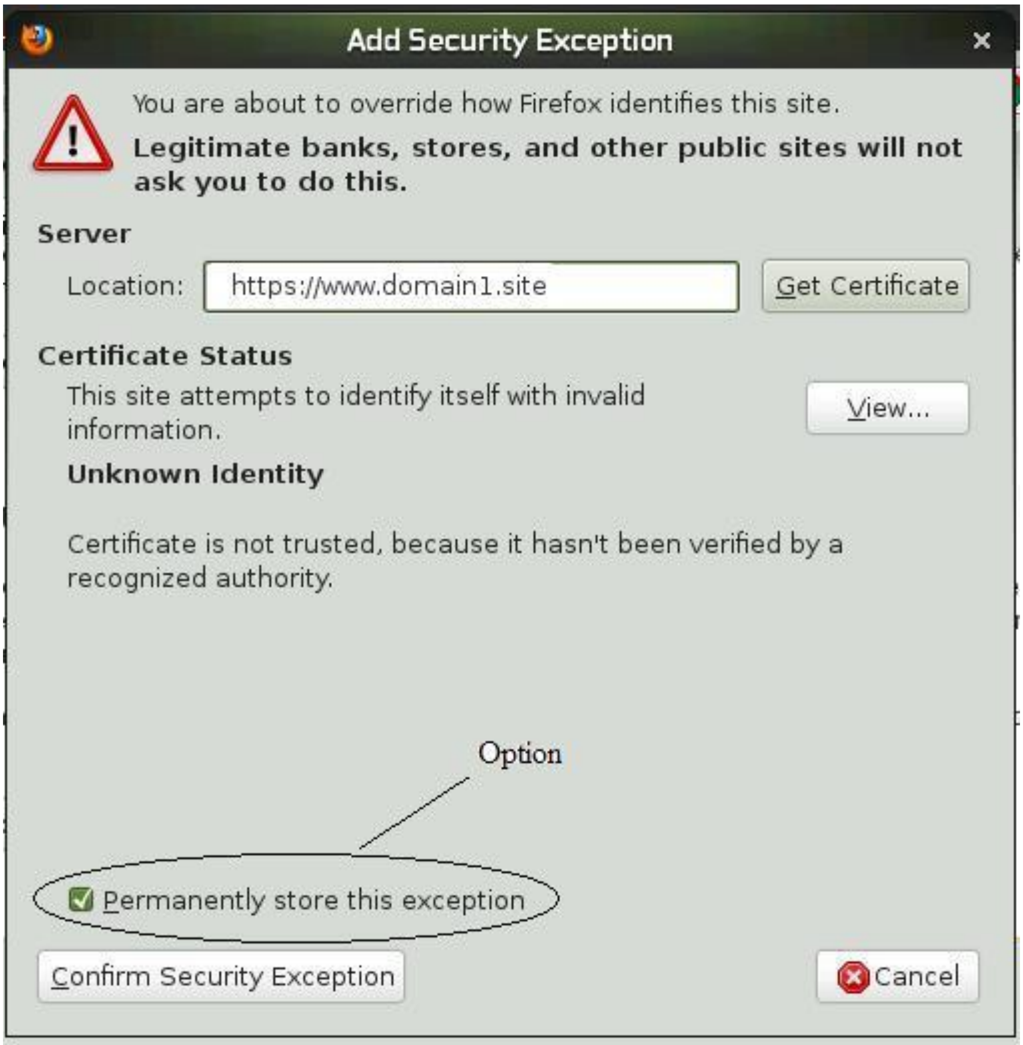


I Understand the Risks

If you understand what's going on, you can tell Firefox to start trusting this site's identification. **Even if you trust the site, this error could mean that someone is tampering with your connection.**

Don't add an exception unless you know there's a good reason why this site doesn't use trusted identification.

And choose “Confirm Security Exception”.



Add Security Exception

You are about to override how Firefox identifies this site.

Legitimate banks, stores, and other public sites will not ask you to do this.

Server

Location: https://www.domain1.site

Certificate Status

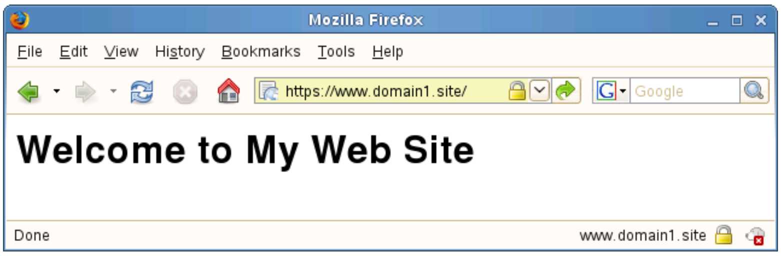
This site attempts to identify itself with invalid information.

Unknown Identity

Certificate is not trusted, because it hasn't been verified by a recognized authority.

☑ Permanently store this exception

You will see the SSL/TLS page as below.


Mozilla Firefox
File Edit View History Bookmarks Tools Help
https://www.domain1.site/
Google

Welcome to My Web Site

Exercise 4 – Apache

1. Make your own simple welcome page at document root and user directory and browse from the other computers.
2. Configure name-based virtual host.
3. Configure SSI.
4. Practice CGI using an example in the text
5. Practice PHP using an example in the text
6. Configure Basic Authentication
7. Configure Digest Authentication
8. Configure SSL

5. Proxy Server (Squid) <Day 5-7>

5.1. Squid Introduction

Squid is a popular open source Proxy server and web cache. It has a variety of uses, from speeding up a web server by caching repeated requests, to caching web, DNS, and other network lookups for a group of people sharing network resources.

Caching is a way to store requested Internet objects (i.e., data available via the HTTP, FTP) on a system closer to the requesting site. Web browsers can then use the local Squid cache as a proxy HTTP server, reducing access time as well as bandwidth consumption. This is often useful for ISPs to increase speed to their customers, and LANs that share an Internet connection.

There are two methods that automatically clients use the proxy without browser's configuration.

- WPAD: It configures browser's proxy setting automatically (application level)
- Transparent Proxy: It intercepts web requests to the proxy automatically (transport level)

The Web Proxy Auto Discovery (WPAD) Protocol is a method used by web browsers to locate a Proxy Auto Config (PAC) file automatically.

The Transparent Proxy is that all outgoing HTTP requests are intercepted by a proxy and all responses are cached at transport layer level. This is configured at a router or a firewall which is a gateway to the Internet.

5.2. Squid Configuration

5.2.1. Installation

Currently, there are two packages available for Squid as.

- `squid3`
- `squid-beta`

The Beta version is still not supported by many tools, so install the stable version.

```
# rpm -ihv squid-3.0.STABLE10-2.11.i586.rpm
```

Before you make any changes, backup the squid configuration file.

```
# cp /etc/init.d/squid /etc/init.d/squidbk
```

If you change the stop option of Squid, you can quickly stop the Squid. Edit `/etc/init.d/squid`

```
…
         # $SQUID_BIN -k shutdown
         $SQUID_BIN -k interrupt
…
```

- `-k shutdown`: Wait all active sessions to close, and then stop
- `-k interrupt`: Stop immediately without waiting active sessions to close.

To improve the performance of Squid, edit `/etc/init.d/squid` to replace the `ulimit` line and add the lines as below. This will increase the number of open file descriptors. -H options change and report the hard limit associated with a resource. -S options change and report the soft limit associated with a resource and -n options is the maximum number of open file descriptors.

```
# ulimit -n 4096
ulimit -HSn 8192
```

5.2.2. Basic Configuration

Edit /etc/squid/squid.conf

- http_port

The socket addresses where Squid will listen for HTTP client requests. It could be changed to 8080.

```
# http_port 3128
http_port 8080
```

- cache_mem

Squid provides several options for configuring cache memory. The `cache_mem` option sets the memory allocated primarily for objects currently in use (objects in transit). If available, the space can also be used for frequently accessed objects (hot objects) and failed requests (negative-cache objects). The default is 8MB. You may increase if you have enough memory. Monitor by top command and modify it.

```
# cache_mem 8 MB
```

```
cache_mem 32 MB
```

- maximum_object_size

Objects larger than this size will NOT be saved on disk. The value is specified in kilobytes, and the default is 4MB. If you wish to get a high BYTES hit ratio, you should probably increase this (one 32 MB object hit counts for 3200 10KB hits). If you wish to increase speed more than your want to save bandwidth you should leave this low.

```
# maximum_object_size 4096 KB
# maximum_object_size 32768 KB   #  Save bandwidth
maximum_object_size 1024 KB   # High speed
```

- cache_dir

The usage of cache_dir is

```
cache_dir ufs Directory-Name Mbytes Level1 Level2 [options]
```

In which "ufs" is the old well-known Squid storage format that has always been there, "Mbytes" is the amount of disk space (MB) to use under this directory, the default is 100MB. Change this to suit your configuration. Do NOT put the size of your disk drive here. Instead, if you want Squid to use the entire disk drive, subtract 20% and use that value.

"Level1" is the number of first-level subdirectories which will be created under the Directory. The default is 16. "Level2" is the number of second-level subdirectories which will be created under each first-level directory. The default is 256.

Change the disk space to 1000MB.

```
# cache_dir ufs /var/cache/squid 100 16 256
cache_dir ufs /var/cache/squid 1000 16 256
```

- ftp_user

You can specify the anonymous FTP login password. Some FTP server validate the email address is valid, otherwise rejected. You can use any domain name, but the real your domain is more informative to the FTP server.

```
# ftp_user Squid@
ftp_user Squid@google.com
```

The following changes may improve the performance of the Squid

- half_closed_clients

Some clients may shutdown the sending side of their TCP connections, while leaving their receiving their receiving sides open. You can change this option to “off” and Squid will immediately close client connection.

```
# half_closed_clients on
half_closed_clients off
```

- cache_swap_low and cache_swap_high

```
# cache_swap_low 90
# cache_swap_high 95
cache_swap_low 80
cache_swap_high 100
```

5.2.3. Cache Hierarchy

One of reasons to setup proxy is to its cache feature. Proxy stores site information when a client access to the sire. Next time, when the same request occurs, the proxy returns the object to a client from its cache instead of allowing direct access to the site. As a result, the cache contributes to the reduction in bandwidth utilization, and enables fast access.

However, in the large network housing more than 500 clients, the requests are concentrated to the proxy. This causes traffic bottlenecks.

A cache hierarchy brings the solution in this case. As is shown Figure 2, a cache hierarchy is a collection of caching proxy servers organized in a logical parent/child and sibling arrangement. When a cache requests an object from its parent, and the parent does not have the object in its cache, the parent fetches the object, caches it, and delivers it to the child. The benefits of deploying cache hierarchy are to reduce the load on the proxy, the reduction of bandwidth utilization, fast access to the object, and to build a rich cache.

In the hierarchy cache environment, ICP (Internet Cache Protocol) is used for communication among squid caches. ICP locates specific objects in sibling caches. If a squid cache does not have a requested document, it sends an ICP query to its siblings, and the siblings respond with ICP replies indicating a ``HIT'' or a ``MISS.''

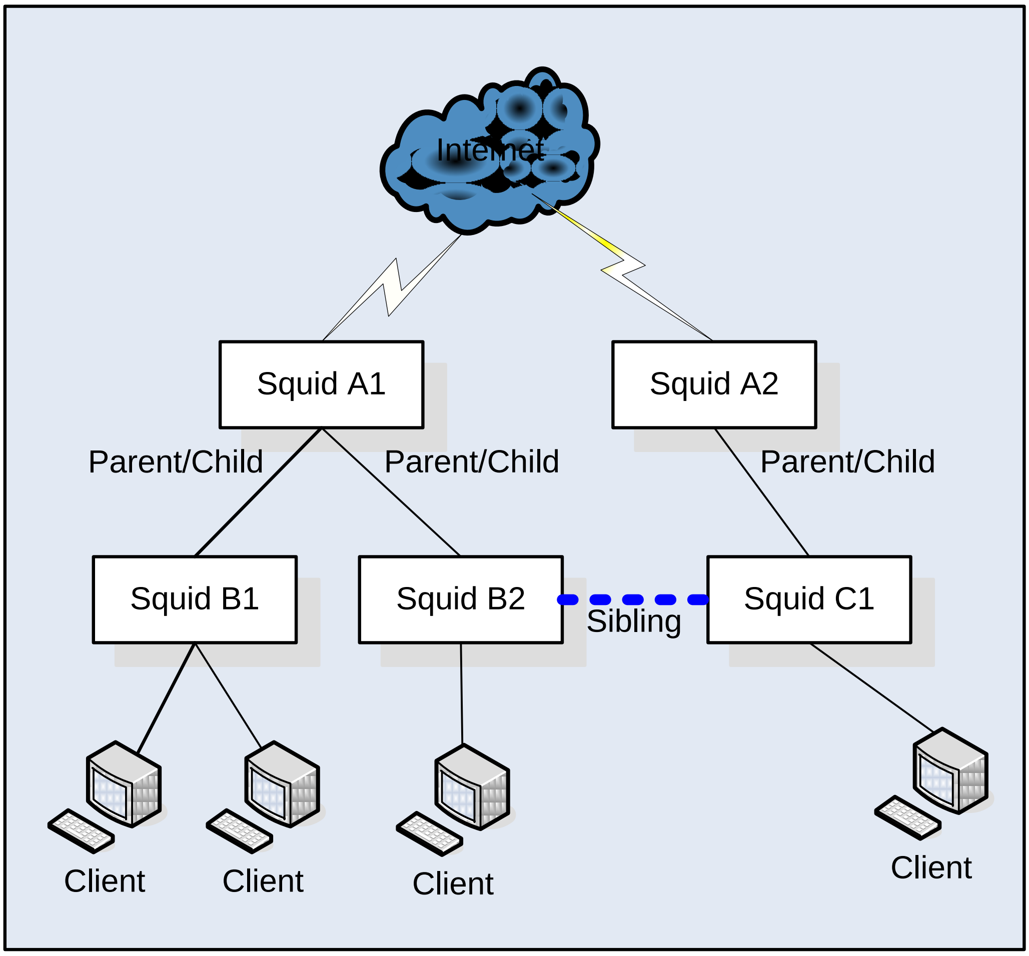


Figure 2 – Cache Hierarchy

Edit `/etc/squid/squid.conf` and add following lines at appropriate location

- cache_peer

To specify other caches in a hierarchy, use the format:

```
cache_peer hostname type proxy-port icp-port [options]
```

type: either 'parent', 'sibling', or 'multicast'.

proxy-port: the port number where the cache listens for proxy requests.

icp-port: Used for querying neighbor caches about objects

no-query: not to send ICP queries to this neighbor

default: if this is a parent cache which can be used as a last-resort if a peer cannot be located by any of the peer-selection mechanisms. If specified more than once, only the first is used.

Add the following lines near the TAG: cache_peer. The entire request will be forwarded to the parent proxy. In this case, the parent proxy is 192.168.0.3:8080.

```
cache_peer 192.168.0.3 parent 8080 0 no-query default
```

Note: this configuration does not use ICP, and then any proxy server can be a parent.

- peer_connect_timeout

This option is how long to wait for a pending TCP connection to a peer cache. You might increase this.

```
# peer_connect_timeout 30 seconds
peer_connect_timeout 60 seconds
```

- always_direct

This option specifies to always access without using the proxy cache, or a parent. This option is used for your local servers.

```
acl local-servers-ip dst 192.168.0.0/16
acl local-servers-domain dstdomain .site
always_direct allow local-servers-ip
always_direct allow local-servers-domain
```

- never_direct

This option is to always forward all requests to a parent or siblings.

```
never_direct allow all
```

Then, start Squid as,

```
# /etc/init.d/squid start
```

If you changed the configuration, you can quickly restart the service using reload option

```
# /etc/init.d/squid reload
```

You should enable Squid to run automatically. So it starts on run level 3 and 5.

```
# chkconfig squid on
# chkconfig --list | grep squid
squid                  0:off  1:off  2:off  3:on   4:off  5:on   6:off
```

5.2.4. Access Control

Access controls enable system administrators to grant access to authorized users, or to restrict, to prevent access from unwanted users. Access controls involves two different components.

- Access control list (ACL) elements
- Access list rule.

ACL element is the building blocks of Squid's access control implementation. Each ACL element has a name, which is referred in the access list rules. The basic syntax of an ACL element is as follows,

```
acl name type value1 value2
```

Squid has 25 different ACL types. To avoid the redundancy, the text introduces a few of them.

- `src`: source (client) IP addresses
- `dst`: destination (server) IP addresses
- `srcdomain`: source (client) domain name
- `dstdomain`: destination (server) domain name
- `port`: destination (server) port number
- `ident`: string matching on the user's name
- `proto`: transfer protocol (http, ftp, etc)
- `proxy_auth`: user authentication via external processes

Applying the access list rules is the second step. In the access list rule, access control elements are combined to *allow*, or *deny* certain actions. Squid have a number of access list rules. Below are frequently used ones.

- `http_access`: Allows HTTP clients (browsers) to access the HTTP port. This is the primary access control list.
- `http_reply_access`: Allows HTTP clients (browsers) to receive the reply to their request. This further restricts permissions given by http_access, and is primarily intended to be used together with the rep_mime_type acl type for blocking different content types.
- `never_direct`: Controls which requests should never be forwarded directly to origin servers.
- `snmp_access`: Controls SNMP client access to the cache.

Allow or Deny access based on defined access lists. To allow access from LAN, you may specify as below,

```
acl our_networks src 192.168.0.0/24 192.168.1.0/24
http_access allow our_networks
http_access allow localhost
http_access deny all
```

This configuration controls the access time for a certain network. Net0 has always access. Net1 has access only during working hours. Net2 has access only during lunchtime.

```
acl Net0 src 192.168.0.0/24
acl Net1 src 192.168.1.0/24
acl Net2 src 192.168.2.0/24
acl WorkingHours time 08:00-16:30
acl Lunchtime time MTWHF 12:00-13:00
http_access allow localhost
http_access allow Net0
http_access allow Net1 WorkingHours
http_access allow Net2 Lunchtime
http_access deny all
```

The following day abbreviations can be used:

S	Sunday
M	Monday
T	Tuesday
W	Wednesday
H	Thrusday
F	Friday
A	Saturday

5.2.5. Proxy Authentication

Squid has a feature to support HTTP proxy authentication. With proxy authentication, the client's HTTP request includes a header containing authentication credentials – username and password. Squid decodes the credential information, and check whether it is valid.

To create password entry

```
# touch -c /etc/squid/passwd
# htpasswd2 -c /etc/squid/passwd user1
```

```
New password:
Re-type new password:
Adding password for user user1
```

To add more users, just type without –c option as,

```
# htpasswd2 /etc/squid/passwd user2
```

Edit authentication parameters at `/etc/squid/squid.conf`

```
# auth_param
auth_param basic program /usr/sbin/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
```

And then add following options to ACL.

```
acl trusted_net src 192.168.0.0/24
acl users_anytime proxy_auth user1 user2
acl users_daytime proxy_auth REQUIRED
acl daytime time 08:00-17:00
http_access allow trusted_net
http_access allow localhost
http_access allow users_anytime
http_access allow users_daytime daytime
http_access deny all
```

In this example, the `trusted_net` computers have access without authentication. The `users_anytime` users need authentication but have access whole day. The other users need authentication and only have access during daytime.

Note that there is an issue that you can not use proxy authentication with transparent proxy.

5.2.6. Delay Pools

Delay pools are a feature for rate limiting, and traffic shaping. They work by limiting the rate at which Squid returns data for cache misses. Cache hits are sent as quickly as possible provided that local bandwidth is wide enough.

The delay pool is attributed “bandwidth buckets”. A response delayed until some amount of bandwidth is available from an appropriate bucket. In the delay pool configuration, “maximum available bits per second”, and “the size of a bucket” are defined. The former allows users to "save up" bandwidth if users don't use the maximum, and it makes some burst speeds available. When a burst empties the “bucket”, they are limited to the fill rate. So it rewards saving users, and puts the brakes on heavy users. The later determines how much burst bandwidth is available to a user.

There are five types of buckets and among them following three are common used:
Class 1 pool: A single aggregate bucket, shared by all users
Class 2 pool: One aggregate bucket, 256 individual buckets
Class 3 pool: One aggregate bucket, 256 network buckets, 65,536 individual buckets

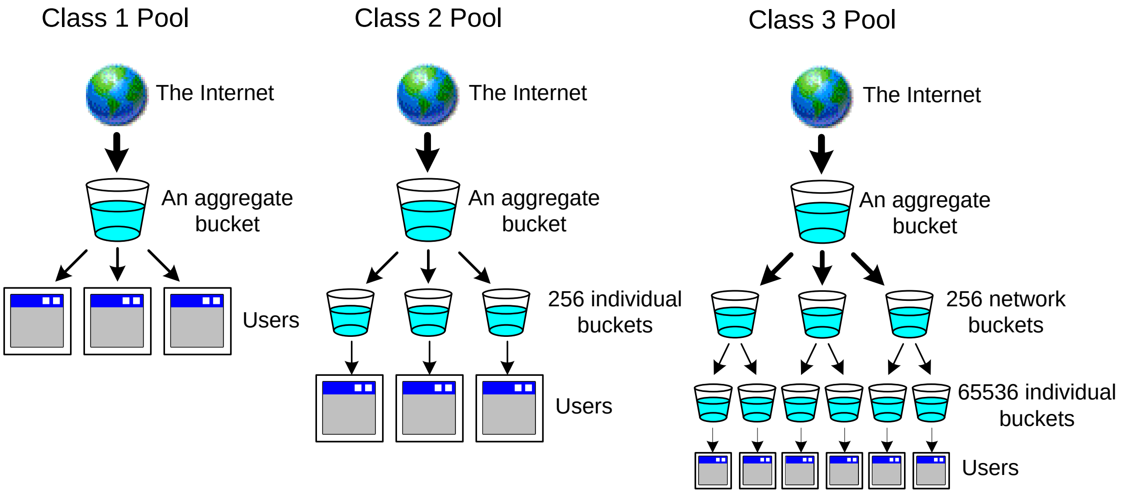


Figure 3 – Delay Pool Classes

(1) Configuration – squid.conf

There are some directives related to delay-pools configuration

- delay_pools: defines how many pools we want to use.

```
delay_pools 1        # 1 delay pool
```

- delay_class: tells which type of pool is being used.

```
delay_class 1 1      # pool 1 is a class 1 pool
delay_class 2 1      # pool 2 is a class 1 pool
```

- delay_parameters: sets our restrictions, fill rate/maximum bucket size.

```
delay_parameters pool aggregate individual network
```

- `pool`: a pool number - ie, a number between 1 and the number specified in `delay_pools` as used in `delay_class` lines.
- `aggregate`: the "delay parameters" for the aggregate bucket (class 1, 2, 3).
- `individual`: the "delay parameters" for the individual buckets (class 2, 3).
- `network`: the "delay parameters" for the network buckets (class 3).

A pair of delay parameters is written restore/maximum, where restore is the number of bytes (not bits) per second placed into the bucket, and maximum is the maximum number of bytes which can be in the bucket at any time.

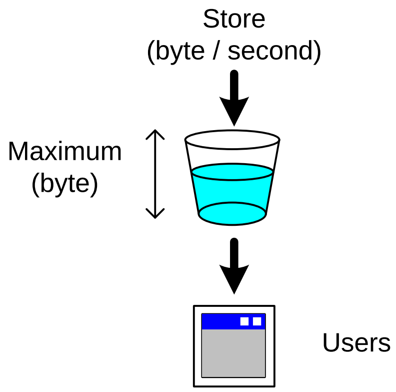


Figure 4 – Delay Pool Bucket

(2) Limiting Download Speed

Class 1 pools restrict the download rate of all connections in the class are added together and Squid keeps this aggregate value below a given maximum value. In the following example, all users who used URL that contain "*abracadabra*" proceed to download at full speed until they have downloaded 128kbps.

```
Acl magic_words url_regex –i abracadabra
delay_pools 1                    # 1 delay pool
delay_class 1 1                  # pool 1 is a class 1 pool
delay_parameters 1 16000/16000
delay_access 1 allow magic_words
```

(3) Individual Restrictions

Class 2 pools are perfect for limiting individual users on networks with fewer than 255 users. For example, if delay pool number 1 is a class 2 delay pool as in the above example, and is being used to strictly limit each host to 64kbps (plus overheads), with no overall limit, the line is:

```
delay_pools 1       # 1 delay pool
delay_class 1 2     # pool 1 is a class 2 pool
# limit each host to 64kbps plus overheads
delay_parameters 1 -1/-1 8000/8000
delay_access 1 allow all
```

Note that the figure -1 is used to represent "unlimited".

(4) Selected Host Restrictions

This case provides different classes of service. In the above listed example, some users are granted more bandwidth by selecting a specific range of IPs.

This configuration uses class 2 delay pool and individual bucket sizes are configured.

```
delay_pools 2       # 2 delay pools
delay_class 1 2     # pool 1 is a class 2 pool
delay_class 2 2     # pool 2 is a class 2 pool
delay_parameters 1 -1/-1 -1/-1     # individual unlimited/unlimited
delay_parameters 2 -1/-1 2000/64000 # individual 16kbps/512kbps
acl lecturer src 192.168.0.0/24
delay_access 1 allow lecturer
delay_access 1 allow localhost
delay_access 2 allow all
```

You can see how the delay pools are working as,

```
# squidclient -p 8080 mgr:delay | less
```

5.2.7. Troubleshooting

Check `/var/log/messages` for any error messages as

```
# less /var/log/messages
```

Press “G” to move the bottom of this file. You might search the string “squid”

This command always shows the bottom of the file, and then you can monitor.

```
# tail -f /var/log/messages
```

Table 11 – Squid log files

File	Description

`/var/log/messages`	Error message, log messages
`/var/log/squid/access.log`	HTTP and ICP request logs
`/var/log/squid/cache.log`	General Information about cash's behaviour.

5.3. Cache Manager - Squid

Squid includes a tool `cachemgr.cgi`. If you copy this file to `/srv/www/cgi-bin/`, you can then go to `http://yourhost/cgi-bin/cachemgr.cgi` and view comprehensive information about the state of the squid cache. This assumes you have the Apache web server set up and running, so that it can run these CGI scripts.

```
# cd /srv/www/cgi-bin/
# cp /usr/lib/squid/cachemgr.cgi .
```

In `/etc/squid/squid.conf`,

```
# cache_mgr webmaster
cache_mgr admin
…
#Example
# cachemgr_passwd secret shutdown
# cachemgr_passwd lesssssssecret info stats/objects
# cachemgr_passwd disable all
#
#Default:
# none
cachemgr_passwd admin all
```

In `/etc/squid/cachemgr.conf`,

```
#localhost
localhost:8080
```

5.4. WPAD (Web Proxy Auto Discovery)

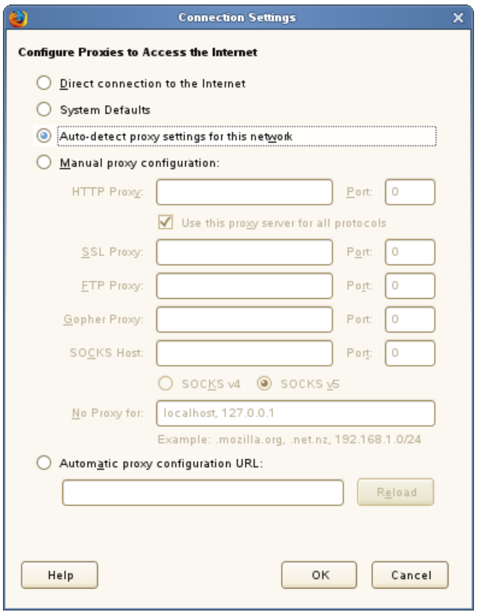
The Web Proxy Auto Discovery (WPAD) Protocol is a method used by web browsers to locate a proxy auto-config file automatically and use this to configure the browser's web proxy settings. Internet Explorer, Mozilla Firefox and Opera have this functionality.

The WPAD standard defines two alternative methods how the system administrator can publish the location of the proxy configuration file, using the Dynamic Host Configuration

Protocol (DHCP) or the Domain Name System (DNS):

5.4.1. Browser Configuration

Configure the browser's web proxy settings. For WPAD, only Internet Explorer, Mozilla Firefox and Opera can work.



Connection Settings

Configure Proxies to Access the Internet

○ Direct connection to the Internet
○ System Defaults
● Auto-detect proxy settings for this network
○ Manual proxy configuration:

HTTP Proxy: Port: 0
☑ Use this proxy server for all protocols
SSL Proxy: Port: 0
FTP Proxy: Port: 0
Gopher Proxy: Port: 0
SOCKS Host: Port: 0
○ SOCKS v4 ● SOCKS v5
No Proxy for: localhost, 127.0.0.1
Example: .mozilla.org, .net.nz, 192.168.1.0/24

○ Automatic proxy configuration URL:

Figure 5 – WPAD configuration on Firefox

Change the “Configure Proxies to Access the Internet” to “Auto-detect proxy settings for this network”.

5.4.2. DHCP Configuration

DHCP has a higher priority than DNS: if DHCP provides the WPAD URL, no DNS lookup is performed

Edit `/etc/dhcpd.conf`, and restart DHCP server

```
…
authoritative;
option wpad code 252 = string;
option wpad "http://wpad.domain1.site/wpad.dat";
…
```

Edit `/etc/apache2/httpd.conf`

```
…
```

```
AddType application/x-ns-proxy-autoconfig .dat
```

5.4.3. DNS Configuration

If the DHCP server does not provide the WPAD information, DNS is used. If, for example, the network name of the user's computer is pc.section.example.site, the browser will try the following URLs in turn until it finds a proxy configuration file:

- http://**wpad**.section.example.site/wpad.dat
- http://**wpad**.example.site/wpad.dat
- http://**wpad**.site/wpad.dat

Edit the master forward zone file, and add an A record as,

```
srv1           IN A           192.168.0.10
www            IN CNAME       srv1
mail           IN CNAME       srv1
admin          IN CNAME       srv1
…
wpad           IN A           192.168.10.1
```

In the case of our server, the 192.168.0.10 is an external IP address, and the 192.168.10.1 is an internal IP address. If you are running a name-based virtual host on the Apache, use the other IP address like above.

5.4.4. Apache Configuration

If the Apache runs several name-based virtual hosts, the browser might not get the `wpad.dat` from the WPAD virtual host's document root. The browser resolves the IP address of the WPAD host, and accesses by the IP address instead of the FQDN. If the FQDN is not used by the browser, the Apache returns one of the virtual host documents (it is likely decided by the alphabetical order, and in our case admin virtual host would be decided instead of wpad).

This is suggested that you configure an IP based virtual host instead of the name-based virtual host for the WPAD.

The IP based virtual host configuration uses the IP address at the <VirtualHost> directive instead of using "*" (asterisk). The `wpad.conf` would look like this.

```
<VirtualHost 192.168.10.1:80>
   ServerName wpad.domain1.site
   DocumentRoot /srv/www/vhosts/wpad
   CustomLog /var/log/apache2/wpad-access_log combined
   <Directory "/srv/www/vhosts/wpad">
      Options none
      Order allow,deny
      Allow from all
   </Directory>
</VirtualHost>
```

5.4.5. WPAD Script Configuration

Create a `wpad.dat` file at the wpad document root. The host wpad must be able to serve a web page, and place at the document root as `/srv/www/vhosts/wpad/wpad.dat.`

```
function FindProxyForURL(url, host) {
  PROXY = "PROXY 192.168.10.1:8080; DIRECT";
  if (isInNet(host,"192.168.0.0","255.255.0.0")||
     dnsDomainIs(host,"localhost")||
     dnsDomainIs(host,"*.site"))
    return "DIRECT";
  else {
    if ((url.substring(0, 5) == "http:") ||
        (url.substring(0, 4) == "ftp:") ||
        (url.substring(0, 6) == "https:") ||
        (url.substring(0, 6) == "snews:")) {
      return PROXY;
    } else {
      return "DIRECT";
    }
  }
}
```

Windows Internet Explorer has a bug that the last character of the URL is removed, so create a link `wpad.da` to the `wpad.dat` as,

```
# ln -s wpad.dat wpad.da
```

5.4.6. WPAD Test

Open a workstation, renew the address from DHCP server, and change the browser configuration to auto-detect. When you browse the Internet, you have an access at /var/log/apache2/wpad-access_log as,

```
192.168.10.100  -  -  [24/Jun/2007:14:41:30  +0000]  "GET  /wpad.dat
HTTP/1.1" 200 158 "-" "WinHttp-Autoproxy-Service/5.1"
```

Check the /var/log/squid/access.log. You must have the access log as,

```
1182697886.164     19977  192.168.10.100  TCP_MISS/200   6327   GET
http://www.google.com - DEFAULT_PARENT/parentproxy text/html
```

5.5. Transparent Proxy

Many organizations — including corporations, schools, and families — use proxy servers to enforce network use policies or provide security and caching services. A normal Web proxy is not transparent to the client application: the client must be configured to use it, manually or with a configuration script. Thus, it can be evaded by simply resetting the client configuration. A transparent proxy or transproxy combines a proxy server with NAT so that connections are routed into the proxy without client-side configuration.

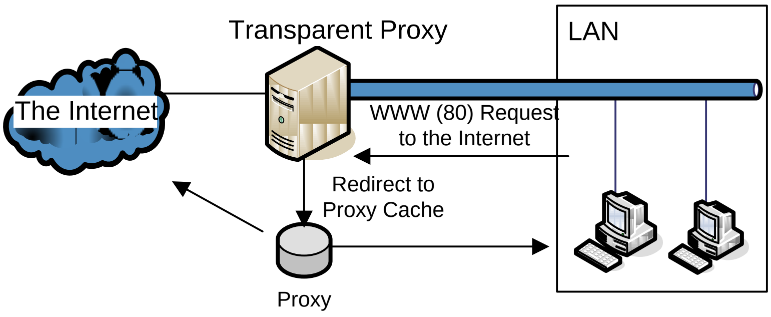


Figure 6 – Transparent Proxy using local Squid Server

To support transparent proxy on Squid, give transparent at the end of http_port line at /etc/squid/squid.conf as,

```
http_port 8080 transparent
```

5.5.1. Redirect Configuration on Firewall

Edit /etc/sysconfig/SuSEfirewall2 for redirecting the http request. Format is,

```
FW_REDIRECT="<source network>,<destination network>,<protocol>,<dport>,<lport>"
```

The SuSEfirewall2 is a front-end of iptables command which is also known as Netfilter. If you have any number of configurations, separate by a space.

This configuration intercepts a tcp packet from 192.168.10.0/24 network to anywhere destined for 80 ports except 192.168.0.0/24 network, and redirected to the local 8080 ports which is your proxy server listening.

```
FW_REDIRECT="192.168.10.0/24,!192.168.0.0/24,tcp,80,8080"
```

This configuration intercepts both 80, and 8080 requests to the local proxy. This will also intercepts the browser's request which is configured to use the external proxy server.

```
FW_REDIRECT="192.168.10.0/24,!192.168.10.0/24,tcp,80,8080 192.16
8.200.0/24,!192.168.10.0/24,tcp,8080,8080"
```

After the firewall configuration, restart the firewall.

```
# rcSuSEfirewall2 restart
```

This command can show the current NAT rules configured by iptables.

```
# iptables -t nat -n -L
Chain PREROUTING (policy ACCEPT)
target     prot opt source             destination
REDIRECT    tcp  --  192.168.10.0/24    !192.168.10.0/24    tcp dpt:80
redir ports 8080
…
```

The issue of the transparent proxy is that, HTTPS and FTP protocol cannot intercept to the proxy. The HTTPS protocol is due to a security reason which violates the "man-in-the-middle attack". The FTP protocol uses either active or passive modes, and simply intercepting the FTP packet does not work for this protocol.

5.6. Content Filtering (Squid Guard)

SquidGuard has a function of content filtering, redirector and access controller plug-in for Squid. It can limit the web access for some users. It can also redirect blocked URLs to an information page. It lets you define multiple access rules with different restrictions for different user groups on a Squid cache. SquidGuard can do the following:

- Limit the Web access for some users to a list of accepted or well-known Web servers or URLs.
- Block access to some listed or blacklisted Web servers or URLs for some users.

- Block access to URLs matching a list of regular expressions or words for some users.
- Redirect blocked URLs to an “intelligent” CGI-based information page.
- Redirect unregistered users to a registration form.
- Redirect banners to an empty GIF.
- Use different access rules based on time of day, day of the week, date, etc.
- Use different rules for different user groups.

squidGuard and Squid cannot be used to:

- Edit, filter, or censor text inside documents.
- Edit, filter, or censor HTML-embedded script languages, such as JavaScript or VBscript.

5.6.1. Squid Guard Configuration

Install `squidGuard` from YaST

- `squidGuard`
- `squidGuard-doc`

Create a script such as `/root/bin/mysquidguard` to download an online blacklist, and install.

```
#!/bin/bash
TMP=/tmp
LIST=/var/lib/squidGuard/db
cd $TMP
rm -f $TMP/blacklists.tgz
wget -c http://squidguard.mesd.k12.or.us/blacklists.tgz
if [ $? -ne 0 ]; then
echo "Failed to download. Execute it later"
exit 1
fi
tar zxvf blacklists.tgz
rm -fr $LIST/blacklists.bak
if [ -e "$LIST/blacklists" ]; then
mv $LIST/blacklists $LIST/blacklists.bak
fi
cp -rf $TMP/blacklists/ $LIST/blacklists
/usr/sbin/squidGuard -C all
```

```
chmod -R 755 $LIST

chown -R squid:root $LIST

/usr/sbin/squid -k reconfigure

rm -rf $TMP/blacklists

exit 0
```

This will download the latest blacklist from the Internet, and install automatically. However, this file is not often updated now, so not necessary to update regularly.

Give permissions, and execute it once.

```
# chmod 755 mysquidguard
# ./mysquidguard
```

Create a warning page. This is an example created at `/srv/www/cgi-bin/blocked`

```
# cd  /usr/share/doc/packages/squidGuard/samples/
# cp squidGuard-simple.cgi  /srv/www/cgi-bin/blocked
# chmod 755 /srv/www/cgi-bin/blocked
```

Edit `/srv/www/cgi-bin/blocked`, and change the appropriate information at following lines,

```
#       print   "                 <A   HREF=\"http://www.squidguard.org/\"><IMG
SRC=\"/images/your-logo.gif\"\n";

#       print "      BORDER=0></A>\n   </P>\n\n";

…

#My $PROXYMAIL = "proxymaster\@foo.bar";

My $PROXYMAIL = "admin\@domain1.site";
```

Note that there are several places to modify, so search by "`your-logo`", and "`proxymaster`".

Edit `/etc/squidguard.conf`. Change the ip addresses and redirect URL to your script.

```
logdir /var/log/squidGuard

dbhome /var/lib/squidGuard/db

# TIME RULES:

# abbrev for weekdays:

# s = sun, m = mon, t =tue, w = wed, h = thu, f = fri, a = sat

time workhours {

weekly mtwhf 08:00 - 16:30
```

```
date *-*-01 08:00 - 16:30
}
src allow-users {
ip 192.168.10.1-192.168.10.10 127.0.0.1 192.168.0.10
user user1 user2
within workhours
}
src guests {
ip 192.168.10.10-192.168.10.254
ip 192.168.11.0/24
}
# DESTINATION CLASSES
dest blacklist {
domainlist blacklist/domains
urllist blacklist/urls
expressionlist blacklist/expressions
}
# Following lists are updated automatically
dest ads {
domainlist blacklists/ads/domains
urllist blacklists/ads/urls
}
dest aggressive {
domainlist blacklists/aggressive/domains
urllist blacklists/aggressive/urls
}
dest audio-video {
domainlist blacklists/audio-video/domains
urllist blacklists/audio-video/urls
}
dest drugs {
domainlist blacklists/drugs/domains
urllist blacklists/drugs/urls
}
dest gambling {
domainlist blacklists/gambling/domains
```

```
}
dest hacking {
domainlist blacklists/hacking/domains
urllist blacklists/hacking/urls
}
dest mail {
domainlist blacklists/mail/domains
}
dest porn {
domainlist blacklists/porn/domains
urllist blacklists/porn/urls
## expressionlist blacklists/porn/expressions
}
dest proxy {
domainlist blacklists/proxy/domains
## urllist blacklists/proxy/urls
}
dest redirector {
domainlist blacklists/redirector/domains
urllist blacklists/redirector/urls
}
dest spyware {
domainlist blacklists/spyware/domains
urllist blacklists/spyware/urls
}
dest suspect {
domainlist blacklists/suspect/domains
## urllist blacklists/suspect/urls
}
dest violence {
domainlist blacklists/violence/domains
urllist blacklists/violence/urls
}
dest warez {
domainlist blacklists/warez/domains
urllist blacklists/warez/urls
```

```
}
acl {
guests {
# It should be one line!!!!!!
pass !blacklist !ads !aggressive !audio-video !drugs !gambling
!hacking !mail !porn !proxy !redirector !spyware !suspect !violence !warez !in-addr any
}
allow-users {
pass all
}
default {
pass none
# It should be one line!!!!!!
redirect
http://www.domain54.site/cgi-bin/blocked?clientaddr=%a&clientname=%n&clientuser=%i&\
clientgroup=%s&targetgroup=%t&url=%u
}
}
```

Edit `/etc/squid/squid.conf` and add one line as,

```
…
redirect_program /usr/sbin/squidGuard
```

Create the databases for squidGuard blacklists,

```
# squidGuard -C all
```

Change the owner and permissions for all databases,

```
# chmod -R 755 /var/lib/squidGuard/db/*
# chown -R squid:root /var/lib/squidGuard/db/*
# squid -k reconfigure
```

Reload Squid

```
# /etc/init.d/squid reload
```

You have to check the squidGuard log file. If successfully started, you see the messages at `/var/log/squidGuard/squidGuard.log`

```
2006-08-28 14:19:31 [10927] squidGuard 1.2.0 started (1156756768.997)

2006-08-28 14:19:31 [10927] squidGuard ready for requests (1156756771.444)
```

Otherwise, squidGuard is in emergency mode. In this mode, you can, however, still use the squid without filtering.

```
2006-08-05 14:44:15 [16284] going into emergency mode
```

Note: Don’t forget to off “transparent” mode in /etc/squid/squid.conf otherwise squidGuard will be in emergency mode.

5.6.2. Maintenance

You might encounter a negative detection such as a word “sex” describing a medical or health. You can modify the blacklist files.

Exercise 5 – Squid

1. Configure Squid with Authentication
2. Configure Squid with Delay Pool
3. Configure Squid with WPAD
4. Configure Squid with Transparent Proxy
5. Configure Squid with SquidGuard

6. Samba <Day 7-8>

6.1. Samba Introduction

Samba is a free software implementation of Microsoft's networking system. As of version 3, samba not only provides file and print services for various Microsoft Windows clients but can also provide domain services, either as a Primary Domain Controller (PDC) or as a Backup Domain Controller (BDC). It can also be a member of an Active Directory domain.

The name samba comes from Microsoft Windows network file system use, called Server Message Block (SMB).

6.1.1. SMB / CIFS

SMB (Server Message Block) is an extension of NetBIOS (Network Basic Input/Output System), which IBM originally designed for DOS in early days to allow file and printer sharing among Windows. Nowadays, SMB uses NBT (NetBIOS over TCP/IP). NetBIOS operates with a number of lower-layer protocols, including NetBEUI, IP. When network is so small that routing is not required, NetBEUI - NetBIOS was used. However, as network is become large, non-routable protocol, that is NetBEUI is replaced with IP. Nowadays, SMB uses NBT (NetBIOS over TCP/IP). Besides Windows, this protocol is widely spread among other operating system, such as UNIX, or MVS.

As for CIFS (Common Internet File System), it refers to as an extension of SMB, the specification of CIFS is in public. Then SMB was integrated to CIFS.

6.1.2. Samba

Samba was developed at ANU (Australian National University), as a replacement for Windows NT file & print services. Samba speaks the CIFS/SMB protocol. Using CIFS protocol, Samba enables UNIX servers to communicate with Microsoft Windows products.

The main features of Samba are,

- To share file-systems
- To share printers installed on both the server and its clients
- Assist clients with Network Neighbourhood browsing

- Authenticate clients logging onto a Windows domain
- Provide or assist with WINS (Windows Internet Naming Service) server resolution
- Windows NT Domain controller
- Microsoft DFS support

It might be needed to mention some characteristic features.

- Windows NT domain controller

Samba offers Windows NT domain controller's feature. Moreover, Samba supports advanced features including Windows NT domain logins, roaming windows user profiles, and CIFS print spooling.

- Microsoft DFS support

Microsoft DFS (Distributed File System) refers to shared resources dispersed among a number of servers in the network, which appear to users as though they are located under a certain directory tree on a server for the purpose to make look simple in relation to shared directory. A system administrator is able to setup DFS system is on a Samba installer server, instead of using Windows server.

- Join Windows 2000/2003 Active Directory

Recently released Samba 3.0 includes support for Kerberos 5 authentication and LDAP, which are required to act as clients in an Active Directory domain. Moreover, Samba 3.0 supports for Unicode, which can make international languages supports easily.

However, Samba still does not fully support Active Directory, since Windows domain protocols are proprietary, and veiled. The table listed below shows what Samba support, and what it does not.

Table 12 – Samba roles

Role	Can perform?
File server	Yes
Printer server	Yes
Microsoft DFS server	Yes
Primary domain controller	Yes
Backup domain controller	Yes
Active Directory domain controller	No
Windows 95/98/Me authentication	Yes

Windows NT/2000/XP authentication	Yes
Local master browser	Yes
Local backup browser	Yes
Domain master browser	Yes
Primary WINS server	Yes
Secondary WINS server	No

6.2. Samba Configuration

6.2.1. Samba Installation

Samba's three daemons – smbd, nmbd, winbindd

- **smb:** daemon implements file and printer sharing on a CIFS network and provides authentication and authorization for CIFS clients.
- **nmb:** daemon provide the other name resolution, and service announcement
- **winbindd:** daemon allows Samba to authenticate, and authorize users thought Windows NT/2000/2003 server.

Install the following packages from http://www.ictti.site/share/samba-maintained-11.2

- samba
- samba-winbind
- samba-client
- samba-doc

The start-up scripts are `/etc/rc.d/smb`, and `/etc/rc.d/nmb` (NetBIOS name server), so make sure these start automatically. If you are using a member server of Windows NT Server, or 2000 Server, you also need to start winbind.

```
# chkconfig smb on
# chkconfig nmb on
# /etc/init.d/smb restart
# /etc/init.d/nmb restart
# chkconfig --list | less
```

The original smb.conf is, `/usr/share/doc/packages/samba/examples/smb.conf.SUSE` so you may copy it to make the default configuration back.

```
# cp /etc/samba/smb.conf /etc/samba/smb.conf.bak
# cp /usr/share/doc/packages/samba/examples/smb.conf.SUSE /etc/samba/smb.conf
```

6.2.2. SWAT Configuration

SWAT (Samba Web Administration Tool) provides a graphical interface for configuring Samba. Swat is already installed along with samba package. It is disabled and also limited access from the local. You can enable, and also may allow access from your LAN (but depending on your security policy). Open /etc/xinetd.d/swat

```
# SWAT is the Samba Web Administration Tool.
service swat
{
        socket_type     =  stream
        protocol        =  tcp
        wait            =  no
        user            =  root
        server          =  /usr/sbin/swat
        only_from       =  127.0.0.1
        only_from       =  192.168.10.0/24
        log_on_failure  += USERID
        disable         =  no
}
```

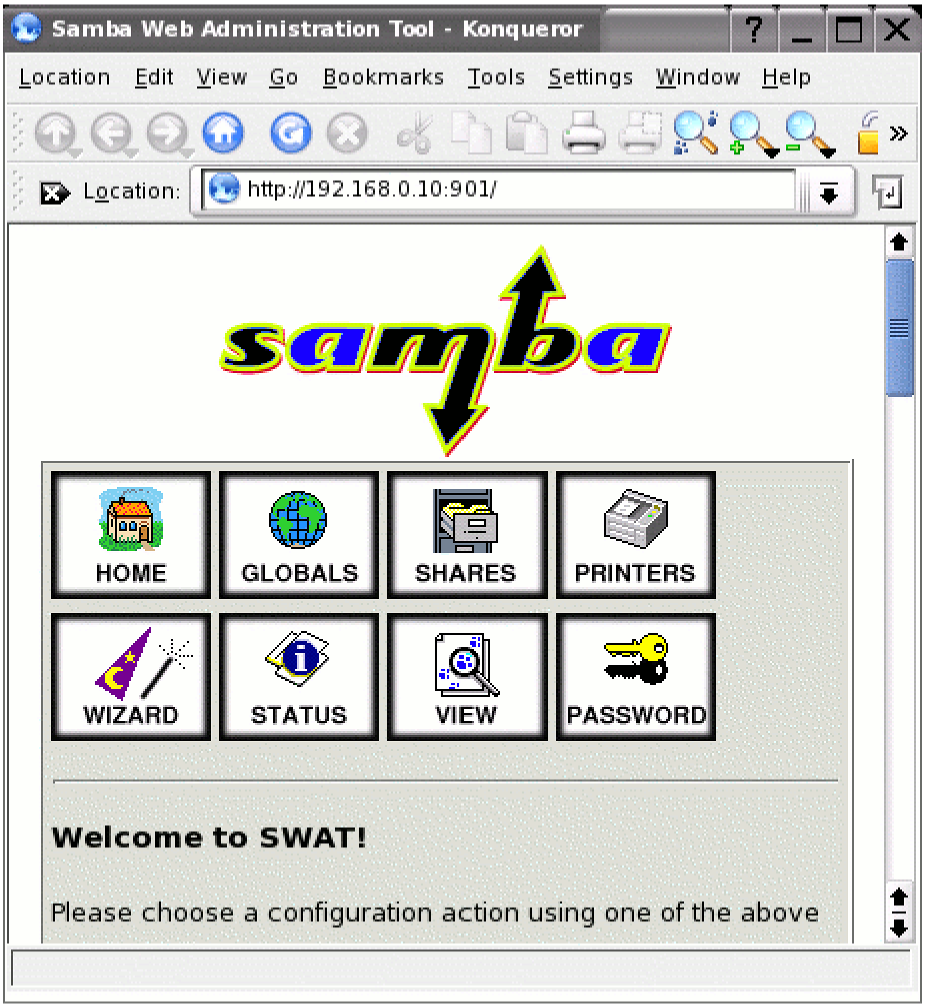
Once you modify files under /etc/xinet.d you need to restart xinetd.

```
# /etc/init.d/xinetd restart
Shutting down xinetd:                                                      done
Starting INET services. (xinetd)                                            done
```

SWAT runs on 901 port, so you may verify whether 901 port is a status of listen by netstat command.

```
# netstat -ln
```

Now you can access http://hostname:901 by browser. You need to login as root user. It is better to access directly to the SWAT without proxy (disable proxy access) otherwise the new configuration may not be reflected on the browser.


Samba Web Administration Tool - Konqueror
Location Edit View Go Bookmarks Tools Settings Window Help
Location: http://192.168.0.10:901/
samba
HOME
GLOBALS
SHARES
PRINTERS
WIZARD
STATUS
VIEW
PASSWORD

Welcome to SWAT!

Please choose a configuration action using one of the above

Figure 7 – Samba Web Administration Tool (SWAT)

6.2.3. Samba User Management

You need to provide a way to allow Samba to authenticate the users. The easy way is to use a flat file as the account database. This file is managed from the command line. In this case, you want to serve the home directory for user `user1`. The username and password should match the account on Windows client, Samba User account, and Linux User account.

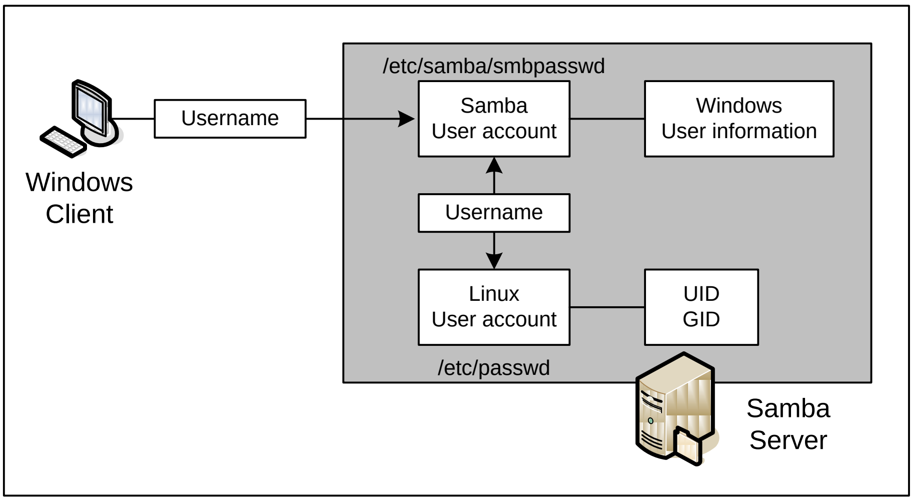


Figure 8 – Windows, Samba, and Linux account

With these configurations in place, `user1` should be able to log in on the Windows client and browse via "My Network Places" to the workgroup and NetBIOS name defined for your Samba server corresponding to user1's home directory on the server.

(1) To add a new user

- Add a Linux account

```
# useradd -m user1
# passwd user1
```

- Add a Samba account. Note that you should give the same password.

```
# pdbedit -a user1
```

(2) To change a user's password

- Change a Linux password.

```
# passwd user1
```

- Change a Samba password

```
# smbpasswd user1
```

(3) To delete the a user's account

- Delete a Samba account

```
# pdbedit -x user1
```

- Delete a Linux account

```
# userdel user1
```

6.2.4. Special Sections

There are three special sections in the `smb.conf`.

- The [global] section

The parameters in this section apply to the Samba server as a whole, or are defaults sections.

- The [home] section

If [home] section is in the `smb.conf`, the share of individual user's home directory is created by the server. When a Windows user login to their Windows PC, they can also access their Linux home directory (`/home/username`) by `\\server\username`.

- The [printers] section

This section is like [homes] but for printers.

6.2.5. Stand Alone Server Configuration

This example is for the following preconditions.

1. Security is maintained by user name and password, so the user needs to login to the Windows PC by the Linux user account to access their home directory.
2. The individual home directory and the public shared directory "share" are published.
3. Printer is not shared.

This is a sample configuration of `/etc/samba/smb.conf` generated by SWAT. You can also directly edit this file. The each parameter is explained later.

```
[global]
        workgroup = DOMAIN1
        server string = File Server
        map to guest = Bad User
        pam password change = Yes
        unix password sync = Yes
        socket options = TCP_NODELAY SO_RCVBUF=8192 SO_SNDBUF=8192
        load printers = No
        printcap name = cups
        logon path = \\%L\profiles\.msprofile
        logon drive = P:
        logon home = \\%L\%U\.9xprofile
        wins server = eth0:192.168.10.3
        wins support = Yes
        ldap ssl = no
        usershare allow guests = Yes
        printing = cups
        cups options = raw
        print command =
        lpq command = %p
        lprm command =
        include = /etc/samba/dhcp.conf

[homes]
        comment = Home Directories
        valid users = %S, %D%w%S
        read only = No
        inherit acls = Yes
        browseable = No

[profiles]
        comment = Network Profiles Service
        path = %H
        read only = No
        create mask = 0600
        directory mask = 0700
        store dos attributes = Yes

[users]
        comment = All users
        path = /home
        read only = No
        inherit acls = Yes
        veto files = /aquota.user/groups/shares/

[groups]
        comment = All groups
        path = /home/groups
        read only = No
        inherit acls = Yes

[printers]
        comment = All Printers
        path = /var/tmp
        create mask = 0600
        printable = Yes
        browseable = No

[print$]
        comment = Printer Drivers
        path = /var/lib/samba/drivers
        write list = @ntadmin, root
        force group = ntadmin
        create mask = 0664
        directory mask = 0775

 [share]
        path = /srv/ftp/
        read only = No
        guest ok = Yes
        create mask = 0660
        directory mask = 0770
```

The common parameters are described below,

- workgroup

Keep the same workgroup as Windows clients, or a domain name. If the domain name is `example.com`, your workgroup name is `EXAMPLE`.

```
workgroup = DOMAIN1
```

- server string

It sets the server which appear in browse lists next to the machine name

```
server string = File Server
```

- security

Access control is done by username and password. UNIX account is necessary.

```
security = USER
```

- encrypt passwords

Encrypt password is enabled for Windows 2000, XP, and Vista

```
encrypt passwords = Yes
```

- pam password change

PAM will be used for password changes

```
pam password change = Yes
```

- unix password sync

Synchronize the UNIX password with the SMB password when the SMB password is changed

```
unix password sync = Yes
```

Note that, if you use `smbpasswd` to change a password by root, Linux password will not be changed. You need `passwd` command afterward.

- Create mask

When a file is created, you can define the permission for that file

```
create mask = 0775
```

- Directory mask

For directory permission,

```
directory mask = 0775
```

- available

This “shares” parameter lets you "turn off" a service. If `available = no`, then *ALL* attempts to connect to the service will fail. Such failures are logged.

```
Available = yes
```

- socket options

Buffer size to improve performance

```
socket options = TCP_NODELAY SO_RCVBUF=8192 SO_SNDBUF=8192
```

- load printers

No printer sharing

```
load printers = No
```

- wins support

Function nmbd process as a WINS server. You should NEVER set to yes on more than one machine in your network

```
wins support = Yes
```

The options ***wins server*** and ***wins support*** must never be enabled at the same time in *smb.conf* file.

To disable dynamic changes of wins server option by dhcp, you need to modify in /etc/sysconfig/network/dhcp

```
#DHCLIENT_MODIFY_SMB_CONF="yes"
DHCLIENT_MODIFY_SMB_CONF="no"
```

6.2.6. Guest Connection

Followings are "global" parameters to enable guest connection

- map to guest
  - **Never**: User login requests with an invalid password are rejected
  - **Bad User**: Means user logins with an invalid password are rejected, unless the username does not exist, in which case it is treated as a guest login
  - **Bad Password**: Means user logins with an invalid password are treated as a guest login

```
map to guest = Bad Password
```

- guest account

Keep as it is as nobody

```
guest account = nobody
```

Followings are "shares" section parameters to enable guest connection on each share.

- guest ok

If yes, no password is required to connect to the service.

```
guest ok = Yes
```

- guest only

Only guest connections to the service are permitted.

```
guest only = Yes
```

6.2.7. Network level access control

- hosts allow

This parameter can apply either the “global” section, or “shares” section. You can specify the hosts by name or IP address. You can restrict access to only the hosts on a Class C subnet 192.168.10.0/24 as,

```
hosts allow = 192.168.10.
```

The syntax of the list is described in the man page. See `man hosts_access`.

6.2.8. Samba Client Configuration

To list all the SMB servers, use `findsmb`,

```
# findsmb
                           *=DMB
                           +=LMB
IP ADDR        NETBIOS NAME    WORKGROUP/OS/VERSION
----------------------------------------------------------------------
192.168.10.1   SRV1         +[SRV1] [Unix] [Samba 3.0.23d-6-1083-SUSE-SL10.2]
```

To list the shares on a specific server, use smbclient,

```
# smbclient -U user1 -L srv1
Password:
Domain=[SRV1] OS=[Unix] Server=[Samba 3.0.23d-6-1083-SUSE-SL10.2]
       Sharename       Type      Comment
       ---------       ----      -------
       profiles        Disk      Network Profiles Service
       users           Disk      All users
       groups          Disk      All groups
       print$          Disk      Printer Drivers
       public          Disk      Public Space
       IPC$            IPC       IPC Service (Samba 3.0.26a-3-1478-SUSE-SL10.3)
Domain=[DOMAIN1] OS=[Unix] Server=[Samba 3.0.26a-3-1478-SUSE-SL10.3]
…
```

To connect to a share and to copy files to or from it.

```
# smbclient -U user1 //srv1/user1
Password:
```

```
smb: \> dir
smb: \> get filename
smb: \> quit
```

To mount the SMB share into the Linux filesystem, use following command,

```
# mount -t cifs //192.168.0.2/share /mnt/share -o username=guest,password=guest
```

To mount the SMB share automatically, edit `/etc/fstab` as,

```
…
//192.168.0.2/share              /mnt/share                cifs
username=guest,password=guest 0 0
```

To access from the GNOME File Browser (Nautilus), or KDE Konqueror type the location as,

```
        smb://servername
```

To access the user’s home directory

```
        smb://servername/username
```

6.2.9. Troubleshooting

Check `/var/log/messages` for any error messages as

```
# less /var/log/messages
```

Press “G” to move the bottom of this file. You might search the string “smbd”

This command always shows the bottom of the file, and then you can monitor.

```
# tail -f /var/log/messages
```

If you get the following error when you use findsmb command, edit this file /usr/bin/findsmb, remove –W at the first line.

```
Scalar value @t1[3] better written as $t1[3] at /usr/bin/findsmb line
45.
Scalar value @t2[3] better written as $t2[3] at /usr/bin/findsmb line
45.
Scalar value @name[0] better written as $name[0] at /usr/bin/findsmb
line 79.
Scalar value @info[0] better written as $info[0] at /usr/bin/findsmb
line 114.
Scalar value @name[0] better written as $name[0] at /usr/bin/findsmb
```

```
line 122.
Use of uninitialized value $_ in pattern match (m//) at /usr/bin/findsmb
line 27.
Use of uninitialized value $_ in pattern match (m//) at /usr/bin/findsmb
line 29.
Use of uninitialized value $_ in pattern match (m//) at /usr/bin/findsmb
line 27.
Use of uninitialized value $_ in pattern match (m//) at /usr/bin/findsmb
line 29.
Use of uninitialized value $BCAST in concatenation (.) or string at
/usr/bin/findsmb line 51.
```

Table 13 – Samba log files

File	Description
/var/log/messages	Error message, log messages
/var/log/samba/	Samba log directory

The smbclient command from your Samba system to see that everything is running and being shared as you expect it to be.

```
# smbclient -L localhost
Unknown socket option SO_RCVBUF_8192
Password:
Domain=[DOMAIN1] OS=[Unix] Server=[Samba 3.0.26A-3-1478-SUSE-SL10.3]

       Sharename      Type     Comment
       ---------      ----     -------
       profiles      Disk     Network Profiles Service
       users         Disk     All users
       groups        Disk     All groups
       print$        Disk     Printer Drivers
       public        Disk     Public Space
       IPC$          IPC      Service(Samba
3.0.26a-3-1478-SUSE-SL10.3)
Domain=[DOMAIN1] OS=[Unix] Server=[Samba 3.0.26a-3-1478-SUSE-SL10.3]

       Server              Comment
```

```
        ---------          -------
        SRV1             domain1
        NW1-02


        Workgroup          Master
        ---------          -------
        DOMAIN1         SRV1
```

The `smbstatus` command can view who is currently using Samba shared resources offered from the Samba system.

```
# smbstatus
```

6.3. On-Access Virus Scanning

6.3.1. Clam Antivirus

Clam Antivirus is an antivirus toolkit for UNIX. This is used with a main exchange server as a server-side email virus scanner, and on-access Samba scanner. ClamAV is open source software, and updates are made available free of charge.

Install following packages for ClamAV

- `clamav,`
- `clamav-db`

If you need a proxy to access the Internet, edit `/etc/freshclam.conf` as,

```
HTTPProxyServer 192.168.0.10
HTTPProxyPort 8080
```

Start ClamAV. FreshClam daemon can update the virus database automatically.

```
# chkconfig clamd on
# chkconfig freshclam on
# /etc/init.d/clamd start
# /etc/init.d/freshclam start
```

Update virus database. However you probably see warning saying ClamAV is outdated as below.

```
# freshclam
```

```
ClamAV update process started at Sat Dec 18 17:49:40 2004
…
Database updated (28424 signatures) from database.clamav.net (195.70.36.141).
```

So you must update to the latest ClamAV. After the update from functionality level 1 to 3, you need to again update then you will not see errors.

```
# freshclam
ClamAV update process started at Wed Jun 27 08:49:32 2007
Reading CVD header (main.cvd): OK (IMS)
main.cvd is up to date (version: 43, sigs: 104500, f-level: 14, builder: sven)
Reading CVD header (daily.cvd): OK (IMS)
daily.cvd is up to date (version: 3333, sigs: 15923, f-level: 15, builder: ccordes)
```

Download Antivirus test file and see whether it can detect it nor not.

Download from `http://www.eicar.org/anti_virus_test_file.htm` or download by `wget`, then

```
# cd /tmp
# wget http://www.eicar.org/download/eicar_com.zip
# clamscan /tmp -i
…
./eicar_com.zip: Eicar-Test-Signature FOUND
…
```

You may scan the file system once a week (i.e., you have Samba share or web contents in your system, etc). Create `/etc/cron.weekly/clamscan.cron`

```
/usr/bin/nice /usr/bin/clamscan -r -i /srv /home
```

Note: This script only detects viruses but does not remove. If you want to remove infected files, use “`--remove`” option but use it carefully.

6.3.2. Samba with ClamAV

Install the following package

- `samba-vscan`

Edit at global section of `/etc/samba/smb.conf` as,

```
[global]
…
```

```
vfs object = vscan-clamav
vscan-clamav: config-file = /etc/samba/vscan-clamav.conf
```

Copy configuration file as,

```
# cd /usr/share/doc/packages/samba-vscan/
# cp vscan-clamav.conf /etc/samba/
```

Create directory named /var/run directory and change the ownership as,

```
# mkdir /var/run/clamd
# chown vscan:vscan /var/run/clamd
```

Create a directory which will be used as quarantine and change the ownership and permission,

```
# mkdir /var/lib/clamav/quarantine
# chown vscan:vscan /var/lib/clamav/quarantine
# chmod 777 /var/lib/clamav/quarantine
```

Edit `/etc/samba/vscan-clamav.conf` such as,

```
[samba-vscan]
max file size = 0
verbose file logging = yes
scan on open = yes
scan on close = yes
deny access on error = yes
deny access on minor error = yes
send warning message = yes
infected file action = quarantine
quarantine directory  = /var/lib/clamav/quarantine
quarantine prefix = vir-
max lru files entries = 100
lru file entry lifetime = 5
exclude file types =
clamd socket name = /var/run/clamd/clamd
libclamav max files in archive = 1000
libclamav max archived file size = 10 * 1048576
libclamav max recursion level = 5
```

Backup the file `/etc/clamd.conf` and make the new file as,

```
LogFile /var/log/clamd
LogFileUnlock yes
LogSyslog yes
LogFacility LOG_MAIL
LogVerbose yes
PidFile /var/lib/clamav/clamd.pid
DatabaseDirectory /var/lib/clamav
LocalSocket /var/run/clamd/clamd
FixStaleSocket yes
TCPSocket 3310
User vscan
Foreground yes
Debug no
```

Create a log file, and then restart the daemon.

```
# touch /var/log/clamd
# chown vscan:vscan /var/log/clamd
```

Edit /etc/init.d/clamd and then restart the daemon.

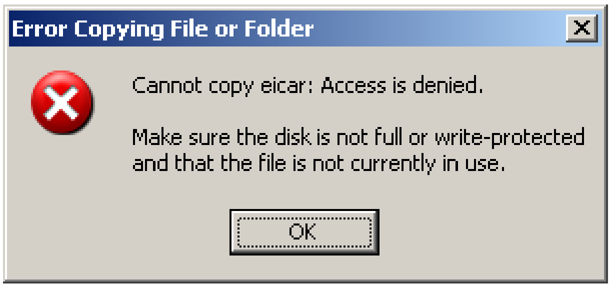
```
case "$1" in
   start)
  echo -n "Starting Clam AntiVirus daemon "
 if ! test -f $CLAMD_DBDIR/main.cvd -o -f $CLAMD_DBDIR/main.cld ; then
   rc_failed
   rc_status -v
   echo "  ClamAV Virus definition files are missing from $CLAMD_DBDIR."
   echo "  Either install the clamav-db package or run freshclam."
 else
  startproc -p $CLAMD_PIDFILE $CLAMD_BIN
  rc_status -v
 fi
  ;;
  stop)
```

```
# /etc/init.d/clamd restart
```

6.3.3. Confirmation

Download testing virus files from
`http://www.eicar.org/anti_virus_test_file.htm`

These are safe. Copy them into the samba shared folder. When you try to access these files, these files are locked and can not access. You would see this message box as,



Error Copying File or Folder

Cannot copy eicar: Access is denied.

Make sure the disk is not full or write-protected and that the file is not currently in use.

Monitor log files at both `/var/log/clamd` and `/var/log/message` by tail command. `/var/log/clamd`. You would see as below.

```
/home/user1/eicar_com.zip: Eicar-Test-Signature FOUND
```

`/var/log/message`

```
Jun 27 13:19:51 srv1 smbd_vscan-clamav[7407]: ALERT - Scan result:
'/home/user1/eicar_com.zip'        infected        with        virus
'Eicar-Test-Signature', client: '192.168.10.10'
```

6.4. Disk Quota

A disk quota is a limit set by a system administrator that restricts file usage on each user and group. Disk quotas are implemented on a per-user or per-group basis. A system administrator defines a usage to a certain user or group on each disk partition.

6.4.1. Quota Installation

Install following packages `quota`,

```
# quota
# quota-nfs
```

And then you need to configure quota for user and group from within YaST.

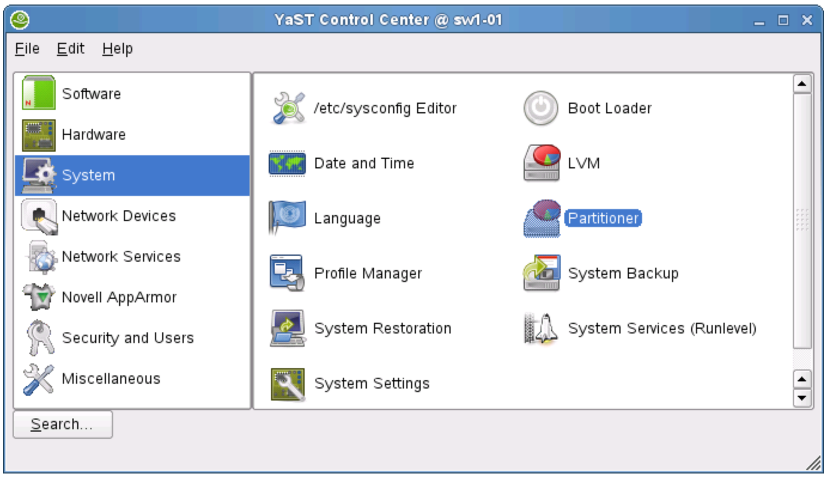
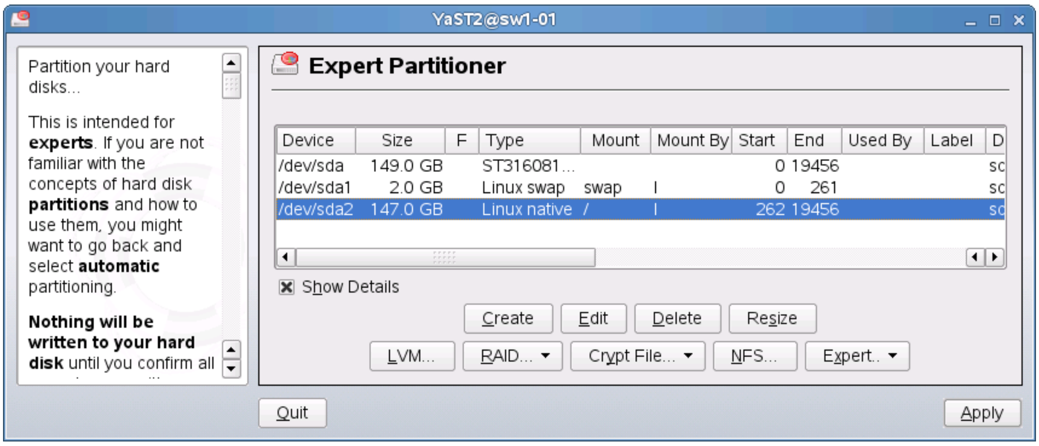


Figure 9 – Enable quota from YaST2

To configure quota support, you need to configure from Partitioner under System tag. From that Expert Partitioner, you can edit `/etc/fstab` file.



Partition your hard disks...

This is intended for **experts**. If you are not familiar with the concepts of hard disk **partitions** and how to use them, you might want to go back and select **automatic** partitioning.

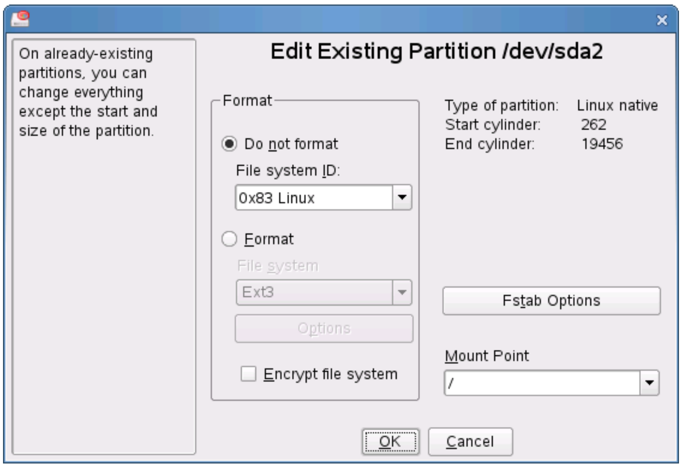
Nothing will be written to your hard disk until you confirm all

Device	Size	F	Type	Mount	Mount By	Start	End	Used By	Label	D
/dev/sda	149.0 GB		ST316081...			0	19456			sc
/dev/sda1	2.0 GB		Linux swap	swap	l	0	261			sc
/dev/sda2	147.0 GB		Linux native	/	l	262	19456			sc

☒ Show Details

Figure 10 – YaST Partitioner

In the “Expert Partitioner” window, you can make enable quota for each disk partition. If you want to make quota for user and group, select available partition and edit that partition. If you have an individual partition for `/home` directory, you need to select the `/home` and edit that device.



On already-existing partitions, you can change everything except the start and size of the partition.

Edit Existing Partition /dev/sda2

Format

● Do not format

File system ID: 0x83 Linux

○ Format

File system: Ext3

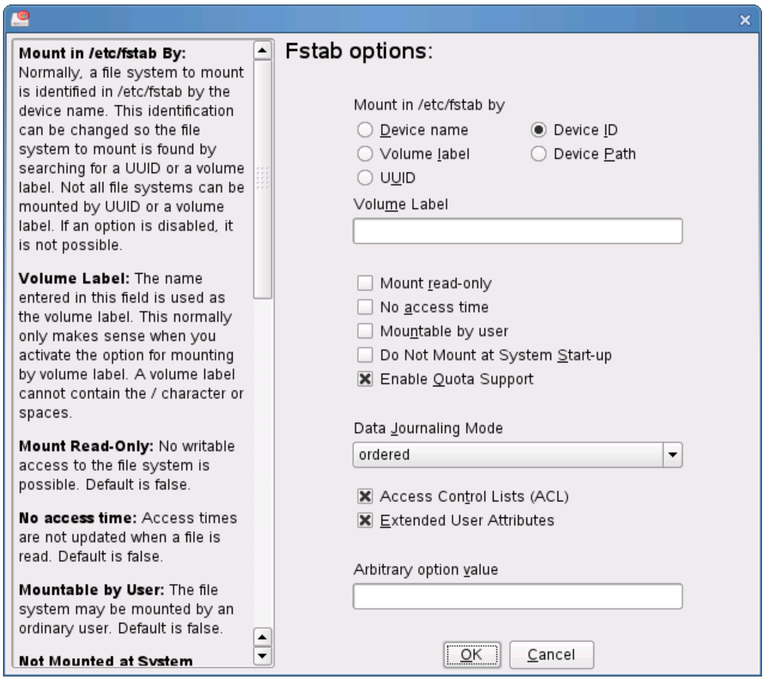
☐ Encrypt file system

Type of partition: Linux native
Start cylinder: 262
End cylinder: 19456

Mount Point: /

Figure 11 – Existing partition

In the “Fstab Options”, there are some options for `/etc/fstab` file. To use disk quota for user and group, you need to activate the “Enable Quota Support” check box.



Mount in /etc/fstab By: Normally, a file system to mount is identified in /etc/fstab by the device name. This identification can be changed so the file system to mount is found by searching for a UUID or a volume label. Not all file systems can be mounted by UUID or a volume label. If an option is disabled, it is not possible.

Volume Label: The name entered in this field is used as the volume label. This normally only makes sense when you activate the option for mounting by volume label. A volume label cannot contain the / character or spaces.

Mount Read-Only: No writable access to the file system is possible. Default is false.

No access time: Access times are not updated when a file is read. Default is false.

Mountable by User: The file system may be mounted by an ordinary user. Default is false.

Not Mounted at System

Fstab options:

Mount in /etc/fstab by

○ Device name ● Device ID
○ Volume label ○ Device Path
○ UUID

Volume Label

☐ Mount read-only
☐ No access time
☐ Mountable by user
☐ Do Not Mount at System Start-up
☒ Enable Quota Support

Data Journaling Mode: ordered

☒ Access Control Lists (ACL)
☒ Extended User Attributes

Arbitrary option value

Figure 12 – Enable Quota Support

If you enable quota support in the partitioner in the running system after the installation, you need to reboot your system.

```
# reboot
```

After rebooting your system, your need to execute boot.quota,

```
# /etc/init.d/boot.quota restart
```

You can verify the mount option by `mount` command,

```
# mount
/dev/sda2 on / type ext3 (rw,acl,user_xattr,usrjquota=aquota.user,grpjquota=aquota.group,jqfmt=vfsv0)
```

After the system has come up, enable quota by following commands,

```
# quotacheck -avugm
quotacheck: Scanning /dev/sda2 [/] done
quotacheck: Checked 22694 directories and 207035 filesquotaon -avug
# quotaon -avug
/dev/sda2 [/]: group quotas turned on
/dev/sda2 [/]: user quotas turned on
```

When you execute it at first time, you will see some message but they are no problem.

Enable the `boot.quota` and `quotad` services.

```
# chkconfig boot.quota on
# chkconfig quotad on
# /etc/init.d/boot.quota restart
# /etc/init.d/quotad restart
```

6.4.2. Edit quota on each user

(1) edquota

The command "`edquota -u username`" takes you into vi to edit quota for the user on each partition that has quota enabled

```
# edquota -u user1
```

Note that a value of zero for any of the limits means that no limit is enforced.

```
Disk quotas for user user1 (uid 1001):
  Filesystem          blocks       soft       hard     inodes     soft     hard
  /dev/sda2              100          0          0         24        0        0
```

- Filesystem

The partition to which this entry relates

- Blocks

The number of 1KB blocks this use is currently using (i.e. 500,000 blocks = 500MB)

- Soft

This is the soft limit on block count. This can be exceeded for a specified grace period, but the user will receive a warning.

- Hard

This is the hard limit on the block count. This cannot be exceeded and the user receives an error.

- Inodes

This is the number of inodes that this user is currently using. This equates to the number of files the user has

- Soft

This is the soft limit on the number of inodes.

- Hard

This is the hard limit on the number of inodes.

The grace period which determines the length of time that a user is allowed to exceed the soft limits, is also configured by `edquota` command.

```
# edquota -u -t
```

Then edit the following,

```
Grace period before enforcing soft limits for users:
Time units may be: days, hours, minutes, or seconds
  Filesystem              Block grace period     Inode grace period
  /dev/sda2                     7days                   7days
```

Sometimes it is desirable to set quota limits on a range of UIDs. This can be done by use of the `-p` option on the `edquota` command. First, assign the desired quota limit to a user, and then run this script. For example, if user `test` has the desired quota limits, the following command can be used to duplicate those quota limits for UIDs more than 999

```
# edquota -p test ` awk -F: '$3 > 999 && $3 != 65534 {print $1}' /etc/passwd `
```

This script does the same but duplicate only users belong to GID 1000.

```
# edquota -p test `awk -F: '$3 > 999 && $4==1000{print $1}' /etc/passwd`
```

The `quota` command reports quotas for a specified user

```
# quota user1
```

(2) repquota

The `repquota` command produces summarized quota information for a file system.

```
# repquota -a
```

If you exceed the quota, you will see the error as,

```
-bash: echo: write error: Disk quota exceeded
```

(3) setquota

By using `setquota`, you can set the quota without using an editor. This is ideal for implementing in a script.

```
# setquota -u user2 200000 250000 0 0 /dev/sda2
# repquota -a | grep user2
user2     --     300  200000  250000           72     0     0
```

For example, to set the soft block limit to 200000 (200M), the hard limit to 250000 (250M), and the soft and the hard inodes are 0.

6.4.3. Warning quota

The `warnquota` checks the disk quota for each filesystem and mails a warning message to those users who have reached their soft limit. Edit `/etc/warnquota.conf`. Use the administrator's mail address..

```
# Standard mail fields
#
FROM              = "root@domain1.site"
SUBJECT            = "Your account quota has exceeded!"
CC_TO             = "root@domain1.site"
…
# These variables are used in the default signatures,
# provided SIGNATURE or GROUP_SIGNATURE is not specified (see below)
#
SUPPORT            = "root@domain1.site"
…
# Comment this out or remove it once you have edited this config file
#
#  FAIL              = "configure /etc/warnquota.conf before running
warnquota"
```

Edit `/etc/quotatab` to set your quota partition.

```
# /dev/hda4: Your home directory
```

/dev/**sda2**: Your home directory

To keep the quotas accurate, it is suggested to run `quotacheck` periodically. The `warnquota` will send mail to users over quota. Create a cron entry as `/etc/cron.daily/quota.sh`

```
#!/bin/bash
# To keep quota accurate
/sbin/quotacheck -avugmf
# To send mail to users over quota
/usr/sbin/warnquota
```

Give permission to the file,

```
# chmod 755 quota.sh
```

The user and the root will receive the message as this (if still not exceeded the hard limit, though)

```
Subject: Your account quota has exceeded!
From: root@domain1.site
To: user1@domain1.site
CC: root@domain1.site
```

```
Hello user user1, I've noticed you use too much space on my disk in srv1.
Delete your files on the following filesystems:

Your home directory (/dev/sda2)

                   Block limits               File limits
Filesystem          used    soft    hard  grace    used  soft  hard  grace
/dev/sda2       +- 229932  200000  250000  6days    135     0     0

See you!
                   Your admin of srv1
```

Exercise 6 – Samba

1. Configure a stand alone Samba server
2. Configure Samba with on-access virus scanner
3. Configure Disk Quota

7. Mail Server (Postfix) <Day 9-12>

7.1. Mail Server Introduction

E-mail, or email, is short for "electronic mail" (as opposed to conventional mail, in this context also called snail mail) and is a method of composing, sending, and receiving messages over electronic communication systems. Most e-mail systems today use the Internet, and e-mail is one of the most popular uses of the Internet.

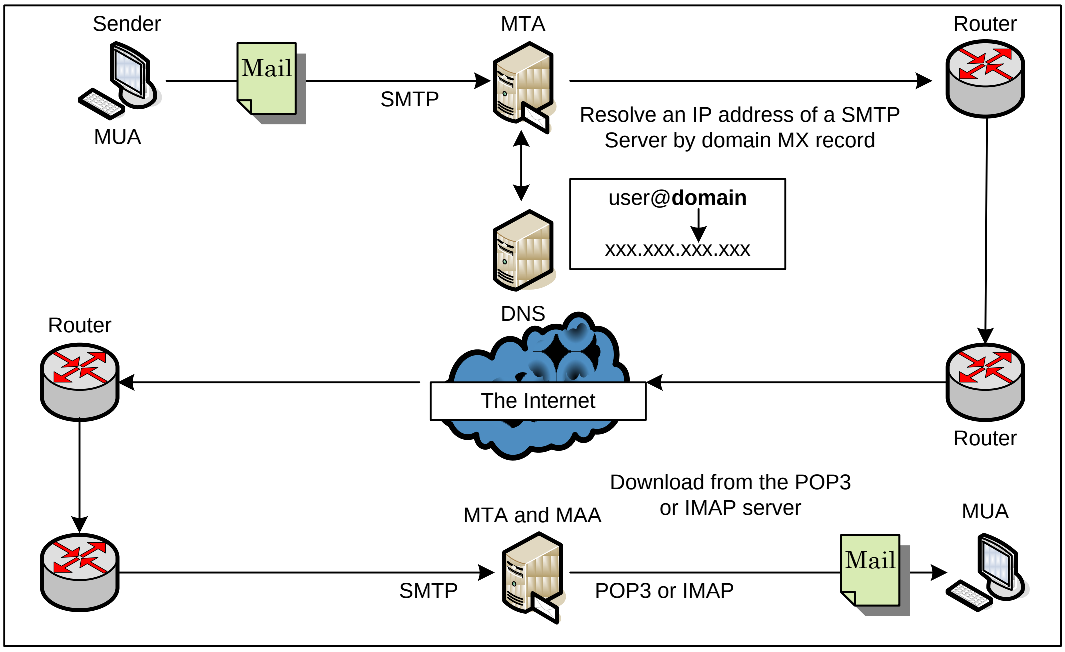


Figure 13 – How E-Mail Works

- MTA (Mail Transfer Agent): SMTP (tcp 25), postfix, sendmail
- MAA (Mail Access Agent): POP 3 (tcp 110), IMAP (tcp 143), courier-imap, cyrus-imapd, dovecot, imap, qpopper.
- MUA (Mail User Agent): Thunderbird, Outlook, Web mail

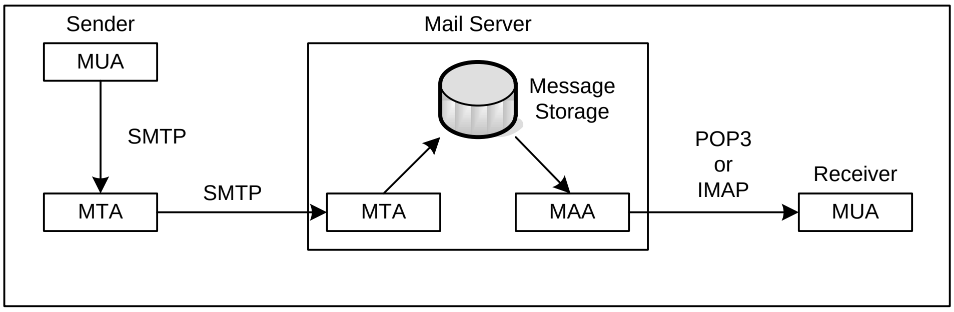


Figure 14 – Mail System Architecture

Followings are the protocols used by email system.

- SMTP (Simple Mail Transfer Protocol): To transfer email between computers
- POP3 (Post Office Protocol 3): To download email from POP3 server
- IMAP (Internet Message Access Protocol): To access remote message folder without downloading.

Postfix is an open source MTA (Mail Transfer Agent), a computer program for the routing and delivery of email, that is intended as a fast, easy to administer and secure alternative to the widely-used Sendmail.

7.2. Postfix Configuration

You are going to setup a mail server for the domain example.com. This mail server will be called mail.example.com. For this exercise, assume that the necessary entries exist in DNS, especially MX (mail exchanger) record for your domain pointing to your mail server. There should be a PTR record in DNS to support reverse lookup of your mail server's IP address.

```
# dig mail.domain1.site  +short
# dig pop3.domain1.site +short
# dig smtp.domain1.site +short
# dig domain1.site mx +short
# dig -x 192.168.0.10 +short
```

Postfix itself requires only one package of,

- `postfix`

Install Postfix if it is not installed.

```
# rpm -qa | grep postfix
```

Stop AppArmor by YaST. Open YaST, [Novell AppArmor], [AppArmor Control Panel], then disable the AppArmor, otherwise it should be configured.

Postfix can be configured by YaST but the detailed configuration is not possible so we will not use YaST. Backup the YaST configuration file not to use it.

```
# mv /etc/sysconfig/postfix /etc/sysconfig/postfix.bak
```

Edit /etc/postfix/main.cf.

Before you edit, backup the file,

```
# cp /etc/postfix/main.cf /etc/postfix.main.cf.bak
```

Then edit the file /etc/postfix/main.cf,

```
# INTERNET HOST AND DOMAIN NAMES
myhostname = srv1.domain1.site

# The mydomain parameter specifies the local internet domain name.
mydomain = domain1.site

# The myorigin parameter specifies the domain that locally-posted
# mail appears to come from. The default is to append $myhostname,
# which is fine for small sites.  If you run a domain with multiple
# machines, you should (1) change this to $mydomain and (2) set up
# a domain-wide alias database that aliases each user to
# user@that.users.mailhost.
myorigin = $mydomain
#
# listen for everything both inside and out
#
inet_interfaces = all

# The mydestination parameter specifies the list of domains that this
# machine considers itself the final destination for.
mydestination = $myhostname, localhost.$mydomain, localhost, $mydomain

# Specify an explicit list of network/netmask patterns, where the
# mask specifies the number of bits in the network part of a host
# address.
mynetworks = 192.168.0.0/16, 127.0.0.0/8

# The relay_domains parameter restricts what destinations this system will
# relay mail to.  See the smtpd_recipient_restrictions restriction in the
# file sample-smtpd.cf for detailed information.
relay_domains = $mydestination, hash:/etc/postfix/relay

# The alias_maps parameter specifies the list of alias databases used
# by the local delivery agent. The default list is system dependent.
alias_maps = hash:/etc/aliases

# The alias_database parameter specifies the alias database(s) that
# are built with "newaliases" or "sendmail -bi".  This is a separate
# configuration parameter, because alias_maps (see above) may specify
# tables that are not necessarily all under control by Postfix.
alias_database = hash:/etc/aliases

# The home_mailbox parameter specifies the optional pathname of a
# mailbox file relative to a user's home directory. The default
# mailbox file is /var/spool/mail/user or /var/mail/user.  Specify
# "Maildir/" for qmail-style delivery (the / is required).
home_mailbox = Maildir/
```

YaST added unnecessary lines in the file, so remove lines bottom of the file after "readme_directory = /usr/share"

That's it, our configuration is done. Now we have to issue the following commands:

```
# /etc/init.d/postfix restart
```

Send a welcome message to users. This first mail creates `Maildir` directory for their home directory.

```
# echo "Welcome" | mail -s "Welcome" test1@domain1.site
```

Note: Without the first mail, the user will receive an error message when they access the mail box by pop3 protocol. To send a welcome message automatically when a new user is created, edit /usr/sbin/useradd.local to send a message.

```
# When you create a user with useradd, this script will be called
# with the login name as parameter. Optional, UID, GID and the HOME
# directory are added.
echo "Welcome" | mail -s "Welcome" $1
```

When you create an account, a message is sent.

```
# useradd -m user1
# passwd user1
# ll /home/user1/Maildir/
total 12
drwx------ 2 user1 users 4096 Jan 28 11:04 cur
drwx------ 2 user1 users 4096 Jan 28 11:04 new
drwx------ 2 user1 users 4096 Jan 28 11:04 tmp
```

7.2.1. aliases

The aliases table provides a system-wide mechanism to redirect mail for local recipients. Edit /etc/aliases, and add one line as below. The message to root user will be redirected to admin user.

```
…
root:   admin
```

Note: user name admin must be existed in the system.

This initializes the aliase database.

```
# newaliases
```

Then a user admin will receive root user’s message.

7.2.2. Postfix Troubleshooting

Check /var/log/mail for any system messages as

```
# less /var/log/mail
```

Press “G” to move the bottom of this file.

This command always shows the bottom of the file, and then you can monitor.

```
# tail -f /var/log/mail
```

Table 14 – Postfix log files

File	Description
`/var/log/mail`	All messages
`/var/log/mail.err`	Error messages
`/var/log/mail.info`	Information messages
`/var/log/mail.warn`	Warning messages

7.3. POP3, POP3-SSL, IMAP and IMAP-SSL

Installing POP3 and IMAP server is simple. Install courier-imap, and courier-authlib. IMAP daemon requires FAMD (File Access Monitoring Daemon).

- `courier-authlib`
- `courier-imap`
- `fam-server`

Run automatically by `chkconfig`. You might need to uninstall another imap package if it is already installed.

```
# chkconfig courier-authdaemon on
# chkconfig courier-imap on
# chkconfig courier-imap-ssl on
# chkconfig courier-pop on
# chkconfig courier-pop-ssl on
# chkconfig fam on
# chkconfig --list | grep courier
courier-authdaemon      0:off  1:off  2:off  3:on   4:off  5:on   6:off
courier-imap            0:off  1:off  2:off  3:on   4:off  5:on   6:off
courier-imap-ssl        0:off  1:off  2:off  3:on   4:off  5:on   6:off
courier-pop             0:off  1:off  2:off  3:on   4:off  5:on   6:off
courier-pop-ssl         0:off  1:off  2:off  3:on   4:off  5:on   6:off
# /etc/init.d/courier-authdaemon restart
# /etc/init.d/courier-imap restart
# /etc/init.d/courier-imap-ssl restart
# /etc/init.d/courier-pop restart
# /etc/init.d/courier-pop-ssl restart
# /etc/init.d/fam restart
```

Note: You should start `courier-authdaemon` before `pop` and `imap`

7.3.1. POP3-SSL, IMAP-SSL

POP3-SSL and IMAP-SSL certificates are already generated. However, the common name is configured as localhost. To modify the certificate for your organization, edit /etc/courier/pop3d.cnf and /etc/courier/imapd.cnf.

```
# C=US
# ST=NY
# L=New York
# O=Courier Mail Server
# OU=Automatically-generated POP3 SSL key
# CN=localhost
# emailAddress=postmaster@example.com
C=MM
ST=YG
L=Yangon
O=ICTTI
OU=Certificate Authority
CN=pop3.domain1.site
emailAddress=root@domain1.site
```

Generate Certificate for POP3-SSL and IMAP-SSL.

```
# mkpop3dcert
# mkimapdcert
```

Restart the servers.

```
# rccourier-pop restart
# rccourier-pop-ssl restart
# rccourier-imap restart
# rccourier-imap-ssl restart
```

Note:

If you see the following error,

```
Oct 10 03:12:59 servers imapd: Error: Input/output error
Oct 10 03:12:59 servers imapd: Check for proper operation and configuration
Oct 10 03:12:59 servers imapd: of the File Access Monitor daemon (famd).
Oct 10 03:12:59 servers imapd: Failed to create cache file: maildirwatch
```

```
(user)
```

You can solve it as follows:

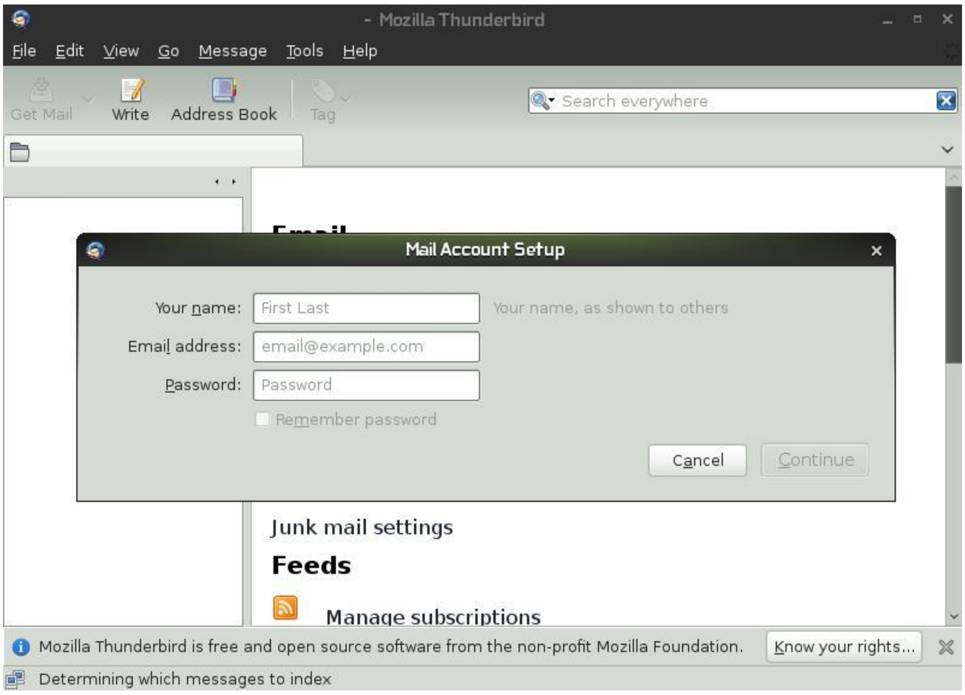
```
# vi /etc/xinetd.d/fam
#
# Add  "flags      = NOLIBWRAP" optionts
#
# so the configuration like :
#
service fam
{
 socket_type  = stream
 protocol     = tcp
 wait         = yes
 user         = root
 group        = root
 server       = /usr/sbin/famd
 disable      = yes
 type         = RPC UNLISTED
 rpc_version  = 2
 rpc_number   = 391002
 flags        = NOLIBWRAP
}
```

7.4. Mail Client Configuration (Thunderbird)

Mozilla Thunderbird is a free, cross-platform e-mail client. Install only a package of,

- MozillaThunderbird

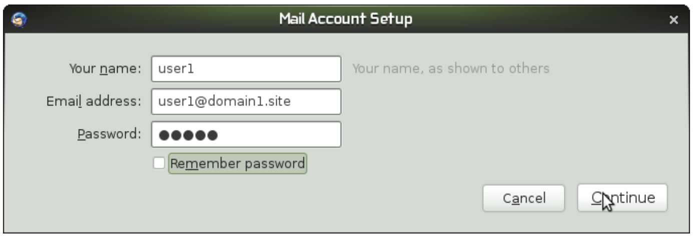
When you start Thunderbird, the following wizard starts automatically.



Your name: First Last — Your name, as shown to others
Email address: email@example.com
Password: Password
□ Remember password

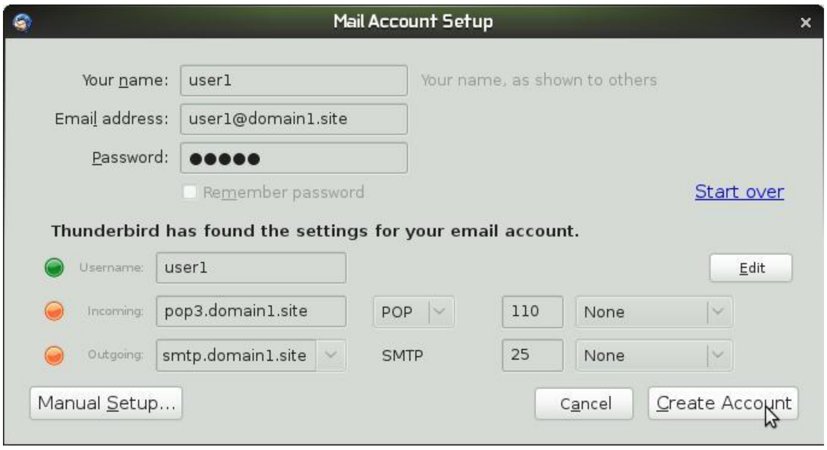
Mozilla Thunderbird is free and open source software from the non-profit Mozilla Foundation.
Determining which messages to index

Fill the user account information as shown in below.



Your name: user1 — Your name, as shown to others
Email address: user1@domain1.site
Password: ●●●●●
□ Remember password

Click [Continue]. This thunderbird version can automatically search the incoming server and outgoing server information for that user account and you will see as follows. Then this account can be created.



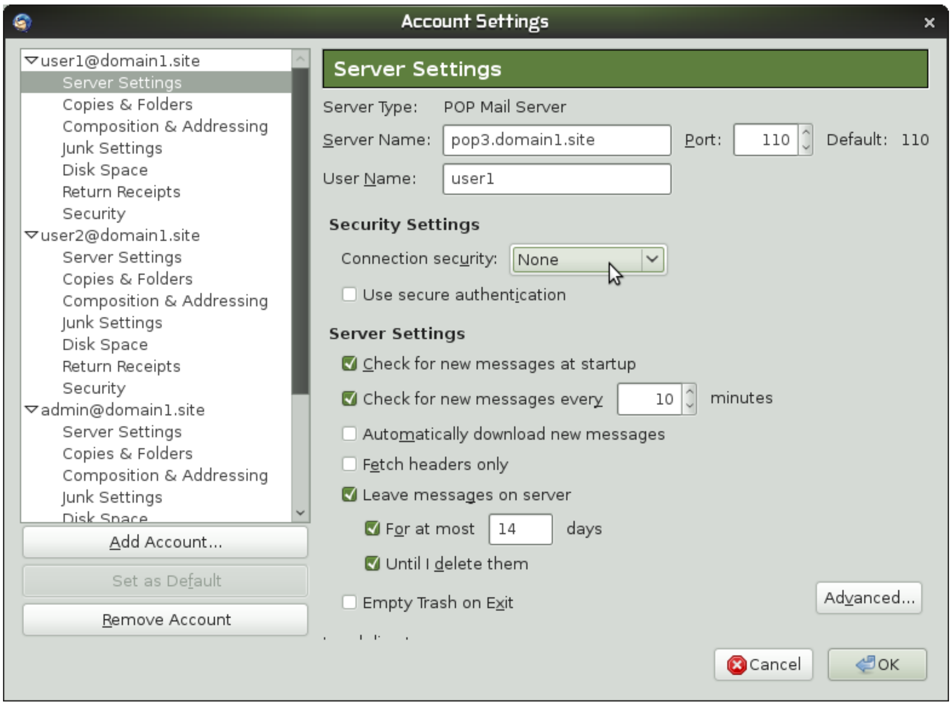
Your name: user1 — Your name, as shown to others
Email address: user1@domain1.site
Password: ●●●●●
□ Remember password

Thunderbird has found the settings for your email account.

Username:	user1			
Incoming:	pop3.domain1.site	POP	110	None
Outgoing:	smtp.domain1.site	SMTP	25	None

Select "Create account", and click "Next"

Change the security setting of POP server, as TLS, or SSL. Open “Edit”, “Account Settings…” from the menu, and select “Server Settings” at the left pane. TLS uses the same port number as POP3 protocol.



Server Settings

Server Type: POP Mail Server

Server Name: pop3.domain1.site Port: 110 Default: 110

User Name: user1

Security Settings

Connection security: None

□ Use secure authentication

Server Settings

☑ Check for new messages at startup

☑ Check for new messages every 10 minutes

□ Automatically download new messages

□ Fetch headers only

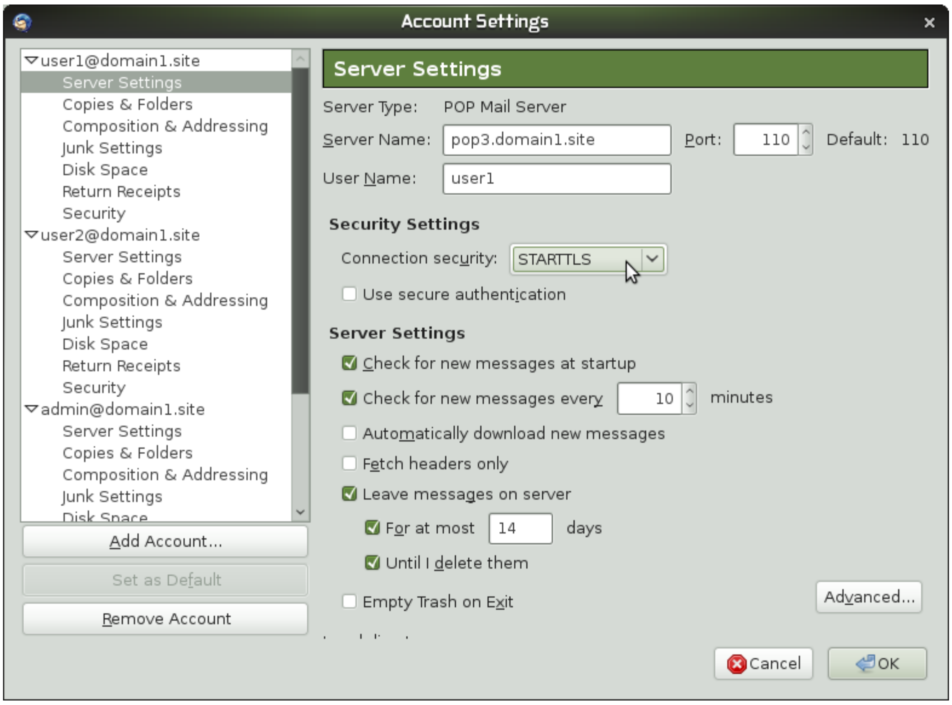
☑ Leave messages on server

☑ For at most 14 days

☑ Until I delete them

□ Empty Trash on Exit

TLS can be used which uses port 110.



Server Settings

Server Type: POP Mail Server

Server Name: pop3.domain1.site Port: 110 Default: 110

User Name: user1

Security Settings

Connection security: STARTTLS

□ Use secure authentication

Server Settings

☑ Check for new messages at startup

☑ Check for new messages every 10 minutes

□ Automatically download new messages

□ Fetch headers only

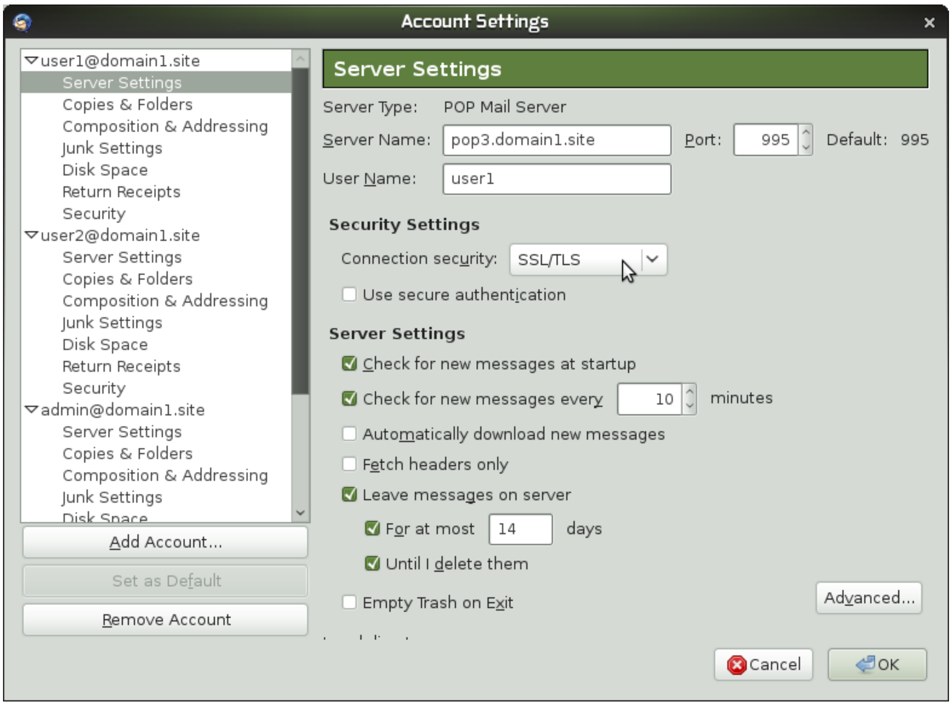
☑ Leave messages on server

☑ For at most 14 days

☑ Until I delete them

□ Empty Trash on Exit

SSL also can be used which uses port 995.



Server Settings

Server Type: POP Mail Server

Server Name: pop3.domain1.site Port: 995 Default: 995

User Name: user1

Security Settings

Connection security: SSL/TLS

□ Use secure authentication

Server Settings

☑ Check for new messages at startup

☑ Check for new messages every 10 minutes

□ Automatically download new messages

□ Fetch headers only

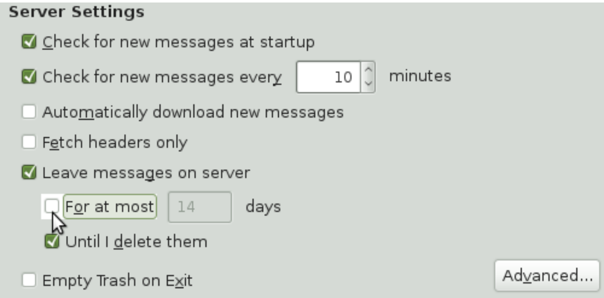
☑ Leave messages on server

☑ For at most 14 days

☑ Until I delete them

□ Empty Trash on Exit

You can leave messages on server. Edit at “Server Settings”.



Server Settings

☑ Check for new messages at startup

☑ Check for new messages every 10 minutes

□ Automatically download new messages

□ Fetch headers only

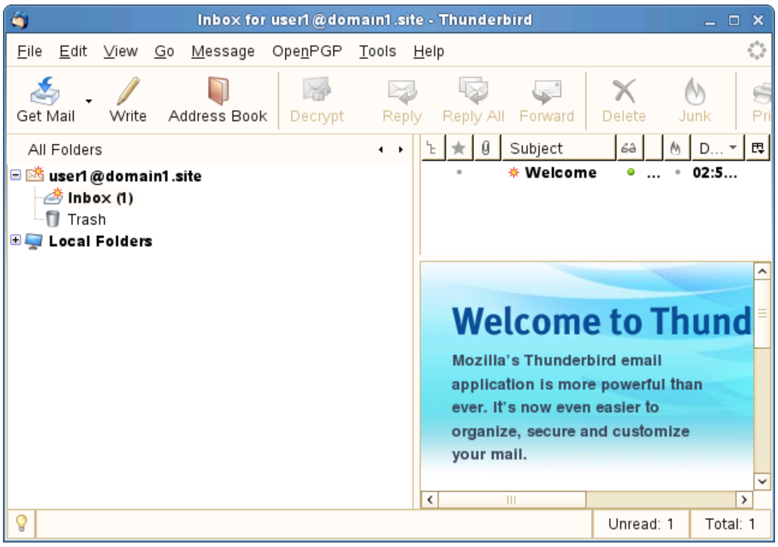
☑ Leave messages on server

□ For at most 14 days

☑ Until I delete them

□ Empty Trash on Exit

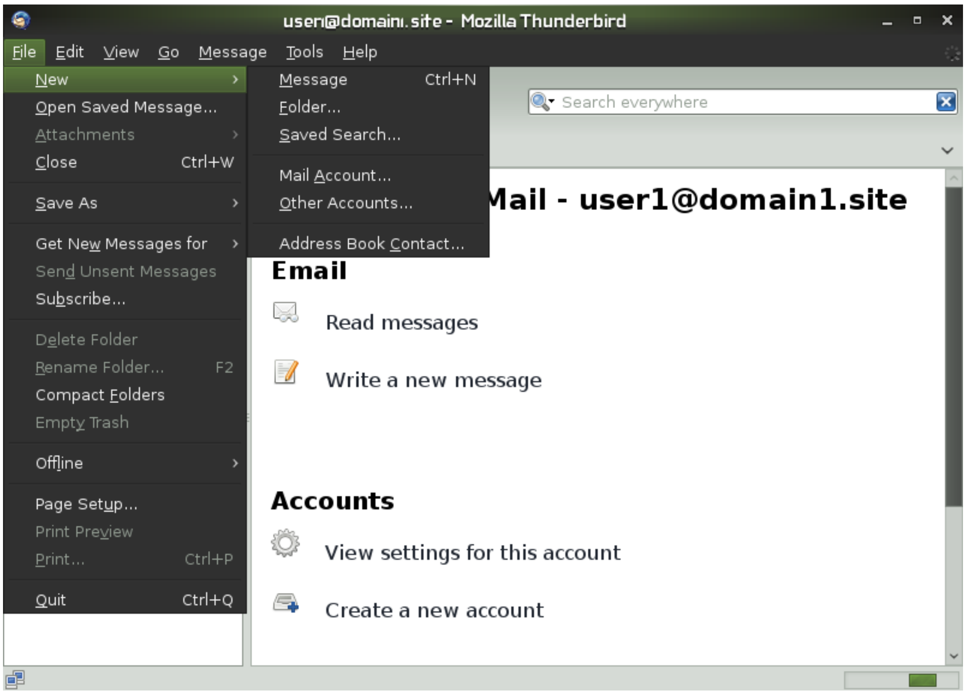
If successfully configured, you will see the welcome message as below,



Welcome to Thund

Mozilla's Thunderbird email application is more powerful than ever. It's now even easier to organize, secure and customize your mail.

If you have multiple email account, Thunderbird can retrieve many accounts from different server. Open "File", "New", "Account…".



7.5. Web Mail (Squirrel Mail)

Squirrel Mail is Web Mail software written by PHP.

7.5.1. Squirrel Mail Configuration

(1) Installation

Download the Squirrel Mail package from http://www.squirrelmail.org/.

- `squirrelmail-1.4.20.tar.gz`

Install following packages by YaST.

- apache2-mod_php5
- php5-mbstring
- php5-gettext
- php5-openssl
- ispell
- ispell-american
- words

To enable the installed Apache modules, restart Apache

```
# rcapache2 restart
```

Install Squirrelmail as,

```
# cp squirrelmail-1.4.20.tar.gz /usr/local/src/
# cd /usr/local/src
# tar zxvf squirrelmail-1.4.20.tar.gz
# cp squirrelmail-1.4.20 /srv/www/htdocs/mail -r
# cd /srv/www/htdocs/mail/
# chown -R root:www data/
# chmod 770 data
# chmod 664 data/*
# mkdir /var/lib/squirrelmail -m 755
# mkdir /var/lib/squirrelmail/attach -m 770
# chown root:www -R /var/lib/squirrelmail/
```

To change the system directory configuration, copy `config_default.php` as `config.php` under `/srv/www/htdocs/mail/config/`

```
#cp config_default.php config.php
```

Edit `config.php`.

```
// $data_dir = '/var/local/squirrelmail/data/';
// $attachment_dir = '/var/local/squirrelmail/attach/';
$data_dir = SM_PATH . 'data/';
```

```
$attachment_dir = '/var/lib/squirrelmail/attach/';
```

When a user is aborting a mail but has uploaded some attachments to it the files will be kept in the directory forever, so remove them by a cron script. Create a file /etc/cron.daily/squirrelmail.

```
find /var/lib/squirrelmail/attach/* -atime +2 -exec /bin/rm {} \;
```

Change the permission

```
# chmod 755 /etc/cron.daily/squirrelmail
```

Configure SquirrelMail by a configuration tool located at the squirrelmail directory as /srv/www/htdocs/mail/configure.

```
# cd /srv/www/htdocs/mail/
# ./configure
```

(2) IMAP Configuration

This is the main menu. Press “D” to choose a pre-defined setting for Curier IMAP.

```
SquirrelMail Configuration : Read: config.php (1.4.0)
---------------------------------------------------------
Main Menu --
1.  Organization Preferences
2.  Server Settings
3.  Folder Defaults
4.  General Options
5.  Themes
6.  Address Books (LDAP)
7.  Message of the Day (MOTD)
8.  Plugins
9.  Database
10. Languages

D.  Set pre-defined settings for specific IMAP servers


C.  Turn color on
S   Save data
Q   Quit
```

```

Command >> D
```

Type “courier” and enter.

```
…
Please select your IMAP server:
    bincimap    = Binc IMAP server
    courier     = Courier IMAP server
    cyrus       = Cyrus IMAP server
    dovecot     = Dovecot Secure IMAP server
    exchange    = Microsoft Exchange IMAP server
    hmailserver = hMailServer
    macosx      = Mac OS X Mailserver
    mercury32   = Mercury/32
    uw          = University of Washington's IMAP server
    gmail       = IMAP access to Google mail (Gmail) accounts

    quit        = Do not change anything
Command >> courier

    imap_server_type = courier
    default_folder_prefix = INBOX.
    trash_folder = Trash
    sent_folder = Sent
    draft_folder = Drafts
    show_prefix_option = false
    default_sub_of_inbox = false
    show_contain_subfolders_option = false
    optional_delimiter = .
    delete_folder = true

Press any key to continue...
```

(3) Orgnaization Preferences

At the main menu, press “1” to change the Organization Preferences.

```
SquirrelMail Configuration : Read: config.php (1.4.0)
```

```
---------------------------------------------------------
Organization Preferences
1.  Organization Name     : ICTTI
2.  Organization Logo     : ../images/sm_logo.png
3.  Org. Logo Width/Height : (308/111)
4.  Organization Title    : SquirrelMail $version
5.  Signout Page          :
6.  Top Frame             : _top
7.  Provider link         : http://www.squirrelmail.org/
8.  Provider name         : SquirrelMail

R   Return to Main Menu
C   Turn color on
S   Save data
Q   Quit

Command >>
```

(4) Server Settings

At the main menu, press “2” to change the Server Settings. Change the domain as,

Configure the Server Settings as,

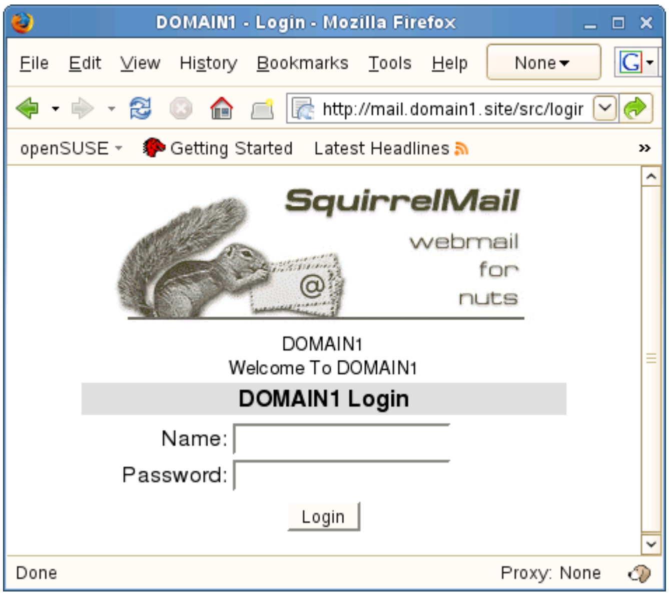
```
SquirrelMail Configuration : Read: config.php (1.4.0)
---------------------------------------------------------
Server Settings

General
-------
1.  Domain                 : domain1.site
2.  Invert Time            : false
3.  Sendmail or SMTP       : SMTP

A.  Update IMAP Settings   : localhost:143 (courier)
B.  Update SMTP Settings   : localhost:25

R   Return to Main Menu
```

```
C   Turn color on
S   Save data
Q   Quit

Command >>
```

(5) Verification

Now you are able to access Squirrel Mail at `http://yourhost/mail/`

You might create a virtual host for the SquirrelMail as `http://`**`mail`**`.yourdomain/`



DOMAIN1 - Login - Mozilla Firefox
File Edit View History Bookmarks Tools Help
None
http://mail.domain1.site/src/logir
openSUSE
Getting Started
Latest Headlines
SquirrelMail
webmail
for
nuts
Login
Done
Proxy: None

DOMAIN1
Welcome To DOMAIN1
DOMAIN1 Login
Name:
Password:

7.5.2. Change Password Plug-in

Allows the user to change own password from the comfort of the SquirrelMail interface. If your email users are system users, this plugin allow your users to change his/her system password in `/etc/passwd` or `/etc/shadow`.

Download followings from `http://www.squirrelmail.org/plugins.php`

- `compatibility-1.3.tar.gz`
- `change_passwd-4.0-1.2.8.tar.gz` (You must use the compatibility version 1.3)

```
# cp change_passwd-4.0-1.2.8.tar.gz /srv/www/htdocs/mail/plugins/
# cp compatibility-1.3.tar.gz /srv/www/htdocs/mail/plugins/
# cd /srv/www/htdocs/mail/plugins/
# tar zxvf change_passwd-4.0-1.2.8.tar.gz
# tar zxvf compatibility-1.3.tar.gz
# cd change_passwd
# cp config.php.sample config.php
```

You may edit config.php as you think necessary.

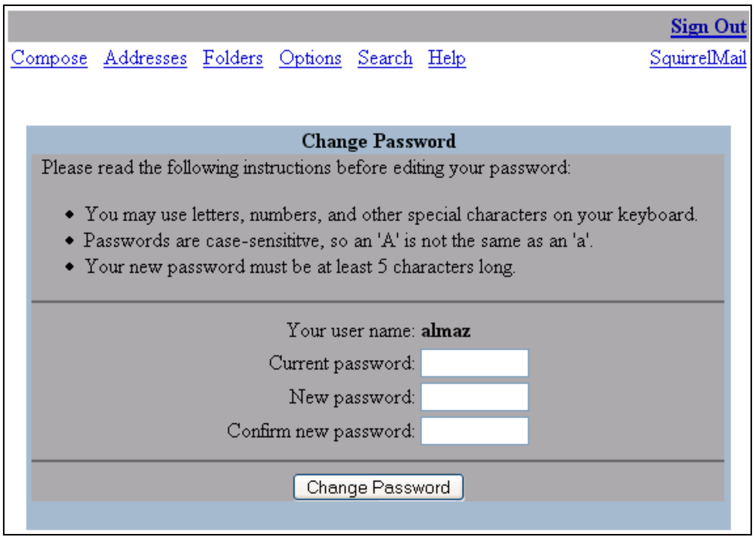
Change the permissions of the `chpasswd` command.

```
# chown root:www chpasswd
# chmod 4750 chpasswd
```

You need to include `compatibility` and `change_passwd` plugins by `configure` command.

```
SquirrelMail Configuration : Read: config.php (1.4.0)
---------------------------------------------------------
Plugins
  Installed Plugins
    1. compatibility
    2. change_passwd

  Available Plugins:
    3. abook_take
…
```

Now you are able to see "Change Password" in the Options screen.



Change Password

Please read the following instructions before editing your password:

- You may use letters, numbers, and other special characters on your keyboard.
- Passwords are case-sensititve, so an 'A' is not the same as an 'a'.
- Your new password must be at least 5 characters long.

Your user name: **almaz**
Current password:
New password:
Confirm new password:

Figure 15 – Change Password Screen

7.5.3. Check Quota Plug-in

Download a following plugin from `http://www.squirrelmail.org/plugins.php`

- `check_quota-1.4-1.2.7.tar.gz`

```
# mv check_quota-1.4-1.2.7.tar.gz /srv/www/htdocs/mail/plugins/
# cd /srv/www/htdocs/mail/plugins/
# tar zxvf check_quota-1.4-1.2.7.tar.gz
# cd check_quota
# cp config.php.sample config.php
```

Edit `config.php` as,

```
// $cq_check_quota_type = 0;
$cq_check_quota_type = 1;
…
// $cq_quota_binary = "/usr/bin/sudo /usr/bin/quota";
$cq_quota_binary = "/usr/bin/sudo /usr/bin/cqcheck";
…
// $cq_do_not_use_flash = 1;
$cq_do_not_use_flash = 0;
```

The `$cq_check_quota_type` option uses UNIX quotas instead of IMAP quotas. The IMAP quotas do not work with courier-imap.

The `$cq_do_not_use_flash` option can be used both Flash and HTML.

Copy the `quota` commad to `cqcheck`.

```
# cp /usr/bin/quota /usr/bin/cqcheck
```

Change the `/etc/sudoers` file to be writeable permission.

```
# chmod u+w sudoers
```

Edit `/etc/sudoers` file, and add one line at the end as,

```
wwwrun  ALL=NOPASSWD: /usr/bin/cqcheck -v *
```

So the command `cqcheck` executed by `wwwrun` user will have a privilege of `root` user.

Change the `/etc/sudoers` file to be read only.

```
# chmod 440 sudoers
```

If you can get quota output by the following command, your configuration is fine.

```
# su - wwwrun
# sudo /usr/bin/cqcheck -v user1
Disk quotas for user user1 (uid 1001):
    Filesystem blocks   quota   limit   grace   files   quota   limit   grace
     /dev/sda2     216  100000  200000             56       0       0
```

You need to include `check_quota` plugin by `configure` command.

```
SquirrelMail Configuration : Read: config.php (1.4.0)
---------------------------------------------------------
Plugins
  Installed Plugins
    1. change_passwd
    2. compatibility
    3. check_quota
```

Now you are able to see "Quota Usage" below folders as Figure 16. This is the Flash version.

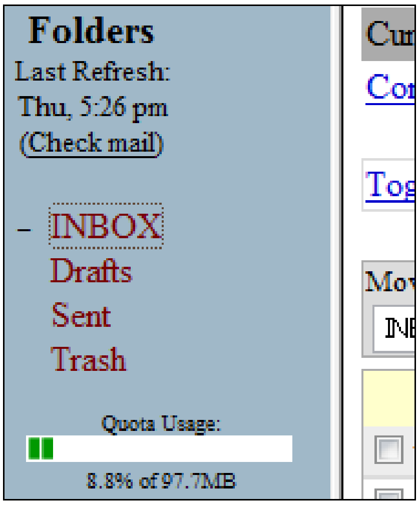


Figure 16 – Check Quota Plugin by Flash

7.6. SMTP Authentication

Email spam is known as bulk or junk email. The SMTP protocol has not authentication by default, so the spammer can pretend to relay a message from any email address. To prevent this, many email providers require the use of SMTP-AUTH, allowing positive identification of the specific account from which an email originates.

Spammers frequently seek out and make use of vulnerable systems such as opne mail relays and open proxy servers. The SMTP system forwards mail from one server to another. Mail servers that ISPs run normally require SMTP-AUTH. However, open relays servers do not properly check who is using the mail server and pass all mail to the destination address. Once your server is marked as an open relay, and blacklisted, your message from the server will never received from the majority of SMTP systems.

Nowadays, 80-85% of incoming mail is “abusive mail”. In 2007, 90 billion of spam messages are exchanged in the Internet. Spammers use networks of virus-infected PCs which is also called zombies or Botnets. In June 2006, an estimated 80% of email spams were sent by Botnets, increase of 30% from the prior year.

7.6.1. SMTP-AUTH Configuration

SMTP-AUTH extends SMTP to include an authentication step through which the client logs in to the mail server during the process of sending mail.

Install `cyrus-sasl-plain` and `cyrus-sasl-saslauthd` RPM to enable plain authentication

- cyrus-sasl-plain
- cyrus-sasl-saslauthd

To configure SMTP Authentication, we need to modify `main.cf`. Add following lines to the end of `/etc/postfix/main.cf`

```
# SMTP-AUTH
smtpd_sasl_auth_enable = yes
smtpd_sasl_security_options = noanonymous
smtpd_recipient_restrictions = permit_sasl_authenticated,reject_unauth_destination
broken_sasl_auth_clients=yes
smtpd_delay_reject=yes
```

The above configuration forces the client to use the SMTP-AUTH otherwise rejected.

Start `saslauthd`, and restart `postfix`

```
# chkconfig saslauthd on
# /etc/init.d/saslauthd start
# /etc/init.d/postfix restart
```

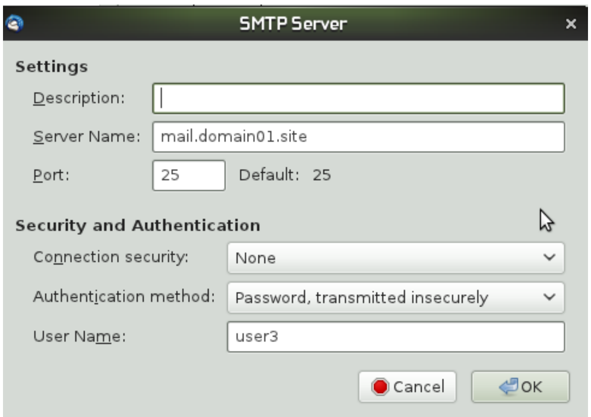
Once you configured SMTP AUTH, you should test it. Connect port 25 by telnet and type EHLO localhost. You should confirm to see `250 AUTH`…

```
# telnet localhost 25
Trying 127.0.0.1...
Connected to localhost.
Escape character is '^]'.
220 srv1.domain1.site ESMTP Postfix
EHLO localhost
…
250-AUTH PLAIN LOGIN
250-AUTH=PLAIN LOGIN
…
QUIT
```

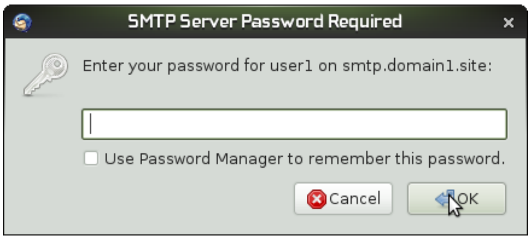
If you see "**`AUTH LOGIN PLAIN`**", SMTP authentication is properly installed.

To enable SMTP Authentication at Thunderbird, open "Account Settings…" from the menu, select "Outgoing Server (SMTP)" at the left pane, and select your SMTP server, and click

“Edit” button. “Use name and password” checkbox should be enabled, and the user name is used for the authentication. Without the authentication, the message is rejected to send.


SMTP Server
Settings
Description:
Server Name: mail.domain01.site
Port: 25 Default: 25
Security and Authentication
Connection security: None
Authentication method: Password, transmitted insecurely
User Name: user3
Cancel
OK

When you send a message, you are asked to enter a password of the user. Without this authentication, you cannot send any message.


SMTP Server Password Required
Enter your password for user1 on smtp.domain1.site:
□ Use Password Manager to remember this password.
Cancel
OK

7.6.2. SMTP-TLS

Transport Layer Security (TLS, formerly called SSL) provides certificate-based authentication and encrypted sessions. An encrypted session protects the information that is transmitted with SMTP mail or with SASL authentication.

Using TLS, the Postfix SMTP server needs a certificate and a private key. This will make an X.509 certificate and corresponding private key for the SMTP server. The common name should be the SMTP server’s FQDN.

```
# cd /usr/local/ca
# openssl genrsa -out smtp-server.key 1024
# openssl req -new -x509 -key smtp-server.key -out smtp-server.crt
…
-----
Country Name (2 letter code) [AU]:MM
State or Province Name (full name) [Some-State]:Yangon
Locality Name (eg, city) []:Hlaing
```

```
Organization Name (eg, company) [Internet Widgits Pty Ltd]:DOMAIN1
Organizational Unit Name (eg, section) []:Certificate Authority
Common Name (eg, YOUR name) []:smtp.domain1.site
Email Address []:root@domain1.site
```

We need to move the new keys and certs into the proper directories

```
# chmod 400 *.key
# mkdir /etc/postfix/ssl/
# cp smtp-server.crt smtp-server.key /etc/postfix/ssl/
```

Add following lines to `/etc/postfix/main.cf` for TLS configuration

```
# SMTP-TLS (SSL)
smtpd_tls_cert_file = /etc/postfix/ssl/smtp-server.crt
smtpd_tls_key_file = /etc/postfix/ssl/smtp-server.key
smtpd_tls_session_cache_database = sdbm:/etc/postfix/ssl/smtpd_scache
smtpd_tls_loglevel = 1
smtpd_use_tls = yes
tls_daemon_random_source= dev:/dev/urandom
```

The file `/etc/postfix/master.cf` needs to be modified. First, backup the file.

```
# cp master.cf master.cf.bak
```

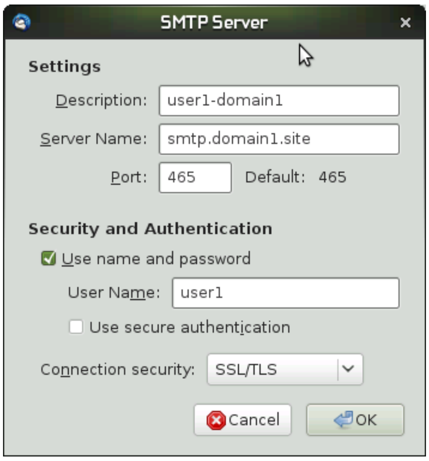
Edit at following lines of `master.cf`. Uncomment *submission*, *smtps*, and *tlsmgr* lines.

```
submission inet n      -      n      -      -      smtpd
     -o smtpd_client_restrictions=permit_sasl_authenticated,reject
...
smtps    inet  n      -      n      -      -      smtpd -o smtpd_tls_wrappermode=yes
...
tlsmgr    unix  -      -      n      1000?   1      tlsmgr
```

Restart Postfix

```
# /etc/init.d/postfix restart
```

Configure SMTP SSL connection from the mail client. Select “TLS” to use TLS connection only.



SMTP Server

Settings

Description: user1-domain1

Server Name: smtp.domain1.site

Port: 465 Default: 465

Security and Authentication

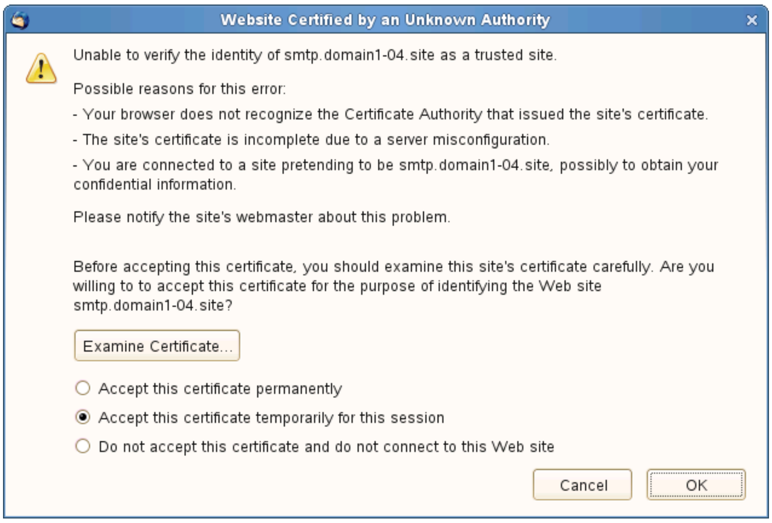
☑ Use name and password

User Name: user1

□ Use secure authentication

Connection security: SSL/TLS

When you send a message, "Website Certificated by an Unknown Authority" will appear. You can examine the certificate, and the configuration is alright, you can accept this certificate.



Website Certified by an Unknown Authority

Unable to verify the identity of smtp.domain1-04.site as a trusted site.

Possible reasons for this error:

- Your browser does not recognize the Certificate Authority that issued the site's certificate.
- The site's certificate is incomplete due to a server misconfiguration.
- You are connected to a site pretending to be smtp.domain1-04.site, possibly to obtain your confidential information.

Please notify the site's webmaster about this problem.

Before accepting this certificate, you should examine this site's certificate carefully. Are you willing to to accept this certificate for the purpose of identifying the Web site smtp.domain1-04.site?

○ Accept this certificate permanently
● Accept this certificate temporarily for this session
○ Do not accept this certificate and do not connect to this Web site

If you have successfully sent a message, the log file `/var/log/mail` would show as,

```
Jul 21 10:59:23 suse113 postfix/smtpd[3465]: Anonymous TLS connection established from
suse113.domainx.site[192.168.114.130]: TLSv1 with cipher DHE-RSA-CAMELLIA256-SHA (256/256
bits
Jul    21    10:59:34    suse113    postfix/smtpd[3465]:    29350E5C09:
client=suse113.domainx.site[192.168.114.130], sasl_method=PLAIN, sasl_username=user2
Jul    21    10:59:34    suse113    postfix/cleanup[3475]:    29350E5C09:
message-id=<4E27AB23.2070802@domainx.site>
```

```
Jul 21 10:59:34 suse113 postfix/qmgr[3408]: 29350E5C09: from=<admin@domainx.site>, size=642,
nrcpt=4 (queue active)
Jul 21 10:59:34 suse113 postfix/smtpd[3465]: disconnect from
suse113.domainx.site[192.168.114.130]
Jul 21 10:59:34 suse113 postfix/local[3476]: 29350E5C09: to=<admin@domainx.site>,
relay=local, delay=0.36, delays=0.1/0.08/0/0.18, dsn=2.0.0, status=sent (delivered to
maildir)
Jul 21 10:59:34 suse113 postfix/local[3477]: 29350E5C09: to=<user1@domainx.site>,
relay=local, delay=0.37, delays=0.1/0.13/0/0.13, dsn=2.0.0, status=sent (delivered to
maildir)
```

7.7. Spam and Virus Filtering

The configuration of Postfix with Spam Assassin and Clam AV is able to block spam, as well as virus infected messages at your mail server. To make this configuration works, Amavisd-new package is used to interface between Postfix, Clam AV and Spam Assassin.

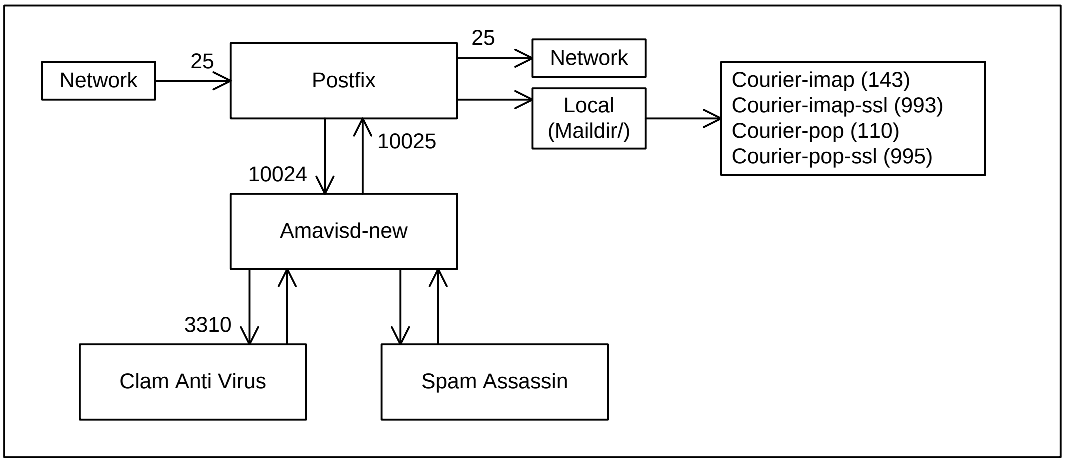


Figure 17 – Spam and Virus Filtering Architecture

Amavisd-new is an interface between MTA (postfix) and content checkers such as virus scanners. In this configuration, we use Clam Antivirus as a virus scanner.

Clam Antivirus is an anti-virus toolkit for UNIX. This software should be already installed. The configuration should be done at the Samba. This software can integrate with mail server to scan attachments. It can be used in conjunction with amavisd-new and postfix to provide a combined e-mail filter for spam and viruses.

SpamAssassin is e-mail spam filtering based on content-matching rules supported by external program and online databases.

7.7.1. Spam Assassin

Before starting, your postfix should be working fine. You can install SpamAssassin from YaST or rpm package.

- `spamassassin`

SpamAssassin configuration file is at `/etc/mail/spamassassin/local.cf`. We will not change it this time.

Start the SpamAssassin daemon,

```
# chkconfig spamd on
# /etc/init.d/spamd restart
```

Spam filters are prepared at `/usr/share/spamassassin`

7.7.2. Amavisd-new

Install Amavisd-new package.

- `amavisd-new`

Edit lines at `/etc/amavisd.conf`, and uncomment and modify ClamAV lines,

```
…
$mydomain = 'domain1.site';   # a convenient default for other settings
…
$myhostname = 'srv1.domain1.site';
…
# $final_spam_destiny       = D_BOUNCE;
$final_spam_destiny       = D_PASS;
…
# ### http://www.clamav.net/
['ClamAV-clamd',
  \&ask_daemon, ["CONTSCAN {}\n", "/var/run/clamd/clamd"],
  qr/\bOK$/, qr/\bFOUND$/,
  qr/^.*?: (?!Infected Archive)(.*) FOUND$/ ],
```

Before starting the service, run as debug mode,

```
# amavisd debug
```

You will see as,

```
…
Jul  21  11:36:44.148  suse113.domainx.site  /usr/sbin/amavisd[3686]:
Using primary internal av scanner code for ClamAV-clamd
…
Jul  21  11:36:44.409  suse113.domainx.site  /usr/sbin/amavisd[3686]:
initializing Mail::SpamAssassin
Jul  21  11:36:54.550  suse113.domainx.site  /usr/sbin/amavisd[3686]:
SpamControl: init_pre_fork on SpamAssassin done
 …
```

From another window, check that it is listening on a local SMTP port 10024 (the default port):

```
# telnet localhost 10024
Trying 127.0.0.1...
Connected to localhost.
Escape character is '^]'.
220 [127.0.0.1] ESMTP amavisd-new service ready
quit
221 2.0.0 [127.0.0.1] amavisd-new closing transmission channel
Connection closed by foreign host.
#
```

Press `Control+C` to stop the debug mode.

Start amavisd-new

```
# chkconfig amavis on
# /etc/init.d/amavis restart
Shutting down virus-scanner (amavisd-new):                          done
Starting virus-scanner (amavisd-new):                               done
```

7.7.3. Postfix

Edit `/etc/postfix/master.cf`. Add “`-o content_fileter=`” line under *`pickup`*, and append rest of lines at the end of file.

```
pickup   fifo  n      -      n      60     1      pickup
    -o content_filter=
…
## Amavis-new
smtp-amavis unix -     -      n      -      2  smtp
    -o smtp_data_done_timeout=1200
    -o smtp_send_xforward_command=yes
    -o disable_dns_lookups=yes
    -o max_use=20

127.0.0.1:10025 inet n  -      n      -      -  smtpd
    -o content_filter=
    -o local_recipient_maps=
    -o relay_recipient_maps=
    -o smtpd_restriction_classes=
    -o smtpd_delay_reject=no
    -o smtpd_client_restrictions=permit_mynetworks,reject
    -o smtpd_helo_restrictions=
    -o smtpd_sender_restrictions=
    -o smtpd_recipient_restrictions=permit_mynetworks,reject
    -o smtpd_data_restrictions=reject_unauth_pipelining
    -o smtpd_end_of_data_restrictions=
    -o mynetworks=127.0.0.0/8
    -o strict_rfc821_envelopes=yes
    -o smtpd_error_sleep_time=0
    -o smtpd_soft_error_limit=1001
    -o smtpd_hard_error_limit=1000
    -o smtpd_client_connection_count_limit=0
    -o smtpd_client_connection_rate_limit=0
    -o receive_override_options=no_header_body_checks,no_unknown_recipient_checks
```

Add one line at the end of `/etc/postfix/main.cf`

```
…
# Scanner (Amavisd-new+ClamAV+SpamAssassin)
content_filter=smtp-amavis:[127.0.0.1]:10024
```

Restart Postfix

```
# /etc/init.d/postfix restart
```

7.7.4. Verification

- Spam Mail

Send a sample spam message which is in your system at,

/usr/share/doc/packages/perl-spamassassin/sample-spam.txt

Otherwise use this string at the message body.

```
XJS*C4JDBQADN1.NSBN3*2IDNEN*GTUBE-STANDARD-ANTI-UBE-TEST-EMAIL*C.34X
```

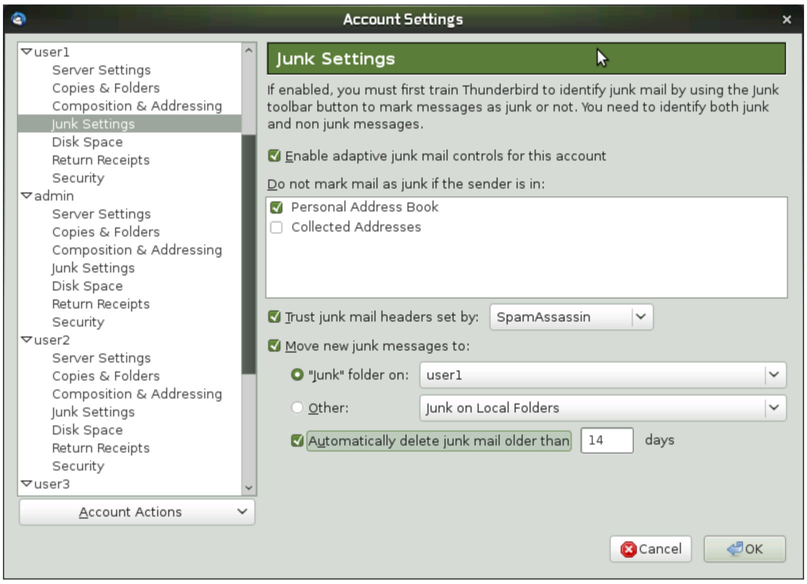
The spam subject would be,

```
****SPAM**** spam test
```

The header would be,

```
X-Virus-Scanned: amavisd-new at domain1.site
X-Spam-Status: Yes, score=998.56 tagged_above=2 required=5
    tests=[ALL_TRUSTED=-1.44, GTUBE=1000]
X-Spam-Score: 998.56
X-Spam-Level:
****************************************************************
X-Spam-Flag: YES
```

This is the configuration of junk mail for Thunderbird. Open “Account Settings”, and select “Junk Settings” from the main menu for each account. The options could be as below. All the messages marked as junk by SpamAssassin will move to Junk folder automatically, and then removed after 14 days.



Junk Settings

If enabled, you must first train Thunderbird to identify junk mail by using the Junk toolbar button to mark messages as junk or not. You need to identify both junk and non junk messages.

☑ Enable adaptive junk mail controls for this account

Do not mark mail as junk if the sender is in:

☑ Personal Address Book
□ Collected Addresses

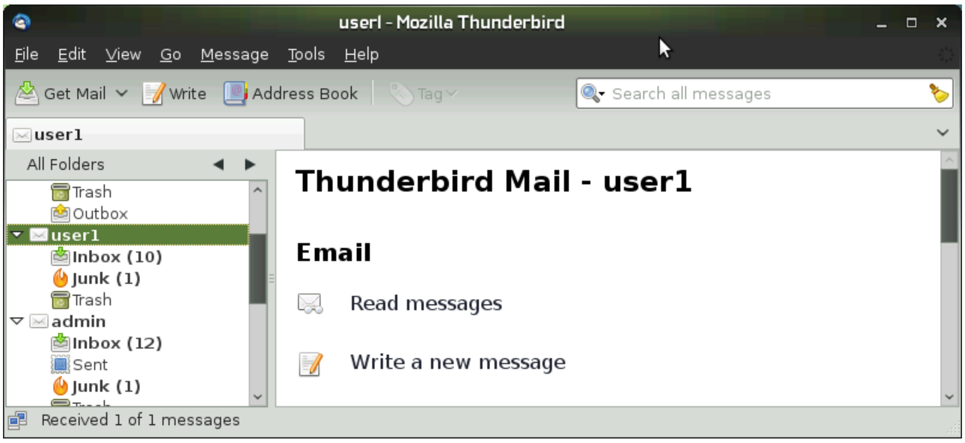
☑ Trust junk mail headers set by: SpamAssassin

☑ Move new junk messages to:

● "Junk" folder on: user1
○ Other: Junk on Local Folders

☑ Automatically delete junk mail older than 14 days

The spam message automatically moved into “Junk” folder.



Thunderbird Mail - user1

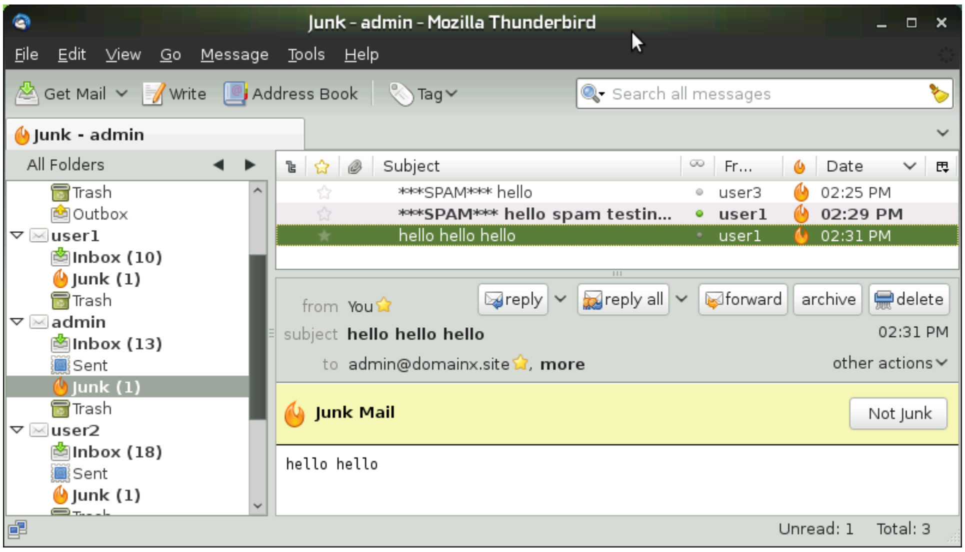
Email

Read messages

Write a new message

Received 1 of 1 messages

If you think this is not junk, click “This is Not Junk” button, then this type of message will not move next time.



Subject	Fr...	Date
SPAM hello	user3	02:25 PM
SPAM hello spam testin...	user1	02:29 PM
hello hello hello	user1	02:31 PM

from You
subject hello hello hello 02:31 PM
to admin@domainx.site, more

Junk Mail

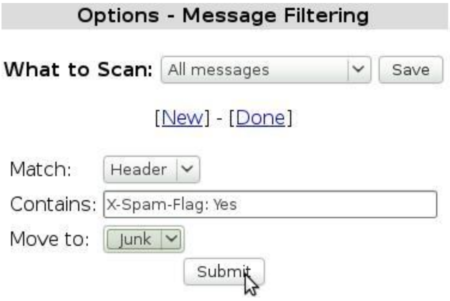
hello hello

By using web mail (squirrelmail), we can filter the spam mail as follows:

First, "filters" plugin is needed to install from existing available plugins by using "configure" command.

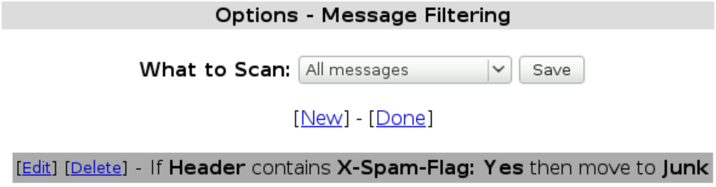
```
SquirrelMail Configuration : Read: config.php (1.4.0)
---------------------------------------------------------
Plugins
  Installed Plugins
    1. filters
```

Second, we need to add message filter rule in "Message Filtering" option. Since we used Spamassassin that means System Header as a rule will use X-Spam-Flag: YES to control. See in below:



What to Scan: All messages

Match: Header
Contains: X-Spam-Flag: Yes
Move to: Junk



Options - Message Filtering

What to Scan: All messages Save

[New] - [Done]

[Edit] [Delete] - If **Header** contains **X-Spam-Flag: Yes** then move to **Junk**

- Virus Mail

In the all messages passing the server, mail header will have,

```
X-Virus-Scanned: amavisd-new at domain1.site
```

Download a virus test file from http://www.eicar.org/anti_virus_test_file.htm

Attach the virus file and send. The root user (or the alias user) will receive a virus alert message.

The subject would be,

```
VIRUS (Eicar-Test-Signature) FROM LOCAL [127.0.0.1] <?@[127.0.0.1]>
```

The message body,

```
A banned name was found:
  multipart/mixed | application/x-zip-compressed,.zip,eicar_com.zip | .asc,eicar.com


Scanner detecting a virus: ClamAV-clamd
…
```

Exercise 7 – Postfix Configuration

1. Configure Postfix on your computer
2. Test sending and receiving messages using Thunderbird from the other computer.
3. Make a Virtual host as **mail** for Squirrel Mail access, and install change password and quota check plugins.
4. Configure SMTP Authentication, and SMTP-TLS
5. Install SpamAssassin, Clam Anti-Virus, and Amavisd-new to your Linux box.

References

Bibliography

Brown, C. (2006). *SUSE Linux*. O'Reilly Media. ISBN-10: 059610183X

Haeder, A, Addison, S, Stanger, J, & Gomes, B. (2010). *Lpi linux certification in a nutshell*. O'Reilly Media. 0596804873. ISBN-10: 0596804873

Liu, C, & Albitz, P. (2006). *Dns and bind*. O'Reilly Media. ISBN-10: 0596100574

Negus, C. (2008). *Linux bible: boot up to Ubuntu, Fedora, KNOPPIX, Debian, SUSE, and 13 other distributions.* John Wiley & Sons Inc. ISBN-10: 0470373679

External Links

openSUSE. (http://www.opensuse.org/).

The Apache Software Foundation. (http://www.apache.org/)

The Postfix Home Page. (http://www.postfix.org/)

Samba - opening windows to a wider world. (http://www.samba.org/)

BIND | Internet Systems Consortium. (http://www.isc.org/software/bind)

Tables and Figures

Figures

Tables

Indexes

Keywords