# CERT-In

## Indian Computer Emergency Response Team

*Handling Computer Security Incidents*

# Implementation of Central Logging Server using syslog-ng

**Department of Information Technology**
**Ministry of Communications and Information Technology**
**Govt. of India**

Issue Date: July 28, 2004

# Table of contents

## 1. Introduction

Logging is a record of actions and events that take place on a computer system. Logs are the primary record keepers of system and network activity. Logging has several benefits which include troubleshooting, security and pro-active system administration. It is a primary part of Security and can be used in the detection of attacks and intrusions. It can also provide useful leads in forensic analysis of systems.

The syslog program is a distributed logging interface providing a standardized framework under which programs (both operating system and applications) can issue messages to be stored either on the local system or sent to a remote host. Though, originally written for UNIX, syslog has become a de facto standard for many network devices and is now also available for the Windows platform.

Logging on UNIX systems can be done through the syslog daemon. It listens for messages from either port 514 (UDP) or through /dev/log, the default UNIX domain socket.

## 2. Centralized syslog

In a centralized logging setup, a common server receives all syslog messages from all systems across the network. These include logs/messages from all Unix/Windows servers, Network devices (routers, switches), firewalls, etc.

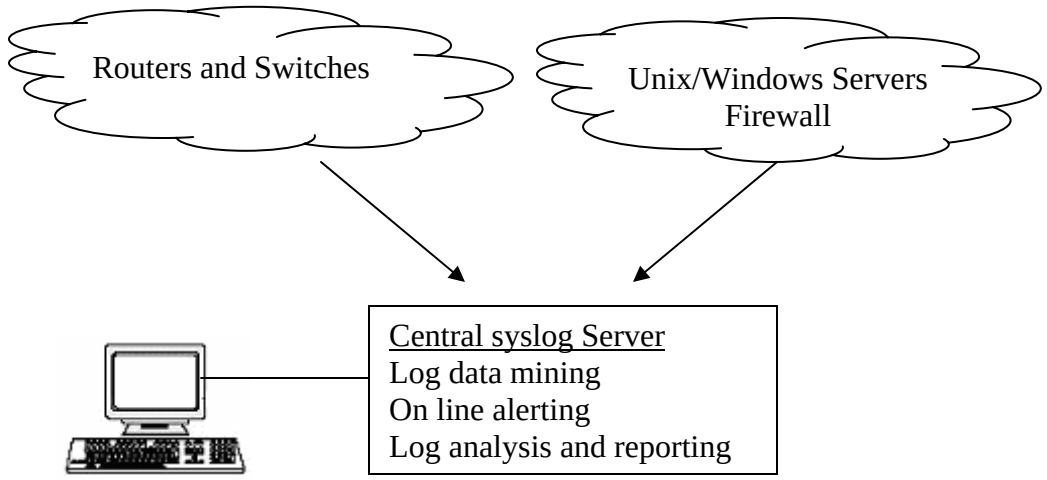


Fig: 1 Centralized Syslog Server

There are several advantages of centralized logging. Some of the advantages of centralized syslogging are as follows.

- The Central syslog can be put on a different segment for secure storage.
- Log messages from all machines could allow for better co-relation of attacks across different platforms.
- Hacker won't be able to delete logs after breaking into a public server.

- Easier Backup Policy, File permission
- Real time alerts can be generated using tools like Swatch (Simple watcher) that can be made to continuously monitor the log files looking for pre-configured signatures.

## 3. syslog levels and facility

Each log message is a single line of text. with two attributes: the log-level or severity and facility.

### 3.1 Levels

The log-level or severity determines the importance of the message. The levels are in order of decreasing importance:

| | |
|---|---|
| LOG_EMERG | A panic condition. This is normally broadcast to all users |
| LOG_ALERT | A condition that should be corrected immediately, such as a corrupted system database. |
| LOG_CRIT | Critical conditions, e.g., hard device errors. |
| LOG_ERR | Error conditions. |
| LOG_WARNING | Warning messages. |
| LOG_NOTICE | Normal, but significant Conditions that should possibly be handled specially. |
| LOG_INFO | Informational messages. |
| LOG_DEBUG | Debug-level Messages |

### 3.2 Facility

The facility argument is used to specify what type of program is logging the message. The developer of a program decides which facility a program will utilize. In some cases, it may be configurable by the end user. Messages from different facilities can be handled differently by editing the syslog configuration file.

| | |
|---|---|
| LOG_AUTH | security/authorization messages (DEPRECATED Use LOG_AUTHPRIV instead) |
| LOG_AUTHPRIV | security/authorization messages (private) |
| LOG_CRON | clock daemon (cron and at) |
| LOG_DAEMON | System daemons without separate facility value |
| LOG_FTP | ftp daemon |
| LOG_KERN | Kernel messages |
| LOG_LOCAL0 through LOG_LOCAL7 | Reserved for local use. |
| LOG_LPR | Line printer subsystem |
| LOG_MAIL | Mail subsystem |
| LOG_NEWS | USENET news subsystem |
| LOG_SYSLOG | messages generated internally by syslogd |
| LOG_USER (default) | generic user-level messages |

| | |
|---|---|
| LOG_UUCP | UUCP subsystem |

## 4. Deployment of Central syslog Server

During the deployment of central syslogging server the following issues should be addressed

### 4.1 Harden the underlying Operating System

The operating system on which syslog server shall be implemented should be hardened

- Minimal installation with only the required services running.
- Disabling unnecessary services (inetd, RPC services etc).
- Configuring iptables to restrict connections to only the desired ports. (eg 514 TCP/UDP)

A detailed Linux OS hardening guideline can be referred at [Ref: 2] CERT-In: Securing Redhat Linux 9.0 as a web server

### 4.2 Clock Synchronization

For proper correlation of log entries across different servers the time of all the devices/systems using the central syslogging server should be synchronized. A NTP server can be used to achieve proper time synchronization.

### 4.3 Server Placement

The syslog server should be placed behind a firewall in a secured segment not accessible from the outside. The firewall should allow traffic only on port 514 TCP/UDP to the syslog server only from trusted machines which have been configured to send logs.

## 5. Default Linux syslog server

Almost all distributions of Linux servers have a syslog daemon by default. However the default configuration of the syslog daemon of Linux doesn't accept syslog messages from the network. To enable a centralized syslog server, one needs to configure the server to listen & accept syslog messages from remote machines across the network.

The syslog server can be configured to accept syslog messages from remote machines across the network by editing the file /etc/sysconfig/syslog

Add -r in the SYSLOGD_OPTIONS so that the line is as shown below.

```
SYSLOGD OPTIONS="-m 0 -r -x"
```

define logging either on the same system or to a central syslog server.
A sample `/etc/syslog.conf` file is shown below

```
kern.*                                                  /dev/console

*.info;mail.none;news.none;authpriv.none;cron.none       @loghost

authpriv.*                                               /var/log/secure

mail.*                                                   /var/log/maillog

cron.*                                                   /var/log/cron

*.emerg                                                  *

uucp,news.crit                                           /var/log/spooler

local7.*                                                 /var/log/boot.log

news.=crit                                          /var/log/news/news.crit
news.=err                                           /var/log/news/news.err
news.notice                                         /var/log/news/news.notice
```

** The IP address of `@loghost` of `/etc/syslog.conf` is defined in `/etc/hosts` so as to enable the system to send the logs to the central syslog server.

# 6. syslog-ng

syslog-ng (new generation) is a centralized syslogging solution by BalaBit IT Security. It provides a centralized, securely stored log of all devices on the network, whatever the platform. syslog-ng also incorporates a host of powerful features, including filtering based on message content, as well as customizable data mining and analysis capabilities.

Some of the advantages of syslog-ng over syslog are:

1. The ability to transport syslog messages over TCP along with UDP.
2. Filtering based on message contents
3. Support for encryption.
4. Ability to run in a chroot-ed environment

## 6.1 Installation

The latest version of syslog-ng and its related libol packages are available at the following sites.

**syslog-ng**
`http://www.balabit.com/downloads/syslog-ng/1.6/src/`

**Libol**
`http://www.balabit.com/downloads/libol/0.3/`

```
libol-0.3.9.tar.gz
libol-0.3.9.tar.gz.asc
```

Check the md5 of the downloaded file

```
# gunzip  libol-0.3.13.tar.gz
# tar xvf  libol-0.3.13.tar
```

Run the commands `configure`, `make`, and `make install` commands to install the package.

Download the latest stable version of syslog-ng.

```
syslog-ng-1.6.4.tar.gz
syslog-ng-1.6.4.tar.gz.asc
```

Check the md5 of the downloaded file

```
# gunzip  syslog-ng-1.6.4.tar.gz
# tar xvf  syslog-ng-1.6.4.tar
```

Run the commands `configure`, `make`, and `make install` commands to install the package.

Refer to [Ref: 6] CERT/CC Advanced Information Assurance Handbook for detailed instructions on installing syslog-ng.

### 6.2 Configuring Server

Create a conf file for syslog-ng `/etc/syslog-ng.conf`

```
options {
         create_dirs(no);dns_cache(yes);use_fqdn(no);keep_hostname(yes);
         long_hostnames(on); use_dns(yes);
};
source gateway {

             unix-stream("/dev/log");
             internal();
             udp(ip(0.0.0.0) port(514));
};
source tcpgateway {

             unix-stream("/dev/log");
             internal();
             tcp(ip(0.0.0.0) port(514) max_connections(1000));
};
destination localhost {
              file("/var/log/syslog-ng.all");
};
destination tcplocalhost {
              file("/var/log/tcpsyslog-ng.all");
};

log {
             source(gateway); destination(localhost);
};
log {
             source(tcpgateway); destination(tcplocalhost);
};
```

The various parameters/options used in the configuration of syslog-ng are as follows.

**i) Options:** Defines the global properties of the configuration file.

**ii) Source:** Defines the source of Log message.
syslog server can accept message either through the default UNIX domain socket or through the network using TCP or UDP.

0.0.0.0 : Indicates syslog-ng will accept messages from all the interfaces
`514` : the syslog port (default)
`max_connections` : maximum number of connections handled at a time

**iii) Destination:** Defines the destination file were the output shall be written.

**iv) Log:** It co-relates the defined source and destination. It ties the source and destination together ie (log= source + destination)

### 6.3 Configuring Client

The systems that shall be sending logs to the central syslog-ng server can either run the default syslog daemon or can run syslog-ng. All systems sending logs to the central syslog server are referred to as clients in this document.

Clients using syslog-ng should use the following syslog-ng.conf file.

```
source gateway {

         unix-stream("/dev/log" max_connections(1000));
         internal();
};

destination shell {
              tcp("192.168.4.3" port(514));
};

log {
              source(gateway); destination(shell);
};
```

The destination keyword shall define the remote syslog server. It can be either in TCP or UDP.

**Command to start syslog-ng**

```
# syslog-ng -f /etc/syslog-ng.conf
```

** If it is configured as a service, the appropriate command to start the service should be run.

### 6.4 Filter syslog messages

Syslog-ng can be used to filter messages. Filters perform log routing inside syslog-ng. Boolean expression can be written using internal functions for filtering the log messages. Filters also have a uniquely identifying name for reference to filters in `log` statements.

Syntax for the filter statement:

```
filter <identifier> { expression; };
```

Available filter functions in syslog-ng

| Name | Synopsis | Description |
|---|---|---|
| facility | facility(facility[,facility]) | Match messages having one of the listed facility code. |
| level() or priority() | Level(pri[,pri1..pri2[,pri3]]) | Match messages based on priority. |
| program() | program(regexp) | Match messages by using a regular expression against the program name field of log messages |
| host() | Host(regexp) | Match messages by using a regular expression against the hostname field of log messages. |
| Match() | Tries to match a regular expression to the message itself. | |
| filter() | Call another filter rule and evaluate its value | |

An example of `/etc/syslog-ng` conf file with the capability to filter messages from the host called '`host1`' is shown below.

```
source gateway {

             unix-stream("/dev/log");
             internal();
             udp(ip(0.0.0.0) port(514));
};

source tcpgateway {

             unix-stream("/dev/log");
             internal();
             tcp(ip(0.0.0.0) port(514) max_connections(1000));
};


destination localhost {
              file("/var/log/syslog-ng.all");
};
destination tcplocalhost {
              file("/var/log/tcpsyslog-ng.all");
};

filter f_host { host("host1"); };

log {
             source(gateway); filter(f_host); destination(localhost);
};
log {
             source(tcpgateway); filter(f_host);
destination(tcplocalhost);
};
```

## 7. Configuring Database logging

The logs being generated by syslog-ng can be ported to a database for easier viewing and analysis.

A MySQL database is required to port the syslog-ng logs. The MySQL package can be downloaded from the website www.mysql.com. It is installed and configured on the syslog-ng server.

A database for syslog-ng is required to be created, with the appropriate table and fields. This is done by creating a file `syslog.sql` with the following content.

```
CREATE DATABASE syslog;
USE syslog;
CREATE TABLE logs (
host varchar(32) default NULL,
facility varchar(10) default NULL,
priority varchar(10) default NULL,
level varchar(10) default NULL,
tag varchar(10) default NULL,
date date default NULL,
time time default NULL,
program varchar(15) default NULL,
msg text,
seq int(10) unsigned NOT NULL auto_increment,
PRIMARY KEY (seq),
KEY host (host),
KEY seq (seq),
KEY program (program),
KEY time (time),
KEY date (date),
KEY priority (priority),
KEY facility (facility)
) TYPE=MyISAM;
```

The following command is run to create the database "`syslog`" and table "`logs`" in mysql

```
# mysql -u root -p < syslog.sql
```

A fifo pipe `mysql.pipe` file is created. This is the file that syslog-ng will store records before writing into the database.

```
# mkfifo /tmp/mysql.pipe
```

The `/etc/syslog-ng.conf` file is edited to pipe to a fifo template and the following lines are added:

```
destination d_mysql {

  pipe("/tmp/mysql.pipe"

  template("INSERT INTO logs (host, facility, priority, level, tag, date,

  time, program, msg) VALUES ( '$HOST', '$FACILITY', '$PRIORITY', '$LEVEL',
  '$TAG',

  '$YEAR-$MONTH-$DAY', '$HOUR:$MIN:$SEC', '$PROGRAM', '$MSG' );\n")
  template-escape(yes));

};

log { source(net); destination(d_mysql);

};
```

syslog-ng is required to be re-started to be able to store records before writing to the database

```
# syslog-ng -f /etc/syslog-ng.conf
```

The following command shall pipe the file mysql.pipe to mysql database

```
# mysql -u root --password=   syslog< /tmp/mysql.pipe
```

The following script checks to make sure the above command is running and restarts it if it has stopped. This script needs to be placed in the system startup directory so that the script restarts when the system is re-started.

```
#!/bin/bash

if [ -e /tmp/mysql.pipe ]; then
     while [ -e /tmp/mysql.pipe ]
     do
         mysql -u root --password=       syslog< /tmp/mysql.pipe
     done
else
     mkfifo /tmp/mysql.pipe
fi
```

## 8. Configuring php-syslog-ng

The messages logged into the database can be viewed using `php-syslog-ng`. It is a web based solution for viewing syslog-ng messages logged to MySQL in realtime. Customized searches can be performed based on device, time, date, priority, and message.

Apache with PHP support needs to be pre-installed and configured on the server for `php-syslog-ng`.

The latest stable version of php-syslog-ng can be downloaded from http://www.vermeer.org/display_project?project=php-syslog-ng

```
# gunzip php-syslog-ng-2.5.tar.gz
# tar xvf php-syslog-ng-2.5.tar
```

Run the above commands and place all the extracted files in the directory

```
<Apache-document-root>/php-syslog-ng-2.5/web
```

The file `includes/common_inc.php` is edited and the following line added. (Replace username and password with the relevant mysql username and password)

```
# $result = mysql_pconnect("localhost", "UserName", "Password");
```

The file `includes/db_fns.php` is edited and the following line added (Replace username and password with the relevant mysql username and password).

```
# $result = mysql_pconnect("localhost", "root", "Password");
```

Apache is started and the following URL can be accessed to view the logs as shown in Fig 2 and fig. 3.

```
http://localhost/index.php
```

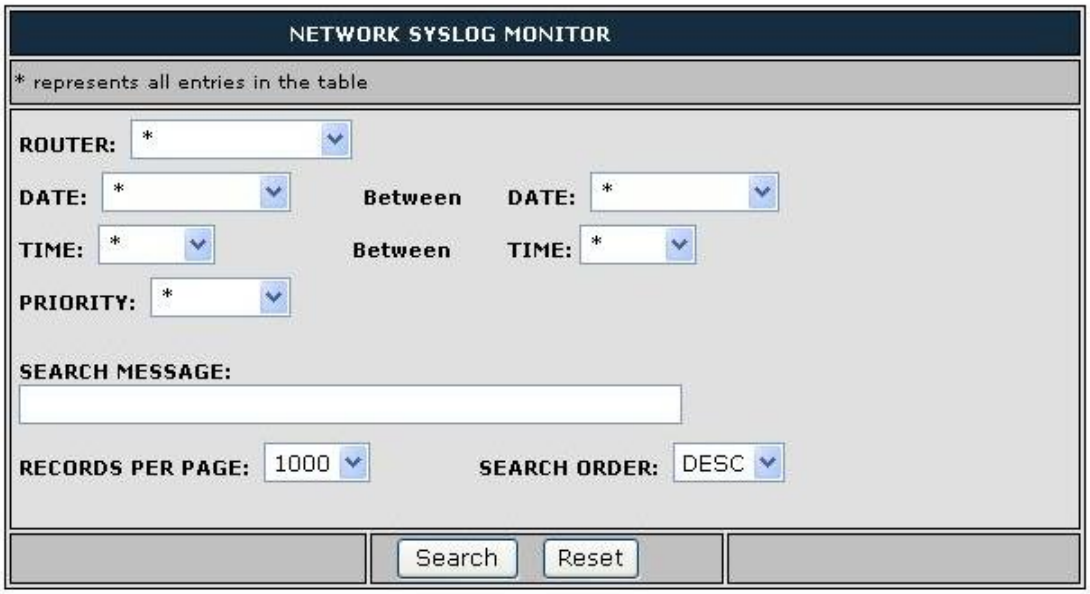
NETWORK SYSLOG MONITOR
* represents all entries in the table
ROUTER: *
DATE: * Between DATE: *
TIME: * Between TIME: *
PRIORITY: *
SEARCH MESSAGE:
RECORDS PER PAGE: 1000
SEARCH ORDER: DESC
Search
Reset

Fig. 2

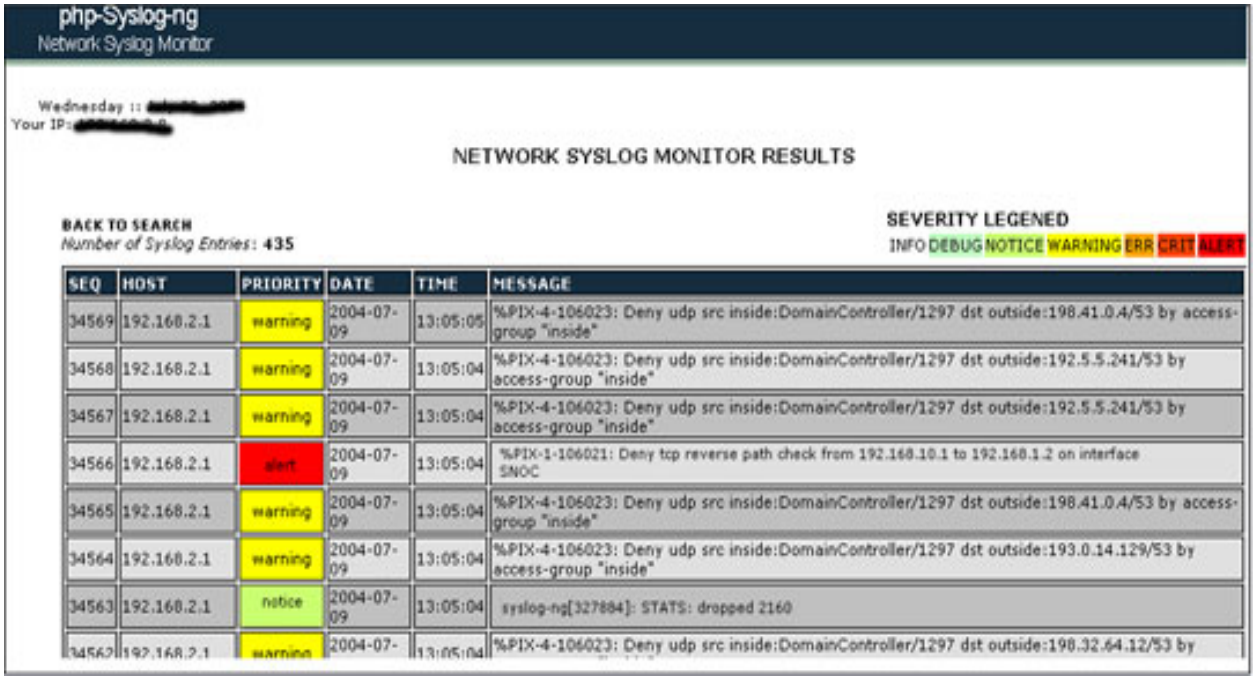
php-Syslog-ng
Network Syslog Monitor
Wednesday ::
Your IP:
NETWORK SYSLOG MONITOR RESULTS
BACK TO SEARCH
Number of Syslog Entries: 435
SEVERITY LEGENED
INFO DEBUG NOTICE WARNING ERR CRIT ALERT
SEQ HOST PRIORITY DATE TIME MESSAGE
34569 192.168.2.1 warning 2004-07-09 13:05:05 %PIX-4-106023: Deny udp src inside:DomainController/1297 dst outside:198.41.0.4/53 by access-group "inside"
34568 192.168.2.1 warning 2004-07-09 13:05:04 %PIX-4-106023: Deny udp src inside:DomainController/1297 dst outside:192.5.5.241/53 by access-group "inside"
34567 192.168.2.1 warning 2004-07-09 13:05:04 %PIX-4-106023: Deny udp src inside:DomainController/1297 dst outside:192.5.5.241/53 by access-group "inside"
34566 192.168.2.1 alert 2004-07-09 13:05:04 %PIX-1-106021: Deny tcp reverse path check from 192.168.10.1 to 192.168.1.2 on interface SNOC
34565 192.168.2.1 warning 2004-07-09 13:05:04 %PIX-4-106023: Deny udp src inside:DomainController/1297 dst outside:198.41.0.4/53 by access-group "inside"
34564 192.168.2.1 warning 2004-07-09 13:05:04 %PIX-4-106023: Deny udp src inside:DomainController/1297 dst outside:193.0.14.129/53 by access-group "inside"
34563 192.168.2.1 notice 2004-07-09 13:05:04 syslog-ng[327884]: STATS: dropped 2160
2004-07- %PIX-4-106023: Deny udp src inside:DomainController/1297 dst outside:198.32.64.12/53 by

Fig. 3

# 9. Logging Apache logs to syslog-ng

## 9.1 Logging error_log

Apache can be configured to be send error logs to the central syslog server.

This is done by editing the file `httpd.conf` and placing `syslog` in the `ErrorLog` option as shown below. This log level option can be configured as required.

```
LogLevel    notice
ErrorLog    syslog
```

Apache uses the `local7` syslog facility id, by default. Thus, a corresponding entry is made in `/etc/syslog.conf`

```
local7.*    @syslog-nghost
```

Further the IP address of the remote syslog server defined as `'@syslog-nghost'` has to be configured in the `/etc/hosts` file.

## 9.2 Logging access_log

Apache can also be configured to log `access_log` entries into the central syslog server. However, this may increase the number of messages sent to the syslog server manifold and could even flood the server.

The httpd.conf file is edited and the following line added.

```
# CustomLog "| /usr/bin/logger –p local1.info" common
```

The following entry is required in `/etc/syslog.conf`

```
# local1.*  @syslog-nghost
```

The IP address of the remote syslog server defined as `'@syslog-nghost'` has to be configured in the `/etc/hosts` file.

## 10. Logging Windows logs to syslog-ng

Windows NT does not natively utilize or interface with syslog. However, with third party software, Windows NT can act as a syslog client and redirect messages from its event log to a centralized syslog server. Various third party windows syslog daemon are available to send logs to a central syslog server.

Some of the available third party software which format all Windows System, Security, and Application event logs into a single line and send them to a syslog server are:

NT syslog
http://ntsyslog.sourceforge.net/

Snare Agent for Windows
http://sourceforge.net/projects/snare/

Kiwi syslog Daemon for Windows
http://www.kiwisyslog.com

Refer to [Ref: 6] CERT/CC Advanced Information Assurance Handbook for detailed instructions on installing NTsyslog Daemon and Kiwi syslog Daemon for Windows.

## 11. References

**Ref:1.** php-syslog-ng
http://vermeer.org

**Ref:2.** CERT-In: Securing Redhat Linux 9.0 as a web server
http://www.cert-in.org.in/guidelines/CISG-2004-02.pdf

**Ref:3.** IETF syslog Working Group HomePage
http://www.employees.org/~lonvick/index.shtml

**Ref:4.** syslog-ng Reference Manual
http://www.balabit.com/products/syslog_ng/reference/book1.html

**Ref:5.** RFC 3164
http://www.ietf.org/rfc/rfc3164.txt

**Ref:6.** CERT/CC Advanced Information Assurance Handbook
http://www.cert.org/archive/pdf/aia-handbook.pdf

**Ref:7.** syslog-ng conf file
http://www.campin.net/syslog-ng/expanded-syslog-ng.conf

feedback : info [at] cert-in.org.in

Indian Computer Emergency Response Team CERT-In
Ministry of Communications and Information Technology
Electronics Niketan, 6, C.G.O. Complex
Lodhi Road, New Delhi-110 003 Phone : +91-11-24368572