syslog-ng

Dieses Dokument beschreibt die Konfiguration und den Betrieb von Syslog-NG unter Fedora Core (5).

syslog-ng ist ein mächtiger syslogd-Ersatz.

Meine syslog-ng Konfiguration:

```
options {
    stats(3600);
    dir_perm(0755);
    perm(0644);
    chain_hostnames(no);
    keep_hostname(yes);
    time_reopen (10);
    log_fifo_size (1000);
    long_hostnames (off);
    use_dns (no);
    use_fqdn (no);
    create_dirs (no);
    keep_hostname (yes);
};

source s_sys {
    file ("/proc/kmsg" log_prefix("kernel: "));
    unix-stream("/dev/log");
    udp(ip(0.0.0.0) port(514));
    internal();
};

# /var/log/messages
filter f_messages { not facility(cron, mail, authpriv); };
filter f_nofirewall { not (facility(kern) and (match("RULE") or match("BLOCKLIST") or match("Act
destination d_messages { file("/var/log/messages"); };
log { source(s_sys); filter(f_messages); filter(f_nofirewall); destination(d_messages); };

# /var/log/firewall
filter f_firewall { match("RULE") or match("BLOCKLIST") or match("Activating firewall script");
destination d_firewall { file("/var/log/firewall"); };
log { source(s_sys); filter(f_firewall); destination(d_firewall); };

# /var/log/secure
filter f_authpriv { facility(authpriv); };
destination d_secure { file("/var/log/secure"); };
log { source(s_sys); filter(f_authpriv); destination(d_secure); };

# /var/log/maillog
filter f_maillog { facility(mail); };
destination d_maillog { file("/var/log/maillog" sync(10)); };
log { source(s_sys); filter(f_maillog); destination(d_maillog); };

# /var/log/cron
filter f_cron { facility(cron); };
destination d_cron { file("/var/log/cron"); };
log { source(s_sys); filter(f_cron); destination(d_cron); };

# consolenmeldung
filter f_emerg { level(emerg); };
destination d_console { usertty("*"); };
log { source(s_sys); filter(f_emerg); destination(d_console); };

# /var/log/spooler
filter f_spooler { facility(uucp,news); };
destination d_spooler { file("/var/log/spooler"); };
log { source(s_sys); filter(f_spooler); destination(d_spooler); };

# /var/log/boot.log
filter f_boot { facility(local7); };
destination d_boot { file("/var/log/boot.log"); };
log { source(s_sys); filter(f_boot); destination(d_boot); };

# alles
```

```
destination d_all { file("/var/log/all.log"); };
log { source(s_sys); destination(d_all); };
```

Revision #1
Created 30 April 2021 12:11:20 by magenbrot
Updated 30 April 2021 12:11:43 by magenbrot