```
#
# LOLLERSKATES config file
#

# Who should we send reports to?
email           = "treed@edirectpublishing.com"

# What SMTP server should we send them through?
smtp_server     = "mail.edirectpublishing.com"

# Where are we installed?
installdir      = "/usr/local/lollerskates"

# Where do we keep state files?
statefiles      = "/var/lib/lollerskates"

# What logfiles should we be checking?
logfiles        = ["/var/log/cron",
                   "/var/log/spooler",
                   "/var/log/messages",
                   "/var/log/maillog",
                   "/var/log/dmesg",
                   "/var/log/secure",
                   "/var/log/boot.log",
                   "/var/log/kernel",
                   "/var/log/audit/audit.log",
                   "/var/log/mysqld.log",
                   "/var/log/ldirectord.log",
                   "/var/log/ha-log",
                   "/opt/munin/log/munin/munin-node.log",
                   "/opt/munin/log/munin/munin-update.log",
                   "/opt/munin/log/munin/munin-graph.log",
                   "/opt/munin/log/munin/munin-html.log",
                   "/opt/munin/log/munin/munin-limits.log",
                   "/opt/munin/log/munin/munin-cgi-graph.log",
                   "/var/log/ethereal/packets.log",
                   "/var/log/mysqld.log",
                   "/var/log/cluster/corosync.log",
                   "/var/lib/mysql/db1.edirectpublishing.com.err",
                   "/var/lib/mysql/db2.edirectpublishing.com.err",
                   "/var/lib/mysql/db3.edirectpublishing.com.err",
                   "/var/lib/mysql/db4.edirectpublishing.com.err",
                   "/var/lib/mysql/newsdb1.edirectpublishing.com.err",
                   "/var/lib/mysql/newsdb2.edirectpublishing.com.err",
                   ]

# Matchdays is the number of days in which if a regex in the ignore file does no
t match anything to warn us
# Regexes which never match are probably typos or just unnecessary.
matchdays       = 90

# If this is set to True we will remove regexes which have not matched in matchd
ays from the ignore.conf file
# and append them to the ignore.conf.removed file.
remove          = True

#
# Define some macros to substitute into our ignore file so it is
# easier to read and type You can add your own if you find it
# handy. It is a python list.
#
# First element of tuple is the token which the regex will be
# substituted for.
#
# Second element is the string that will be used to insert into events
# to add macros to it to make it easier to read and make it suitable
# for adding to our ignore.conf file.
#
# Third element is the actual regex which will be inserted instead of
```



```
# the token. This regex will be matched against the log file.
#
# Note that the order in which these are applied can affect the
# outcome. For example we substitute hostnames before we do IP's
# because many hostnames for dynamically allocated hosts contain the
# IP address in them.

macros = [
    # This is designed to match the date and hostname at the beginning
    # of nearly any syslog generated line
    ("_DATEHOST_","^\w{3} [ :0-9]{11} [-a-zA-Z0-9]+"),
    # Beginning of ethereal packet log
    #  15  15.797419 192.168.3.167 -> 10.0.2.66    SIP Status: 200 OK
    ("_ETHEREAL_","\s*\d+\s+\d+\.\d+\s+"),
    # This is a postfix queue ID which shows up a lot in mail logs
    ("_PFQID_","([A-Z0-9]{6,12}(\.[A-Z0-9]{5})?|NOQUEUE)[:\) ]"),
    # This matches a FQDN style hostname in mail logs etc.
    # 'renttoownhomesllc\.com/IN'
    ("_HOST_","[\'<\[\(= ]([-0-9A-Za-z_]+\.)+[a-zA-Z]{2,4}[\[\]\> \/]?"),
    # Matches any standalone IP
    ("_IP_","(25[0-5]|2[0-4][0-9]|[01]?[0-9][0-9]?)\.(25[0-5]|2[0-4][0-9]|[01]?[0-9][0-9]?)\.(25[0-5]|2[0-4][
0-9]|[01]?[0-9][0-9]?)(\.(25[0-5]|2[0-4][0-9]|[01]?[0-9][0-9]?))"),
    # An ethernet MAC address
    ("_MAC_","(?:[[:xdigit:]]{1,2}[-:]){5}[[:xdigit:]]{1,2}"),
    # A process ID in brackets like what appears in many syslog
    # messages
    ("_PID_","\[\d+\]"),
    # An email address. Spammers throw all kinds of crap in email
    # addresses so you may have to add some unusual characters.
    ("_EMAIL_","[-=A-Za-z0-9\._#\?]+@[-A-Za-z0-9\._]+\.[a-zA-Z]{2,4}"),
    # A date of the format Feb 18 02:31:02
    ("_MON-DD-HH-MM-SS_","(Jan|Feb|Mar|Apr|May|Jun|Jul|Aug|Sep|Oct|Nov|Dec) \d\d \d\d:\d\d:\d\d"),
    # A date of the format YYYY-MM-DD with a space on the front and ending a lin
e
    ("_YYYY-MM-DD_"," \d\d\d\d-\d\d-\d\d$"),
    # A class C address with a space before and paren after like what
    # sqlgrey might write:
    # sqlgrey: grey: early reconnect: 72.52.189(72.52.189.120), treed@ultraviole
t.org -> treed@ultraviolet.
    # sqlgrey: spam: 72\.52\.189: _EMAIL_ -> _EMAIL_ at 1203163029
    ("_CLASSC_","(25[0-5]|2[0-4][0-9]|[01]?[0-9][0-9]?)\.(25[0-5]|2[0-4][0-9]|[01]?[0-9][0-9]?)\.(25[0-5]|
2[0-4][0-9]|[01]?[0-9][0-9]?)[:\(]"),
    # A bunch of digits preceded by a few chars
    ("_DIGITS_","[ =\#\(]\d+")
    ]
```