2^{η} εργασία στις σύγχρονες εφαρμογές ασφάλειας δικτύων

Όνομα: Γεώργιος

Επώνυμο: Βέργος

Αριθμός Μητρώου: 1072604

Ημερομηνία: 5/11/2022

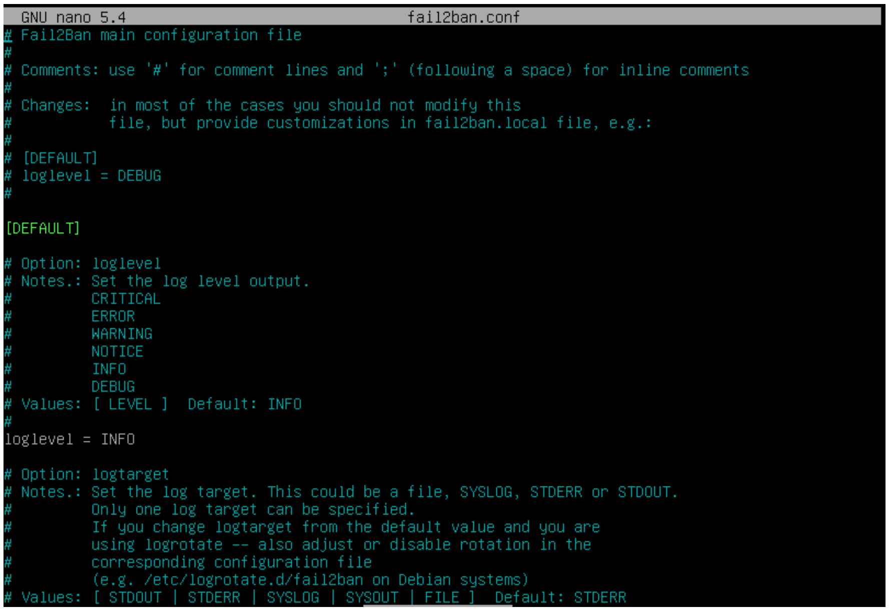
Εξάμηνο: 7^{ο}

Τμήμα: ΤΜΗΥΠ(CEID)

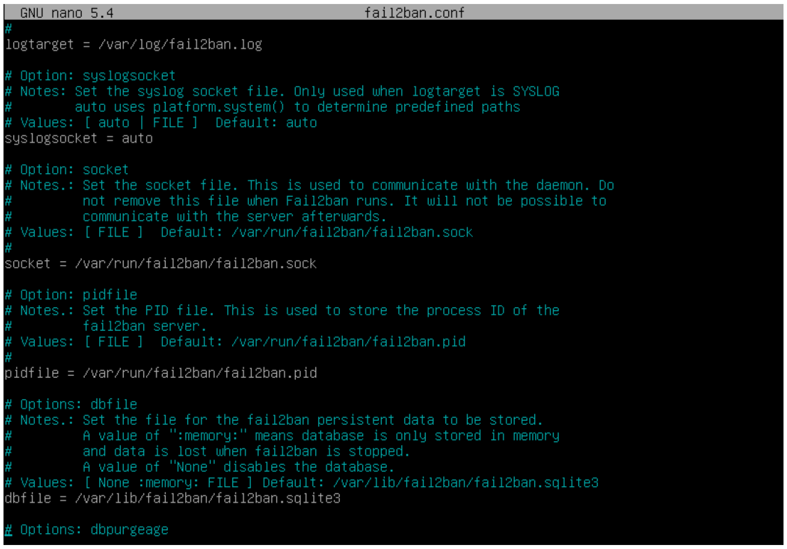
1) Προστασία ανεπιθύμητων επιθέσεων με χρήση του πακέτου fail2ban

Στις παρακάτω εικόνες φαίνονται τα αρχεία διαμόρφωσης fail2ban.conf και jail.conf:

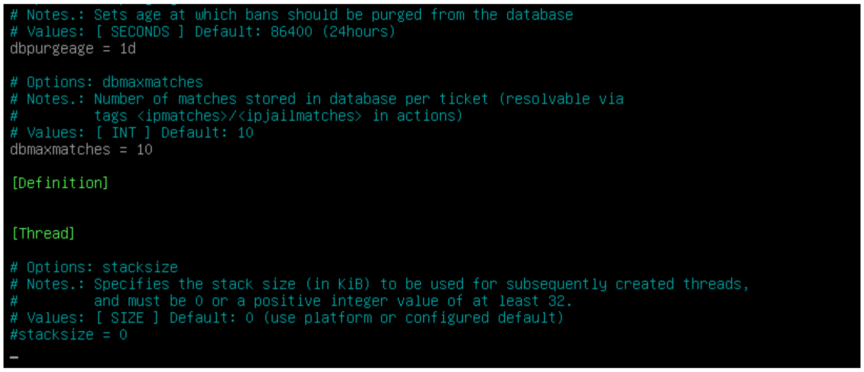
a) fail2ban.conf:



```
  GNU nano 5.4                            fail2ban.conf
# Fail2Ban main configuration file
#
# Comments: use '#' for comment lines and ';' (following a space) for inline comments
#
# Changes:  in most of the cases you should not modify this
#           file, but provide customizations in fail2ban.local file, e.g.:
#
# [DEFAULT]
# loglevel = DEBUG
#

[DEFAULT]

# Option: loglevel
# Notes.: Set the log level output.
#         CRITICAL
#         ERROR
#         WARNING
#         NOTICE
#         INFO
#         DEBUG
# Values: [ LEVEL ]  Default: INFO
#
loglevel = INFO

# Option: logtarget
# Notes.: Set the log target. This could be a file, SYSLOG, STDERR or STDOUT.
#         Only one log target can be specified.
#         If you change logtarget from the default value and you are
#         using logrotate -- also adjust or disable rotation in the
#         corresponding configuration file
#         (e.g. /etc/logrotate.d/fail2ban on Debian systems)
# Values: [ STDOUT | STDERR | SYSLOG | SYSOUT | FILE ]  Default: STDERR
```

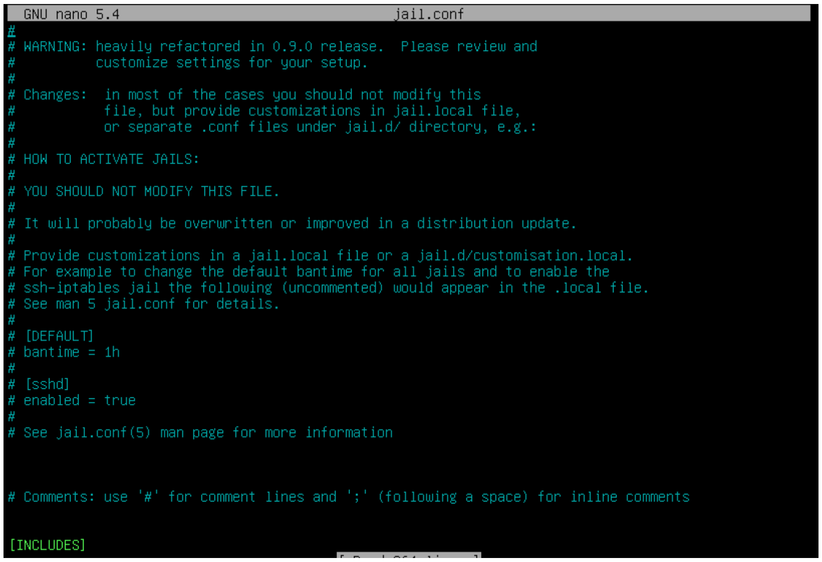


```
  GNU nano 5.4                                          fail2ban.conf
#
logtarget = /var/log/fail2ban.log

# Option: syslogsocket
# Notes: Set the syslog socket file. Only used when logtarget is SYSLOG
#        auto uses platform.system() to determine predefined paths
# Values: [ auto | FILE ]  Default: auto
syslogsocket = auto

# Option: socket
# Notes.: Set the socket file. This is used to communicate with the daemon. Do
#         not remove this file when Fail2ban runs. It will not be possible to
#         communicate with the server afterwards.
# Values: [ FILE ]  Default: /var/run/fail2ban/fail2ban.sock
#
socket = /var/run/fail2ban/fail2ban.sock

# Option: pidfile
# Notes.: Set the PID file. This is used to store the process ID of the
#         fail2ban server.
# Values: [ FILE ]  Default: /var/run/fail2ban/fail2ban.pid
#
pidfile = /var/run/fail2ban/fail2ban.pid

# Options: dbfile
# Notes.: Set the file for the fail2ban persistent data to be stored.
#         A value of ":memory:" means database is only stored in memory
#         and data is lost when fail2ban is stopped.
#         A value of "None" disables the database.
# Values: [ None :memory: FILE ] Default: /var/lib/fail2ban/fail2ban.sqlite3
dbfile = /var/lib/fail2ban/fail2ban.sqlite3

# Options: dbpurgeage
```

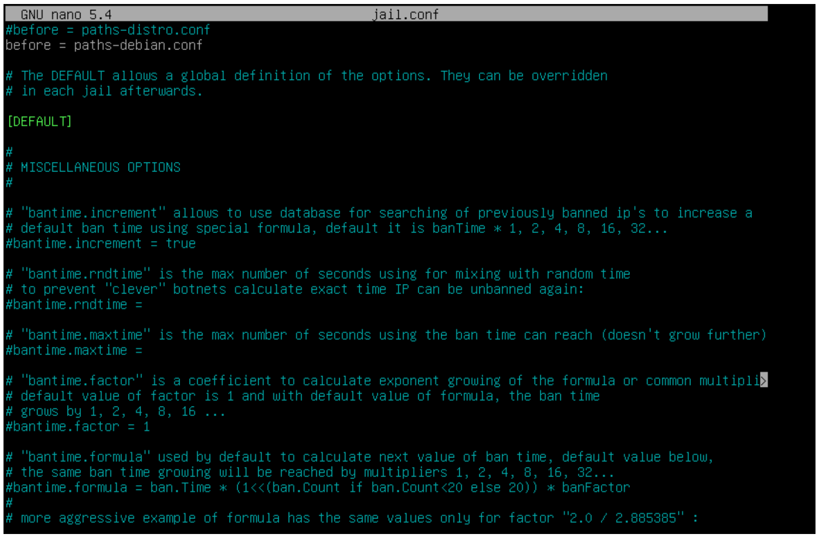


```
# Notes.: Sets age at which bans should be purged from the database
# Values: [ SECONDS ] Default: 86400 (24hours)
dbpurgeage = 1d

# Options: dbmaxmatches
# Notes.: Number of matches stored in database per ticket (resolvable via
#         tags <ipmatches>/<ipjailmatches> in actions)
# Values: [ INT ] Default: 10
dbmaxmatches = 10

[Definition]


[Thread]

# Options: stacksize
# Notes.: Specifies the stack size (in KiB) to be used for subsequently created threads,
#         and must be 0 or a positive integer value of at least 32.
# Values: [ SIZE ] Default: 0 (use platform or configured default)
#stacksize = 0
```

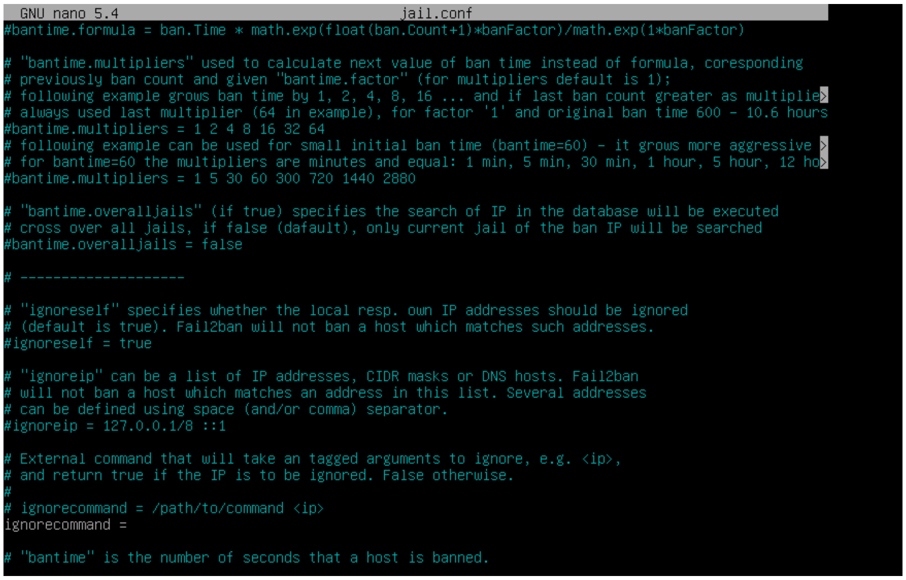
b) jail.conf



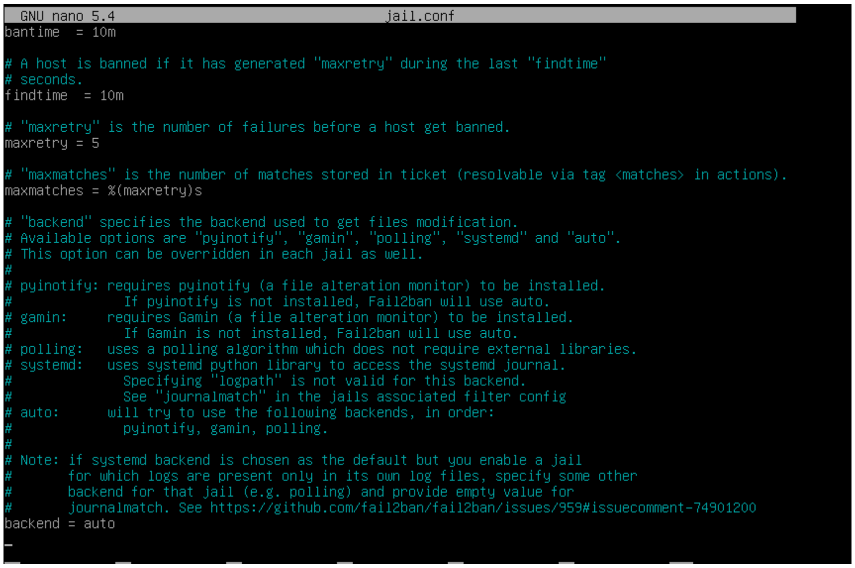
```
  GNU nano 5.4                                            jail.conf
#
# WARNING: heavily refactored in 0.9.0 release.  Please review and
#          customize settings for your setup.
#
# Changes:  in most of the cases you should not modify this
#           file, but provide customizations in jail.local file,
#           or separate .conf files under jail.d/ directory, e.g.:
#
# HOW TO ACTIVATE JAILS:
#
# YOU SHOULD NOT MODIFY THIS FILE.
#
# It will probably be overwritten or improved in a distribution update.
#
# Provide customizations in a jail.local file or a jail.d/customisation.local.
# For example to change the default bantime for all jails and to enable the
# ssh-iptables jail the following (uncommented) would appear in the .local file.
# See man 5 jail.conf for details.
#
# [DEFAULT]
# bantime = 1h
#
# [sshd]
# enabled = true
#
# See jail.conf(5) man page for more information



# Comments: use '#' for comment lines and ';' (following a space) for inline comments


[INCLUDES]
```



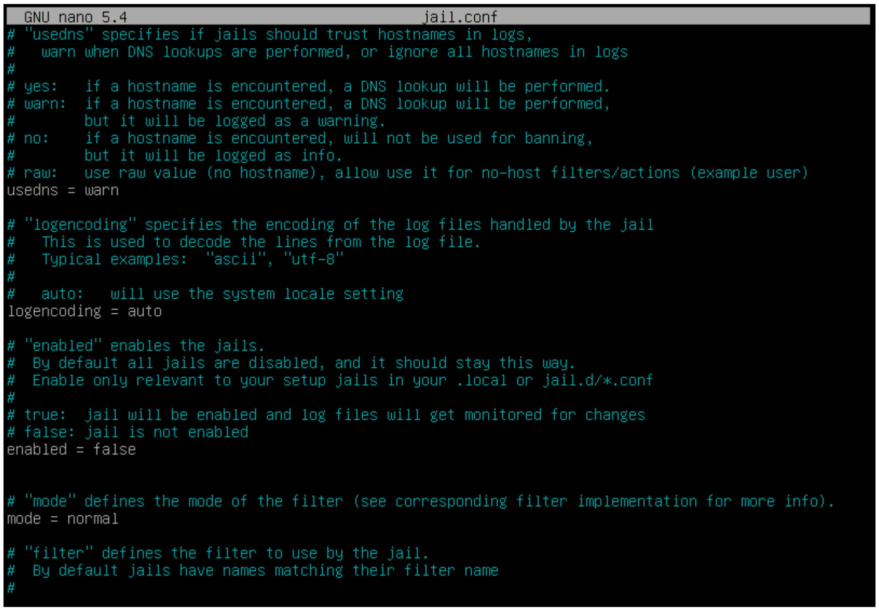
```
  GNU nano 5.4                                 jail.conf
#before = paths-distro.conf
before = paths-debian.conf

# The DEFAULT allows a global definition of the options. They can be overridden
# in each jail afterwards.

[DEFAULT]

#
# MISCELLANEOUS OPTIONS
#

# "bantime.increment" allows to use database for searching of previously banned ip's to increase a
# default ban time using special formula, default it is banTime * 1, 2, 4, 8, 16, 32...
#bantime.increment = true

# "bantime.rndtime" is the max number of seconds using for mixing with random time
# to prevent "clever" botnets calculate exact time IP can be unbanned again:
#bantime.rndtime =

# "bantime.maxtime" is the max number of seconds using the ban time can reach (doesn't grow further)
#bantime.maxtime =

# "bantime.factor" is a coefficient to calculate exponent growing of the formula or common multipli>
# default value of factor is 1 and with default value of formula, the ban time
# grows by 1, 2, 4, 8, 16 ...
#bantime.factor = 1

# "bantime.formula" used by default to calculate next value of ban time, default value below,
# the same ban time growing will be reached by multipliers 1, 2, 4, 8, 16, 32...
#bantime.formula = ban.Time * (1<<(ban.Count if ban.Count<20 else 20)) * banFactor
#
# more aggressive example of formula has the same values only for factor "2.0 / 2.885385" :
```



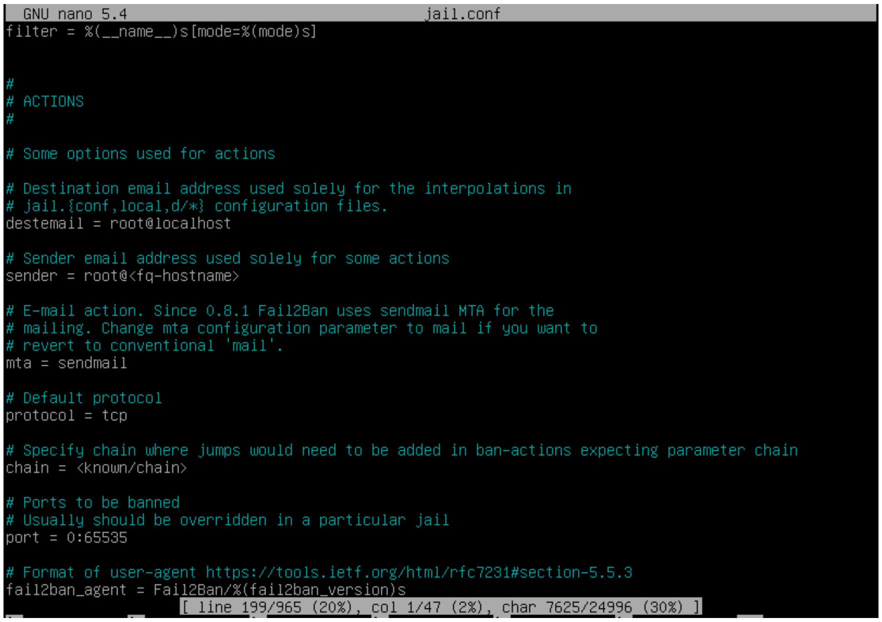
```
  GNU nano 5.4                                 jail.conf
#bantime.formula = ban.Time * math.exp(float(ban.Count+1)*banFactor)/math.exp(1*banFactor)

# "bantime.multipliers" used to calculate next value of ban time instead of formula, coresponding
# previously ban count and given "bantime.factor" (for multipliers default is 1);
# following example grows ban time by 1, 2, 4, 8, 16 ... and if last ban count greater as multiplie>
# always used last multiplier (64 in example), for factor '1' and original ban time 600 - 10.6 hours
#bantime.multipliers = 1 2 4 8 16 32 64
# following example can be used for small initial ban time (bantime=60) - it grows more aggressive >
# for bantime=60 the multipliers are minutes and equal: 1 min, 5 min, 30 min, 1 hour, 5 hour, 12 ho>
#bantime.multipliers = 1 5 30 60 300 720 1440 2880

# "bantime.overalljails" (if true) specifies the search of IP in the database will be executed
# cross over all jails, if false (dafault), only current jail of the ban IP will be searched
#bantime.overalljails = false

# --------------------

# "ignoreself" specifies whether the local resp. own IP addresses should be ignored
# (default is true). Fail2ban will not ban a host which matches such addresses.
#ignoreself = true

# "ignoreip" can be a list of IP addresses, CIDR masks or DNS hosts. Fail2ban
# will not ban a host which matches an address in this list. Several addresses
# can be defined using space (and/or comma) separator.
#ignoreip = 127.0.0.1/8 ::1

# External command that will take an tagged arguments to ignore, e.g. <ip>,
# and return true if the IP is to be ignored. False otherwise.
#
# ignorecommand = /path/to/command <ip>
ignorecommand =

# "bantime" is the number of seconds that a host is banned.
```



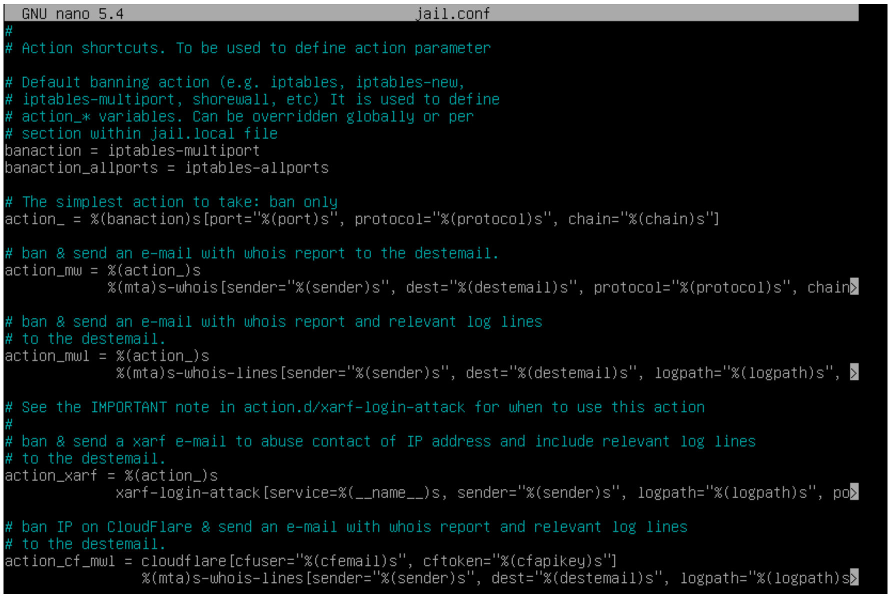
```
  GNU nano 5.4                                 jail.conf
bantime  = 10m

# A host is banned if it has generated "maxretry" during the last "findtime"
# seconds.
findtime  = 10m

# "maxretry" is the number of failures before a host get banned.
maxretry = 5

# "maxmatches" is the number of matches stored in ticket (resolvable via tag <matches> in actions).
maxmatches = %(maxretry)s

# "backend" specifies the backend used to get files modification.
# Available options are "pyinotify", "gamin", "polling", "systemd" and "auto".
# This option can be overridden in each jail as well.
#
# pyinotify: requires pyinotify (a file alteration monitor) to be installed.
#              If pyinotify is not installed, Fail2ban will use auto.
# gamin:     requires Gamin (a file alteration monitor) to be installed.
#              If Gamin is not installed, Fail2ban will use auto.
# polling:   uses a polling algorithm which does not require external libraries.
# systemd:   uses systemd python library to access the systemd journal.
#              Specifying "logpath" is not valid for this backend.
#              See "journalmatch" in the jails associated filter config
# auto:      will try to use the following backends, in order:
#              pyinotify, gamin, polling.
#
# Note: if systemd backend is chosen as the default but you enable a jail
#       for which logs are present only in its own log files, specify some other
#       backend for that jail (e.g. polling) and provide empty value for
#       journalmatch. See https://github.com/fail2ban/fail2ban/issues/959#issuecomment-74901200
backend = auto
```



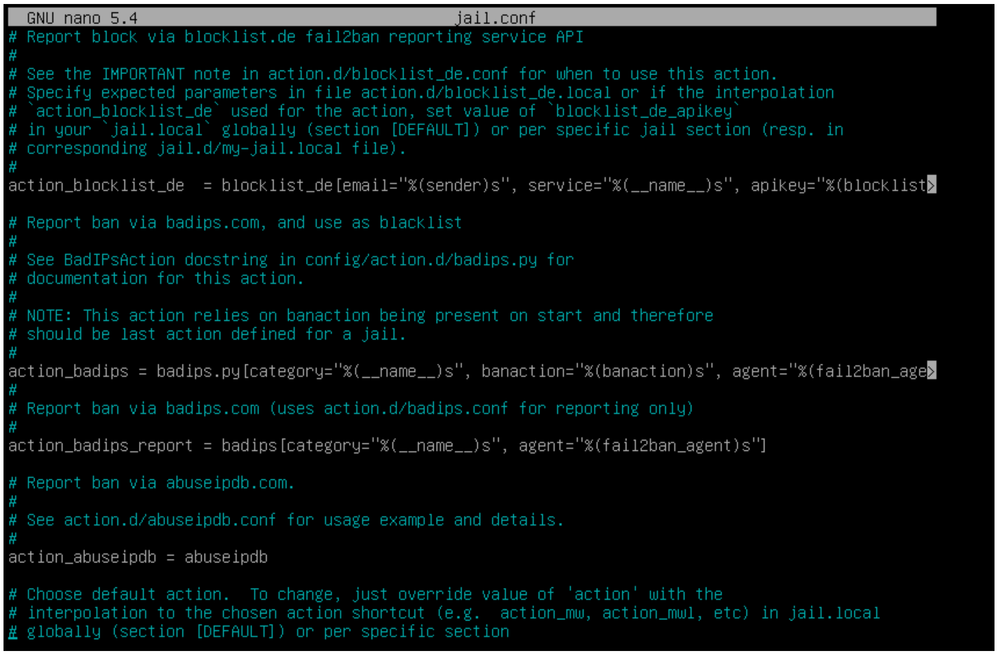
```
  GNU nano 5.4                                     jail.conf
# "usedns" specifies if jails should trust hostnames in logs,
#   warn when DNS lookups are performed, or ignore all hostnames in logs
#
# yes:   if a hostname is encountered, a DNS lookup will be performed.
# warn:  if a hostname is encountered, a DNS lookup will be performed,
#        but it will be logged as a warning.
# no:    if a hostname is encountered, will not be used for banning,
#        but it will be logged as info.
# raw:   use raw value (no hostname), allow use it for no-host filters/actions (example user)
usedns = warn

# "logencoding" specifies the encoding of the log files handled by the jail
#   This is used to decode the lines from the log file.
#   Typical examples:  "ascii", "utf-8"
#
#   auto:   will use the system locale setting
logencoding = auto

# "enabled" enables the jails.
#  By default all jails are disabled, and it should stay this way.
#  Enable only relevant to your setup jails in your .local or jail.d/*.conf
#
# true:  jail will be enabled and log files will get monitored for changes
# false: jail is not enabled
enabled = false


# "mode" defines the mode of the filter (see corresponding filter implementation for more info).
mode = normal

# "filter" defines the filter to use by the jail.
#  By default jails have names matching their filter name
#
```



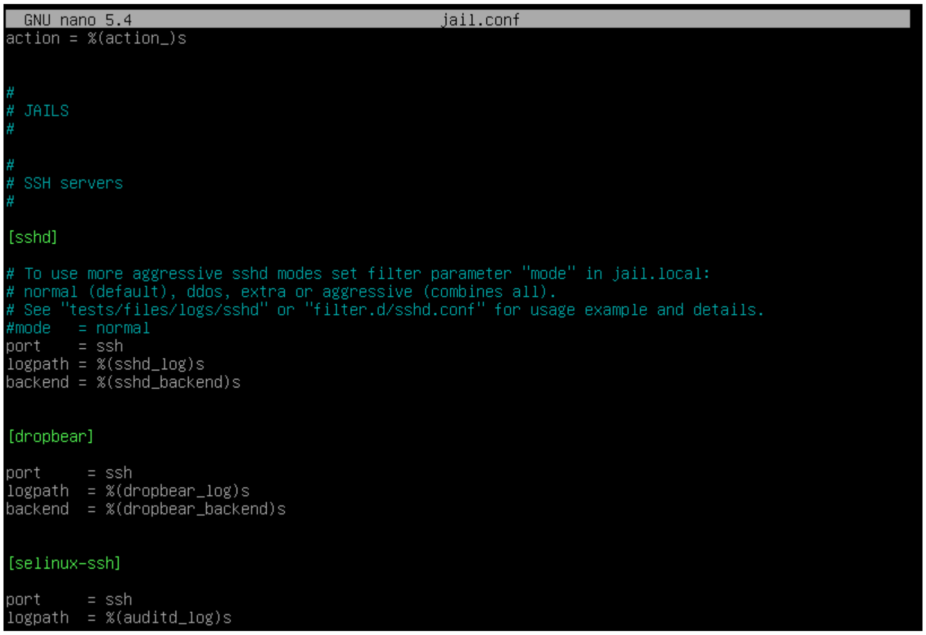
```
  GNU nano 5.4                                     jail.conf
filter = %(__name__)s[mode=%(mode)s]


#
# ACTIONS
#

# Some options used for actions

# Destination email address used solely for the interpolations in
# jail.{conf,local,d/*} configuration files.
destemail = root@localhost

# Sender email address used solely for some actions
sender = root@<fq-hostname>

# E-mail action. Since 0.8.1 Fail2Ban uses sendmail MTA for the
# mailing. Change mta configuration parameter to mail if you want to
# revert to conventional 'mail'.
mta = sendmail

# Default protocol
protocol = tcp

# Specify chain where jumps would need to be added in ban-actions expecting parameter chain
chain = <known/chain>

# Ports to be banned
# Usually should be overridden in a particular jail
port = 0:65535

# Format of user-agent https://tools.ietf.org/html/rfc7231#section-5.5.3
fail2ban_agent = Fail2Ban/%(fail2ban_version)s
                    [ line 199/965 (20%), col 1/47 (2%), char 7625/24996 (30%) ]
```



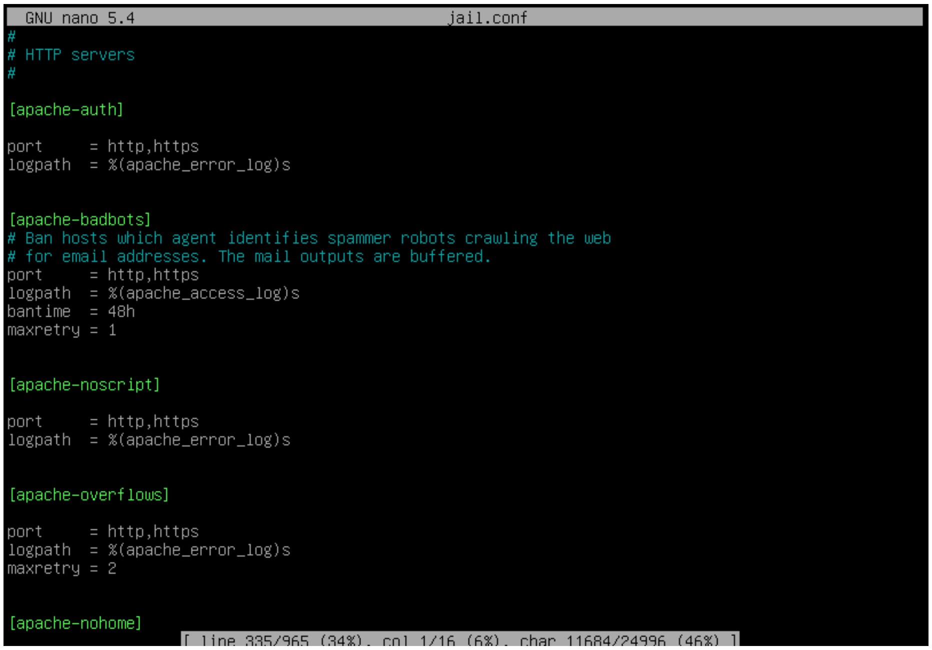
```
  GNU nano 5.4                                             jail.conf
#
# Action shortcuts. To be used to define action parameter

# Default banning action (e.g. iptables, iptables-new,
# iptables-multiport, shorewall, etc) It is used to define
# action_* variables. Can be overridden globally or per
# section within jail.local file
banaction = iptables-multiport
banaction_allports = iptables-allports

# The simplest action to take: ban only
action_ = %(banaction)s[port="%(port)s", protocol="%(protocol)s", chain="%(chain)s"]

# ban & send an e-mail with whois report to the destemail.
action_mw = %(action_)s
            %(mta)s-whois[sender="%(sender)s", dest="%(destemail)s", protocol="%(protocol)s", chain>

# ban & send an e-mail with whois report and relevant log lines
# to the destemail.
action_mwl = %(action_)s
             %(mta)s-whois-lines[sender="%(sender)s", dest="%(destemail)s", logpath="%(logpath)s", >

# See the IMPORTANT note in action.d/xarf-login-attack for when to use this action
#
# ban & send a xarf e-mail to abuse contact of IP address and include relevant log lines
# to the destemail.
action_xarf = %(action_)s
             xarf-login-attack[service=%(__name__)s, sender="%(sender)s", logpath="%(logpath)s", po>

# ban IP on CloudFlare & send an e-mail with whois report and relevant log lines
# to the destemail.
action_cf_mwl = cloudflare[cfuser="%(cfemail)s", cftoken="%(cfapikey)s"]
                %(mta)s-whois-lines[sender="%(sender)s", dest="%(destemail)s", logpath="%(logpath)s>
```



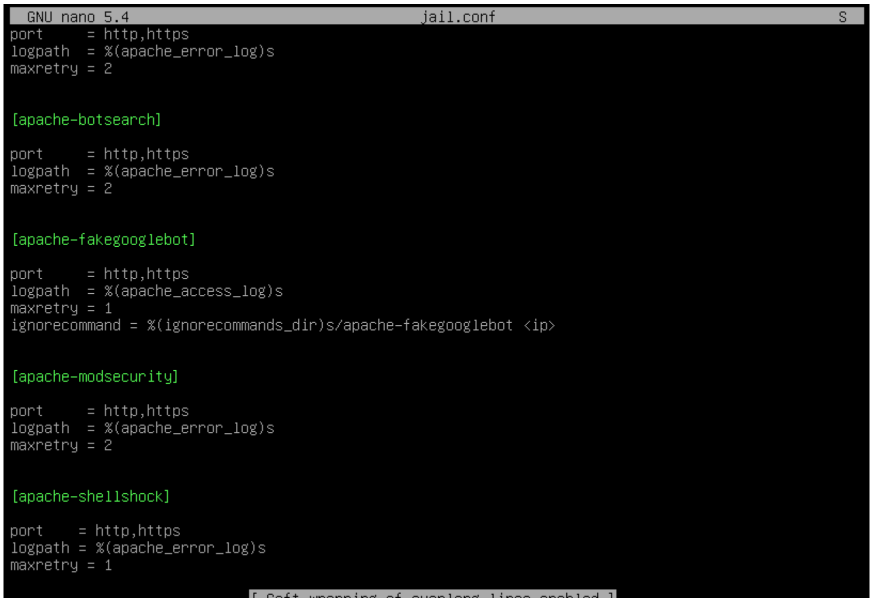
```
  GNU nano 5.4                                         jail.conf
# Report block via blocklist.de fail2ban reporting service API
#
# See the IMPORTANT note in action.d/blocklist_de.conf for when to use this action.
# Specify expected parameters in file action.d/blocklist_de.local or if the interpolation
# `action_blocklist_de` used for the action, set value of `blocklist_de_apikey`
# in your `jail.local` globally (section [DEFAULT]) or per specific jail section (resp. in
# corresponding jail.d/my-jail.local file).
#
action_blocklist_de  = blocklist_de[email="%(sender)s", service="%(__name__)s", apikey="%(blocklist>

# Report ban via badips.com, and use as blacklist
#
# See BadIPsAction docstring in config/action.d/badips.py for
# documentation for this action.
#
# NOTE: This action relies on banaction being present on start and therefore
# should be last action defined for a jail.
#
action_badips = badips.py[category="%(__name__)s", banaction="%(banaction)s", agent="%(fail2ban_age>
#
# Report ban via badips.com (uses action.d/badips.conf for reporting only)
#
action_badips_report = badips[category="%(__name__)s", agent="%(fail2ban_agent)s"]

# Report ban via abuseipdb.com.
#
# See action.d/abuseipdb.conf for usage example and details.
#
action_abuseipdb = abuseipdb

# Choose default action.  To change, just override value of 'action' with the
# interpolation to the chosen action shortcut (e.g.  action_mw, action_mwl, etc) in jail.local
# globally (section [DEFAULT]) or per specific section
```



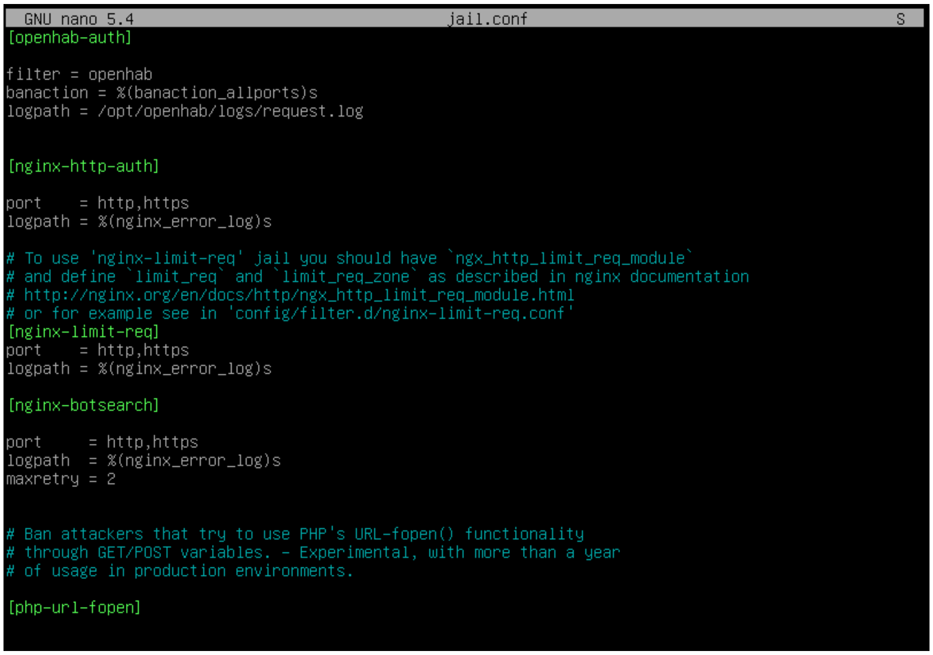
```
  GNU nano 5.4                                      jail.conf
action = %(action_)s


#
# JAILS
#

#
# SSH servers
#

[sshd]

# To use more aggressive sshd modes set filter parameter "mode" in jail.local:
# normal (default), ddos, extra or aggressive (combines all).
# See "tests/files/logs/sshd" or "filter.d/sshd.conf" for usage example and details.
#mode   = normal
port    = ssh
logpath = %(sshd_log)s
backend = %(sshd_backend)s


[dropbear]

port     = ssh
logpath  = %(dropbear_log)s
backend  = %(dropbear_backend)s


[selinux-ssh]

port     = ssh
logpath  = %(auditd_log)s
```



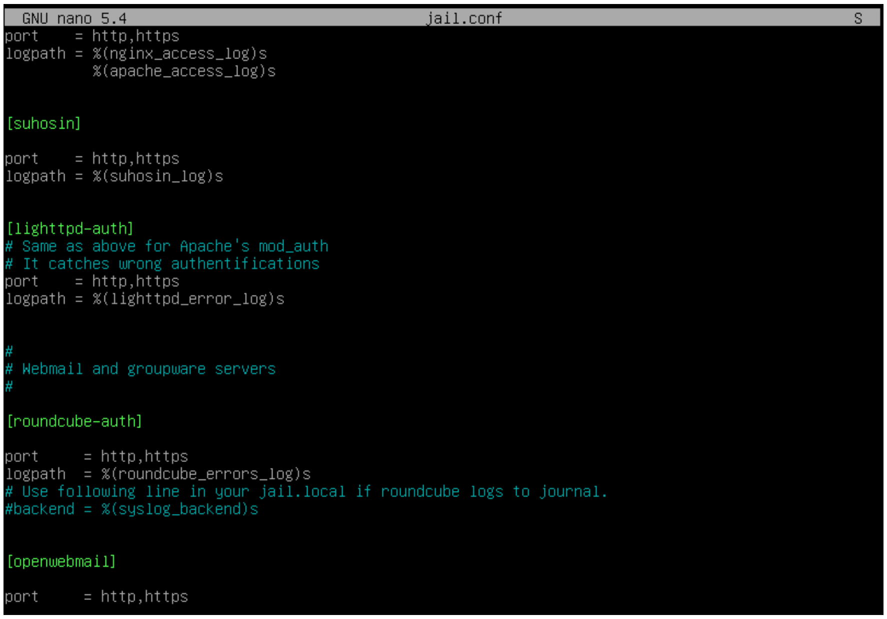
```
  GNU nano 5.4                                      jail.conf
#
# HTTP servers
#

[apache-auth]

port     = http,https
logpath  = %(apache_error_log)s


[apache-badbots]
# Ban hosts which agent identifies spammer robots crawling the web
# for email addresses. The mail outputs are buffered.
port     = http,https
logpath  = %(apache_access_log)s
bantime  = 48h
maxretry = 1


[apache-noscript]

port     = http,https
logpath  = %(apache_error_log)s


[apache-overflows]

port     = http,https
logpath  = %(apache_error_log)s
maxretry = 2


[apache-nohome]
                         [ line 335/965 (34%), col 1/16 (6%), char 11684/24996 (46%) ]
```



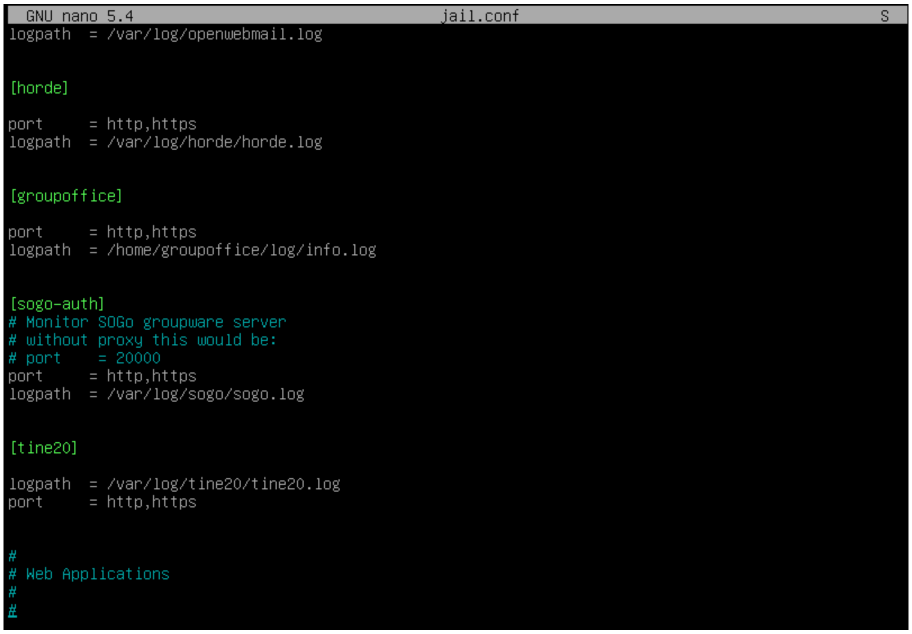
```
  GNU nano 5.4                          jail.conf                          S
port     = http,https
logpath  = %(apache_error_log)s
maxretry = 2


[apache-botsearch]

port     = http,https
logpath  = %(apache_error_log)s
maxretry = 2


[apache-fakegooglebot]

port     = http,https
logpath  = %(apache_access_log)s
maxretry = 1
ignorecommand = %(ignorecommands_dir)s/apache-fakegooglebot <ip>


[apache-modsecurity]

port     = http,https
logpath  = %(apache_error_log)s
maxretry = 2


[apache-shellshock]

port    = http,https
logpath = %(apache_error_log)s
maxretry = 1

                    [ Soft wrapping of overlong lines enabled ]
```



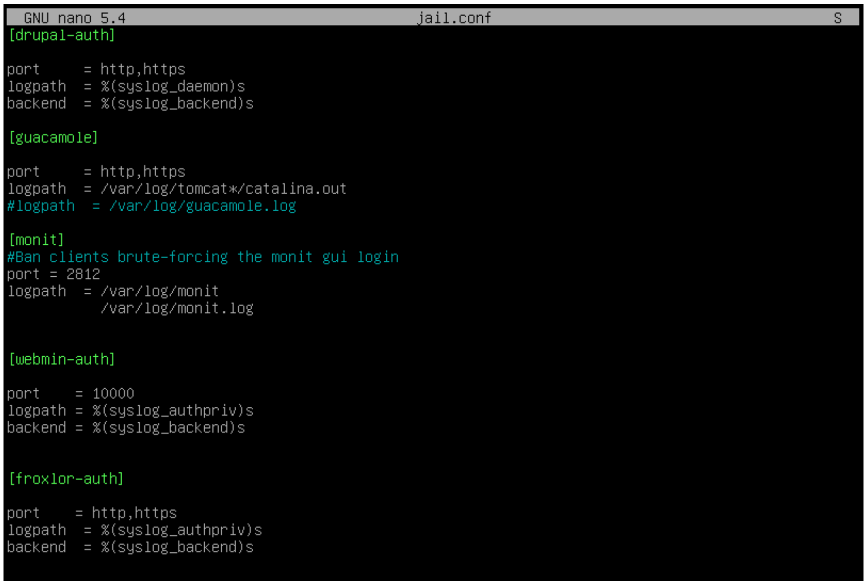
```
  GNU nano 5.4                          jail.conf                          S
[openhab-auth]

filter = openhab
banaction = %(banaction_allports)s
logpath = /opt/openhab/logs/request.log


[nginx-http-auth]

port    = http,https
logpath = %(nginx_error_log)s

# To use 'nginx-limit-req' jail you should have `ngx_http_limit_req_module`
# and define `limit_req` and `limit_req_zone` as described in nginx documentation
# http://nginx.org/en/docs/http/ngx_http_limit_req_module.html
# or for example see in 'config/filter.d/nginx-limit-req.conf'
[nginx-limit-req]
port    = http,https
logpath = %(nginx_error_log)s

[nginx-botsearch]

port     = http,https
logpath  = %(nginx_error_log)s
maxretry = 2


# Ban attackers that try to use PHP's URL-fopen() functionality
# through GET/POST variables. - Experimental, with more than a year
# of usage in production environments.

[php-url-fopen]
```



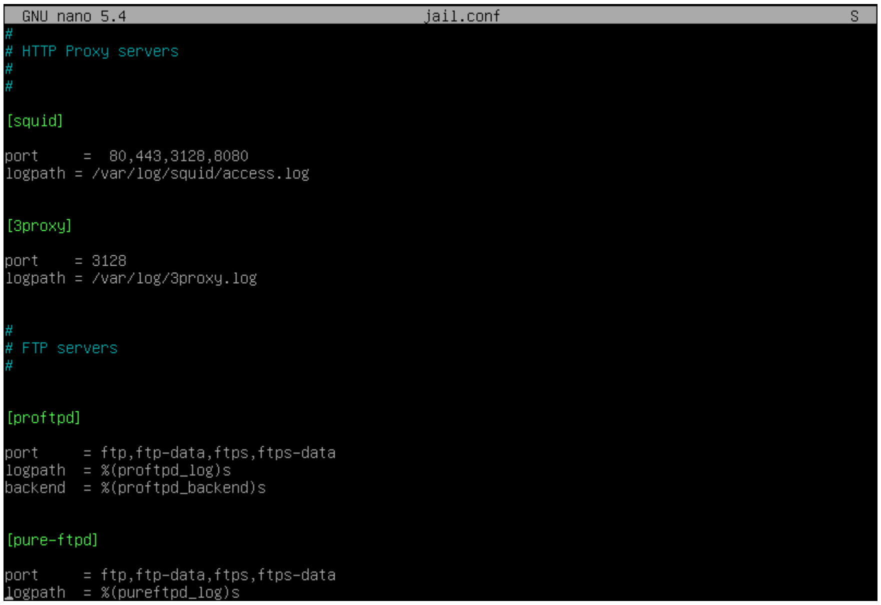
```
  GNU nano 5.4                                jail.conf                                S
port     = http,https
logpath = %(nginx_access_log)s
          %(apache_access_log)s


[suhosin]

port     = http,https
logpath = %(suhosin_log)s


[lighttpd-auth]
# Same as above for Apache's mod_auth
# It catches wrong authentifications
port     = http,https
logpath = %(lighttpd_error_log)s


#
# Webmail and groupware servers
#

[roundcube-auth]

port      = http,https
logpath   = %(roundcube_errors_log)s
# Use following line in your jail.local if roundcube logs to journal.
#backend = %(syslog_backend)s


[openwebmail]

port      = http,https
```



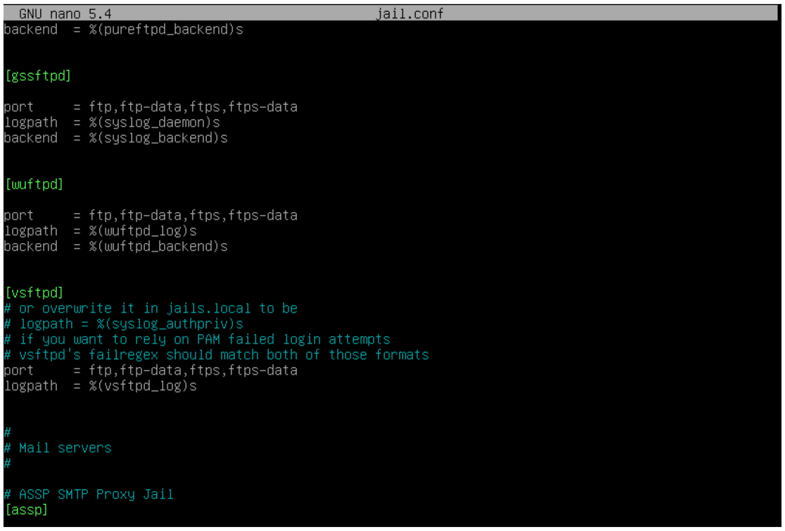
```
  GNU nano 5.4                                jail.conf                                S
logpath  = /var/log/openwebmail.log


[horde]

port     = http,https
logpath  = /var/log/horde/horde.log


[groupoffice]

port     = http,https
logpath  = /home/groupoffice/log/info.log


[sogo-auth]
# Monitor SOGo groupware server
# without proxy this would be:
# port     = 20000
port     = http,https
logpath  = /var/log/sogo/sogo.log


[tine20]

logpath  = /var/log/tine20/tine20.log
port     = http,https


#
# Web Applications
#
#
```



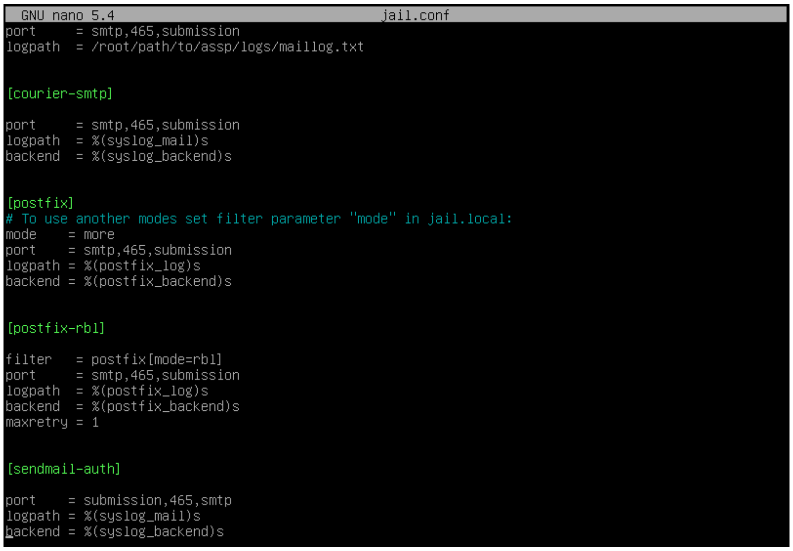
```
  GNU nano 5.4                                jail.conf                                       S
[drupal-auth]

port     = http,https
logpath  = %(syslog_daemon)s
backend  = %(syslog_backend)s

[guacamole]

port     = http,https
logpath  = /var/log/tomcat*/catalina.out
#logpath  = /var/log/guacamole.log

[monit]
#Ban clients brute-forcing the monit gui login
port = 2812
logpath  = /var/log/monit
           /var/log/monit.log


[webmin-auth]

port    = 10000
logpath = %(syslog_authpriv)s
backend = %(syslog_backend)s


[froxlor-auth]

port    = http,https
logpath  = %(syslog_authpriv)s
backend  = %(syslog_backend)s
```



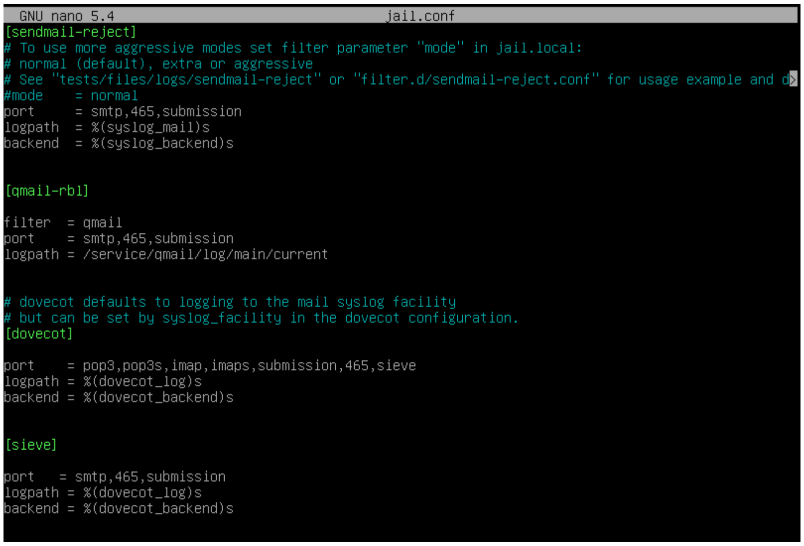
```
  GNU nano 5.4                                 jail.conf                                        S
#
# HTTP Proxy servers
#
#

[squid]

port     =  80,443,3128,8080
logpath = /var/log/squid/access.log


[3proxy]

port    = 3128
logpath = /var/log/3proxy.log


#
# FTP servers
#


[proftpd]

port     = ftp,ftp-data,ftps,ftps-data
logpath  = %(proftpd_log)s
backend  = %(proftpd_backend)s


[pure-ftpd]

port     = ftp,ftp-data,ftps,ftps-data
logpath  = %(pureftpd_log)s
```



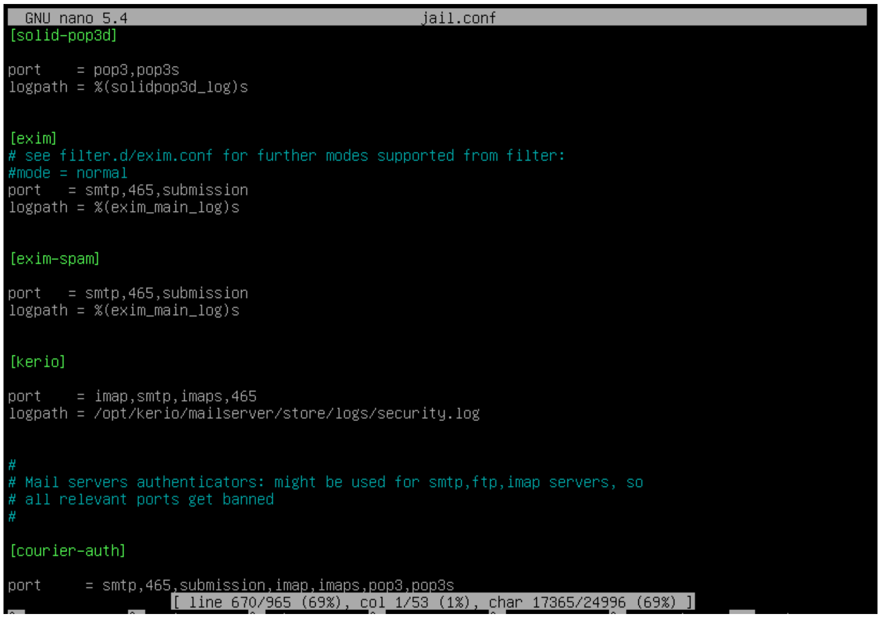
```
  GNU nano 5.4                              jail.conf
backend  = %(pureftpd_backend)s


[gssftpd]

port     = ftp,ftp-data,ftps,ftps-data
logpath  = %(syslog_daemon)s
backend  = %(syslog_backend)s


[wuftpd]

port     = ftp,ftp-data,ftps,ftps-data
logpath  = %(wuftpd_log)s
backend  = %(wuftpd_backend)s


[vsftpd]
# or overwrite it in jails.local to be
# logpath = %(syslog_authpriv)s
# if you want to rely on PAM failed login attempts
# vsftpd's failregex should match both of those formats
port     = ftp,ftp-data,ftps,ftps-data
logpath  = %(vsftpd_log)s


#
# Mail servers
#

# ASSP SMTP Proxy Jail
[assp]
```



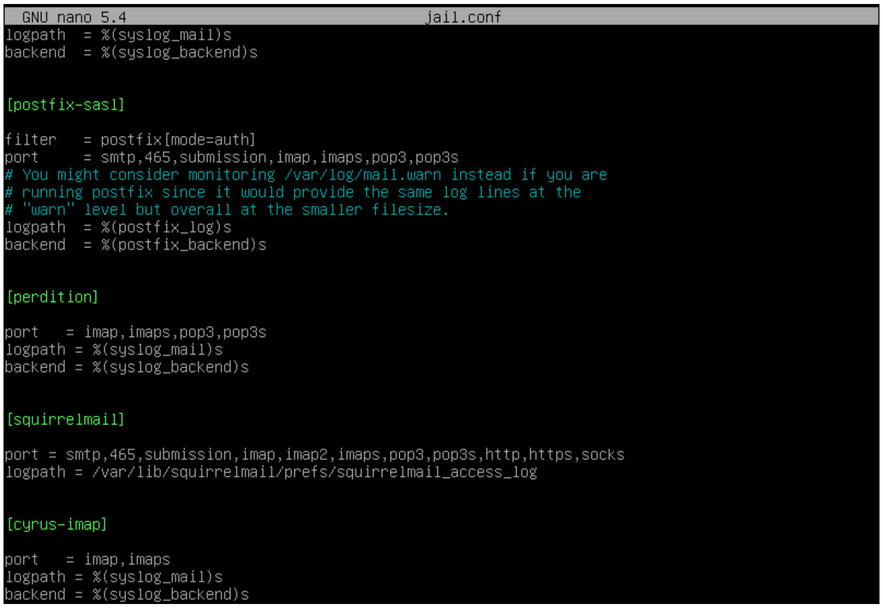
```
  GNU nano 5.4                              jail.conf
port     = smtp,465,submission
logpath  = /root/path/to/assp/logs/maillog.txt


[courier-smtp]

port     = smtp,465,submission
logpath  = %(syslog_mail)s
backend  = %(syslog_backend)s


[postfix]
# To use another modes set filter parameter "mode" in jail.local:
mode    = more
port    = smtp,465,submission
logpath = %(postfix_log)s
backend = %(postfix_backend)s


[postfix-rbl]

filter   = postfix[mode=rbl]
port     = smtp,465,submission
logpath  = %(postfix_log)s
backend  = %(postfix_backend)s
maxretry = 1


[sendmail-auth]

port    = submission,465,smtp
logpath = %(syslog_mail)s
backend = %(syslog_backend)s
```



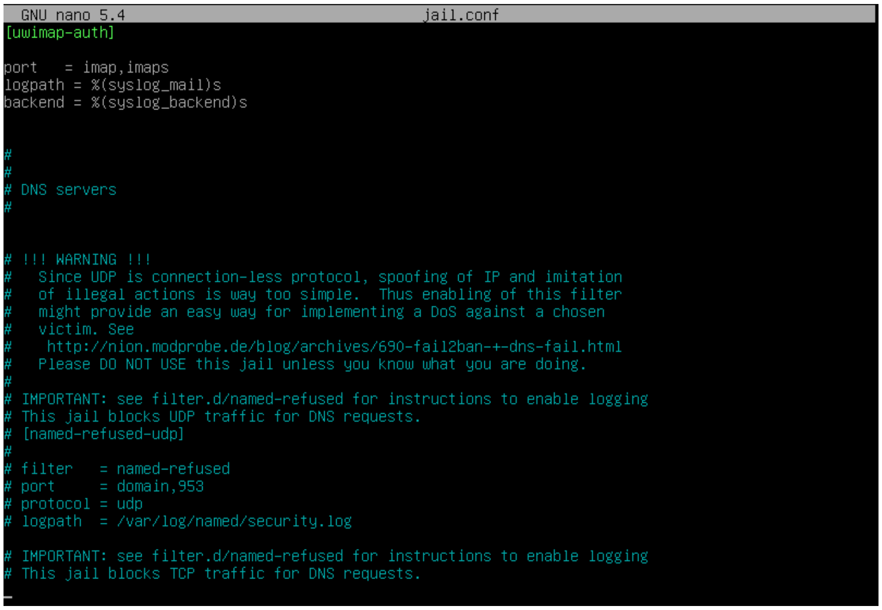
```
  GNU nano 5.4                                          jail.conf
[sendmail-reject]
# To use more aggressive modes set filter parameter "mode" in jail.local:
# normal (default), extra or aggressive
# See "tests/files/logs/sendmail-reject" or "filter.d/sendmail-reject.conf" for usage example and d>
#mode     = normal
port      = smtp,465,submission
logpath   = %(syslog_mail)s
backend   = %(syslog_backend)s


[qmail-rbl]

filter   = qmail
port     = smtp,465,submission
logpath = /service/qmail/log/main/current


# dovecot defaults to logging to the mail syslog facility
# but can be set by syslog_facility in the dovecot configuration.
[dovecot]

port    = pop3,pop3s,imap,imaps,submission,465,sieve
logpath = %(dovecot_log)s
backend = %(dovecot_backend)s


[sieve]

port   = smtp,465,submission
logpath = %(dovecot_log)s
backend = %(dovecot_backend)s
```



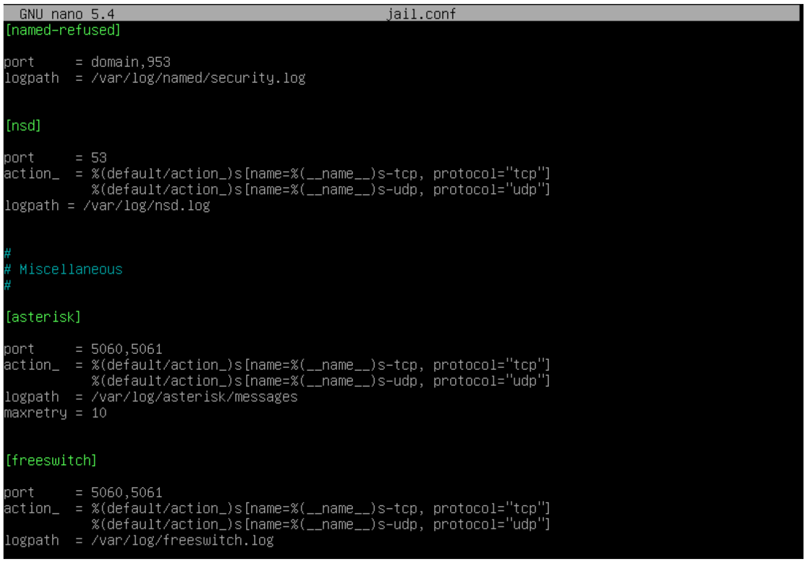
```
  GNU nano 5.4                                          jail.conf
[solid-pop3d]

port     = pop3,pop3s
logpath = %(solidpop3d_log)s


[exim]
# see filter.d/exim.conf for further modes supported from filter:
#mode = normal
port   = smtp,465,submission
logpath = %(exim_main_log)s


[exim-spam]

port   = smtp,465,submission
logpath = %(exim_main_log)s


[kerio]

port     = imap,smtp,imaps,465
logpath = /opt/kerio/mailserver/store/logs/security.log


#
# Mail servers authenticators: might be used for smtp,ftp,imap servers, so
# all relevant ports get banned
#

[courier-auth]

port      = smtp,465,submission,imap,imaps,pop3,pop3s
                     [ line 670/965 (69%), col 1/53 (1%), char 17365/24996 (69%) ]
```



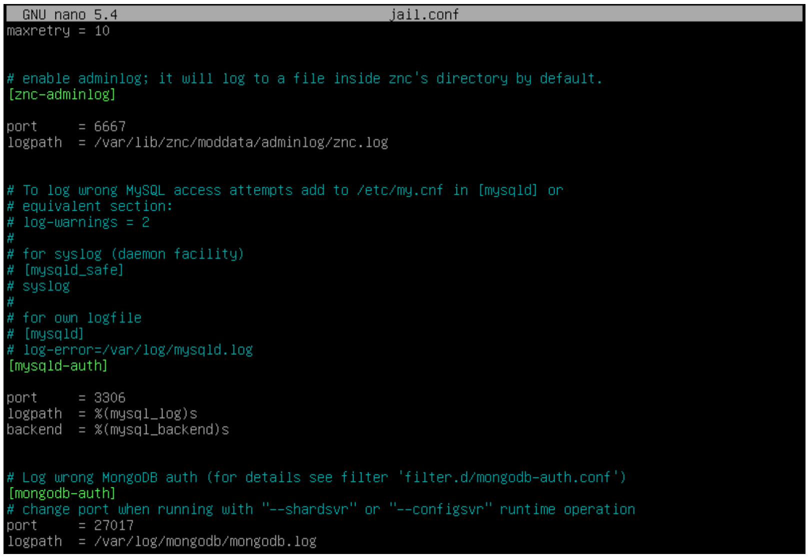
```
logpath  = %(syslog_mail)s
backend  = %(syslog_backend)s


[postfix-sasl]

filter   = postfix[mode=auth]
port     = smtp,465,submission,imap,imaps,pop3,pop3s
# You might consider monitoring /var/log/mail.warn instead if you are
# running postfix since it would provide the same log lines at the
# "warn" level but overall at the smaller filesize.
logpath  = %(postfix_log)s
backend  = %(postfix_backend)s


[perdition]

port   = imap,imaps,pop3,pop3s
logpath = %(syslog_mail)s
backend = %(syslog_backend)s


[squirrelmail]

port = smtp,465,submission,imap,imap2,imaps,pop3,pop3s,http,https,socks
logpath = /var/lib/squirrelmail/prefs/squirrelmail_access_log


[cyrus-imap]

port   = imap,imaps
logpath = %(syslog_mail)s
backend = %(syslog_backend)s
```



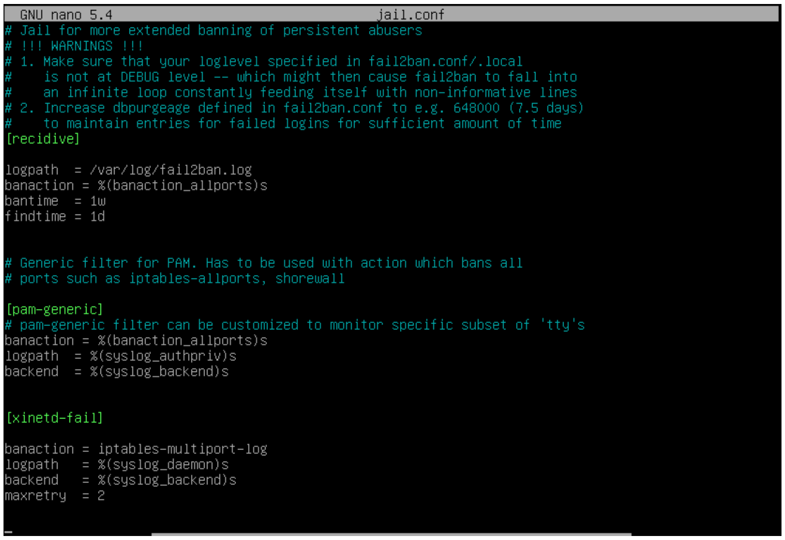
```
[uwimap-auth]

port   = imap,imaps
logpath = %(syslog_mail)s
backend = %(syslog_backend)s


#
#
# DNS servers
#


# !!! WARNING !!!
#   Since UDP is connection-less protocol, spoofing of IP and imitation
#   of illegal actions is way too simple.  Thus enabling of this filter
#   might provide an easy way for implementing a DoS against a chosen
#   victim. See
#    http://nion.modprobe.de/blog/archives/690-fail2ban-+-dns-fail.html
#   Please DO NOT USE this jail unless you know what you are doing.
#
# IMPORTANT: see filter.d/named-refused for instructions to enable logging
# This jail blocks UDP traffic for DNS requests.
# [named-refused-udp]
#
# filter   = named-refused
# port     = domain,953
# protocol = udp
# logpath  = /var/log/named/security.log

# IMPORTANT: see filter.d/named-refused for instructions to enable logging
# This jail blocks TCP traffic for DNS requests.
```



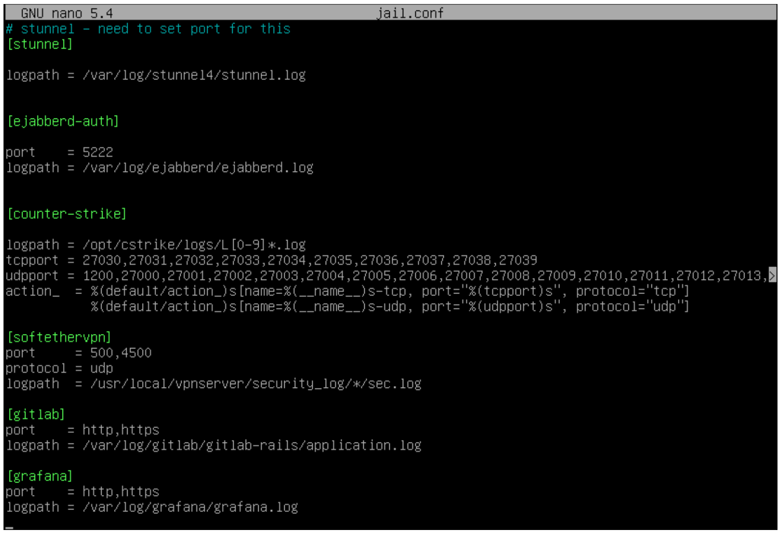
```
[named-refused]

port     = domain,953
logpath  = /var/log/named/security.log


[nsd]

port     = 53
action_  = %(default/action_)s[name=%(__name__)s-tcp, protocol="tcp"]
           %(default/action_)s[name=%(__name__)s-udp, protocol="udp"]
logpath = /var/log/nsd.log


#
# Miscellaneous
#

[asterisk]

port     = 5060,5061
action_  = %(default/action_)s[name=%(__name__)s-tcp, protocol="tcp"]
           %(default/action_)s[name=%(__name__)s-udp, protocol="udp"]
logpath  = /var/log/asterisk/messages
maxretry = 10


[freeswitch]

port     = 5060,5061
action_  = %(default/action_)s[name=%(__name__)s-tcp, protocol="tcp"]
           %(default/action_)s[name=%(__name__)s-udp, protocol="udp"]
logpath  = /var/log/freeswitch.log
```



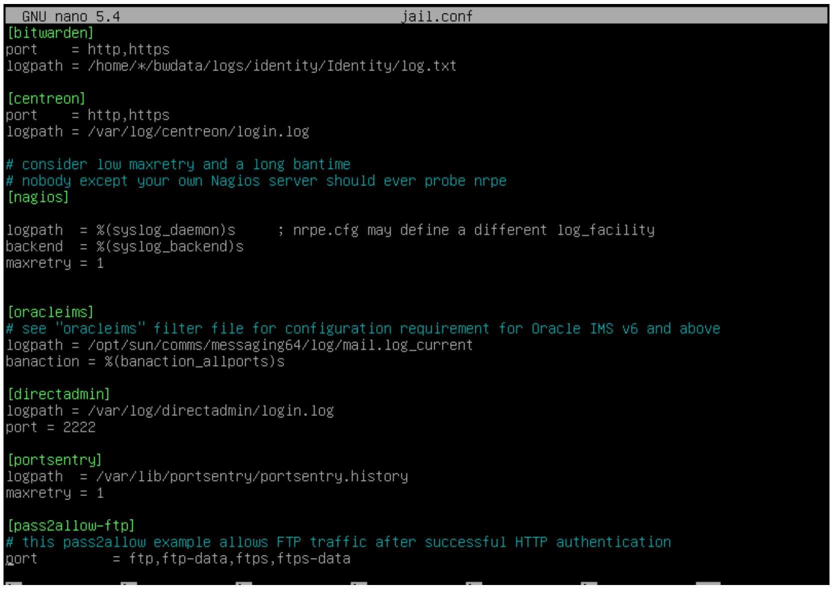
```
maxretry = 10


# enable adminlog; it will log to a file inside znc's directory by default.
[znc-adminlog]

port     = 6667
logpath  = /var/lib/znc/moddata/adminlog/znc.log


# To log wrong MySQL access attempts add to /etc/my.cnf in [mysqld] or
# equivalent section:
# log-warnings = 2
#
# for syslog (daemon facility)
# [mysqld_safe]
# syslog
#
# for own logfile
# [mysqld]
# log-error=/var/log/mysqld.log
[mysqld-auth]

port     = 3306
logpath  = %(mysql_log)s
backend  = %(mysql_backend)s


# Log wrong MongoDB auth (for details see filter 'filter.d/mongodb-auth.conf')
[mongodb-auth]
# change port when running with "--shardsvr" or "--configsvr" runtime operation
port     = 27017
logpath  = /var/log/mongodb/mongodb.log
```



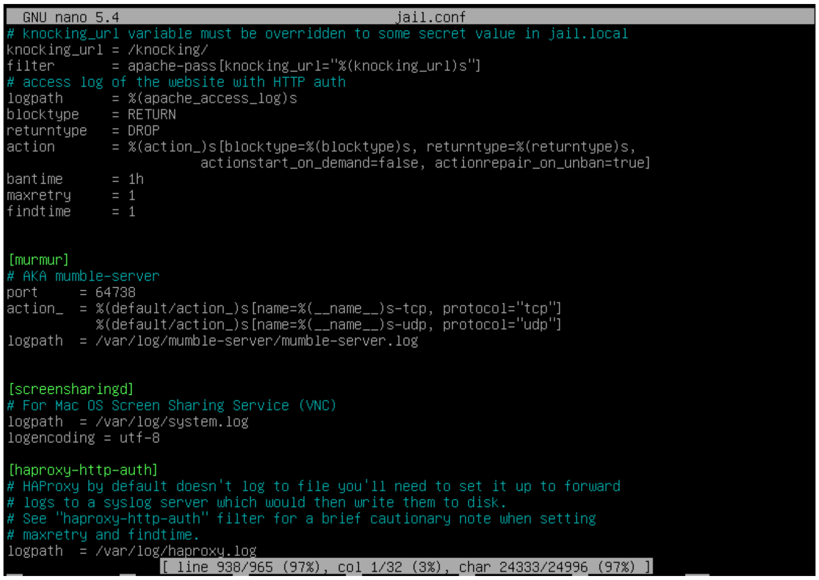
```
  GNU nano 5.4                                    jail.conf
# Jail for more extended banning of persistent abusers
# !!! WARNINGS !!!
# 1. Make sure that your loglevel specified in fail2ban.conf/.local
#    is not at DEBUG level -- which might then cause fail2ban to fall into
#    an infinite loop constantly feeding itself with non-informative lines
# 2. Increase dbpurgeage defined in fail2ban.conf to e.g. 648000 (7.5 days)
#    to maintain entries for failed logins for sufficient amount of time
[recidive]

logpath  = /var/log/fail2ban.log
banaction = %(banaction_allports)s
bantime  = 1w
findtime = 1d


# Generic filter for PAM. Has to be used with action which bans all
# ports such as iptables-allports, shorewall

[pam-generic]
# pam-generic filter can be customized to monitor specific subset of 'tty's
banaction = %(banaction_allports)s
logpath  = %(syslog_authpriv)s
backend  = %(syslog_backend)s


[xinetd-fail]

banaction = iptables-multiport-log
logpath   = %(syslog_daemon)s
backend   = %(syslog_backend)s
maxretry  = 2

```



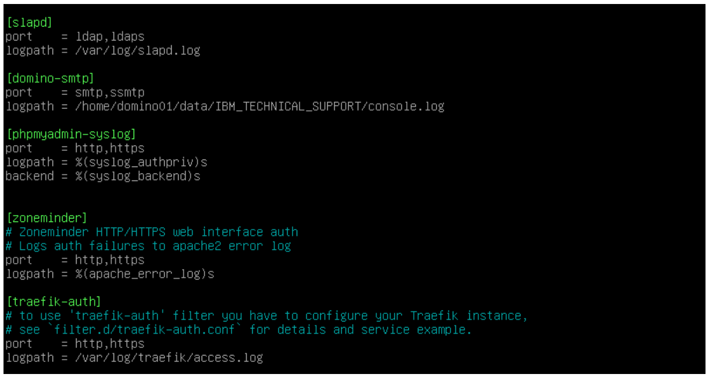
```
  GNU nano 5.4                                    jail.conf
# stunnel - need to set port for this
[stunnel]

logpath = /var/log/stunnel4/stunnel.log


[ejabberd-auth]

port    = 5222
logpath = /var/log/ejabberd/ejabberd.log


[counter-strike]

logpath = /opt/cstrike/logs/L[0-9]*.log
tcpport = 27030,27031,27032,27033,27034,27035,27036,27037,27038,27039
udpport = 1200,27000,27001,27002,27003,27004,27005,27006,27007,27008,27009,27010,27011,27012,27013,>
action_  = %(default/action_)s[name=%(__name__)s-tcp, port="%(tcpport)s", protocol="tcp"]
           %(default/action_)s[name=%(__name__)s-udp, port="%(udpport)s", protocol="udp"]

[softethervpn]
port     = 500,4500
protocol = udp
logpath  = /usr/local/vpnserver/security_log/*/sec.log

[gitlab]
port    = http,https
logpath = /var/log/gitlab/gitlab-rails/application.log

[grafana]
port    = http,https
logpath = /var/log/grafana/grafana.log

```



```
  GNU nano 5.4                                    jail.conf
[bitwarden]
port     = http,https
logpath = /home/*/bwdata/logs/identity/Identity/log.txt

[centreon]
port     = http,https
logpath = /var/log/centreon/login.log

# consider low maxretry and a long bantime
# nobody except your own Nagios server should ever probe nrpe
[nagios]

logpath  = %(syslog_daemon)s     ; nrpe.cfg may define a different log_facility
backend  = %(syslog_backend)s
maxretry = 1


[oracleims]
# see "oracleims" filter file for configuration requirement for Oracle IMS v6 and above
logpath = /opt/sun/comms/messaging64/log/mail.log_current
banaction = %(banaction_allports)s

[directadmin]
logpath = /var/log/directadmin/login.log
port = 2222

[portsentry]
logpath  = /var/lib/portsentry/portsentry.history
maxretry = 1

[pass2allow-ftp]
# this pass2allow example allows FTP traffic after successful HTTP authentication
port         = ftp,ftp-data,ftps,ftps-data
```



```
  GNU nano 5.4                                    jail.conf
# knocking_url variable must be overridden to some secret value in jail.local
knocking_url = /knocking/
filter       = apache-pass[knocking_url="%(knocking_url)s"]
# access log of the website with HTTP auth
logpath      = %(apache_access_log)s
blocktype    = RETURN
returntype   = DROP
action       = %(action_)s[blocktype=%(blocktype)s, returntype=%(returntype)s,
                     actionstart_on_demand=false, actionrepair_on_unban=true]
bantime      = 1h
maxretry     = 1
findtime     = 1


[murmur]
# AKA mumble-server
port     = 64738
action_  = %(default/action_)s[name=%(__name__)s-tcp, protocol="tcp"]
           %(default/action_)s[name=%(__name__)s-udp, protocol="udp"]
logpath  = /var/log/mumble-server/mumble-server.log


[screensharingd]
# For Mac OS Screen Sharing Service (VNC)
logpath  = /var/log/system.log
logencoding = utf-8

[haproxy-http-auth]
# HAProxy by default doesn't log to file you'll need to set it up to forward
# logs to a syslog server which would then write them to disk.
# See "haproxy-http-auth" filter for a brief cautionary note when setting
# maxretry and findtime.
logpath  = /var/log/haproxy.log
                   [ line 938/965 (97%), col 1/32 (3%), char 24333/24996 (97%) ]
```

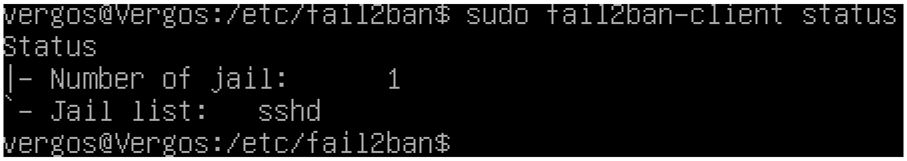


```
[slapd]
port    = ldap,ldaps
logpath = /var/log/slapd.log

[domino-smtp]
port    = smtp,ssmtp
logpath = /home/domino01/data/IBM_TECHNICAL_SUPPORT/console.log

[phpmyadmin-syslog]
port    = http,https
logpath = %(syslog_authpriv)s
backend = %(syslog_backend)s


[zoneminder]
# Zoneminder HTTP/HTTPS web interface auth
# Logs auth failures to apache2 error log
port    = http,https
logpath = %(apache_error_log)s

[traefik-auth]
# to use 'traefik-auth' filter you have to configure your Traefik instance,
# see `filter.d/traefik-auth.conf` for details and service example.
port    = http,https
logpath = /var/log/traefik/access.log
```

b)

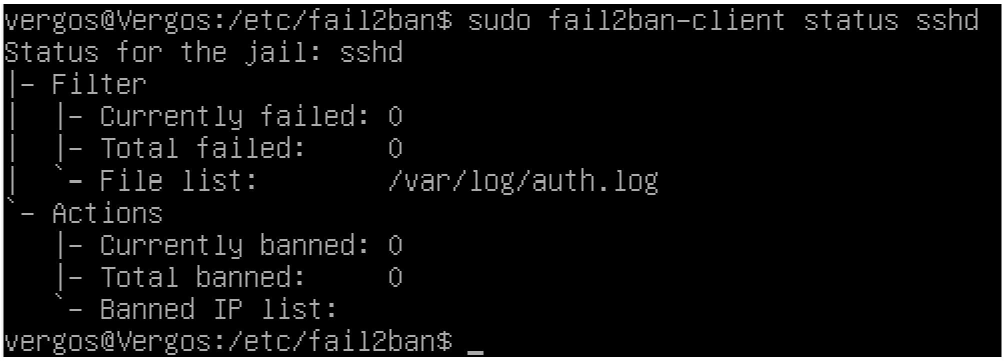
i)

Η κατάσταση των jails με fail2ban-client status:



```
vergos@Vergos:/etc/fail2ban$ sudo fail2ban-client status
Status
|- Number of jail:      1
`- Jail list:   sshd
vergos@Vergos:/etc/fail2ban$
```

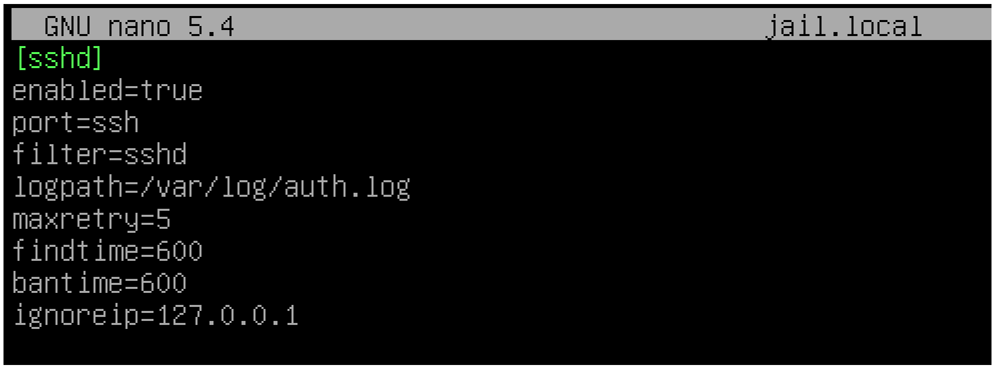
Και fail2ban-client status sshd:



```
vergos@Vergos:/etc/fail2ban$ sudo fail2ban-client status sshd
Status for the jail: sshd
|- Filter
|  |- Currently failed: 0
|  |- Total failed:     0
|  `- File list:        /var/log/auth.log
`- Actions
   |- Currently banned: 0
   |- Total banned:     0
   `- Banned IP list:
vergos@Vergos:/etc/fail2ban$ _
```

ii)

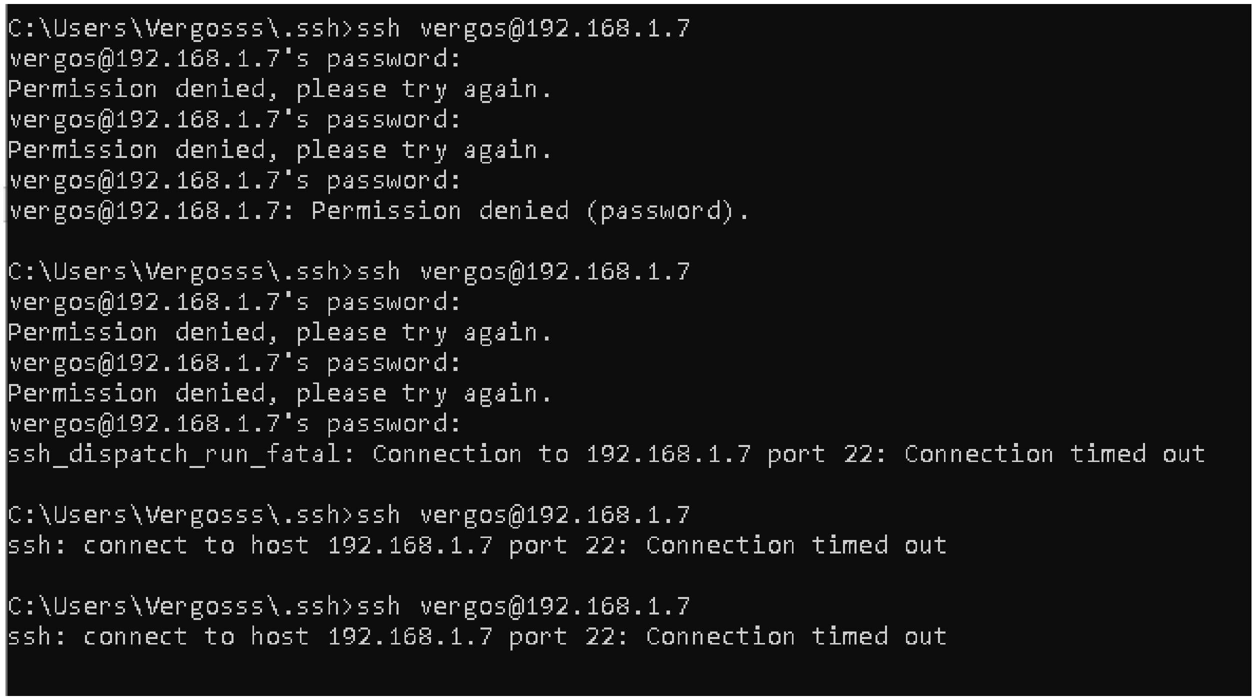
Το φίλτρο για το sshd ορίζεται ως εξής για να κλειδώνει τις συνδέσεις μετά από 5 αποτυχημένες προσπάθειες στα τελευταία 10 λεπτά(600 seconds):



```
  GNU nano 5.4                                      jail.local
[sshd]
enabled=true
port=ssh
filter=sshd
logpath=/var/log/auth.log
maxretry=5
findtime=600
bantime=600
ignoreip=127.0.0.1
```

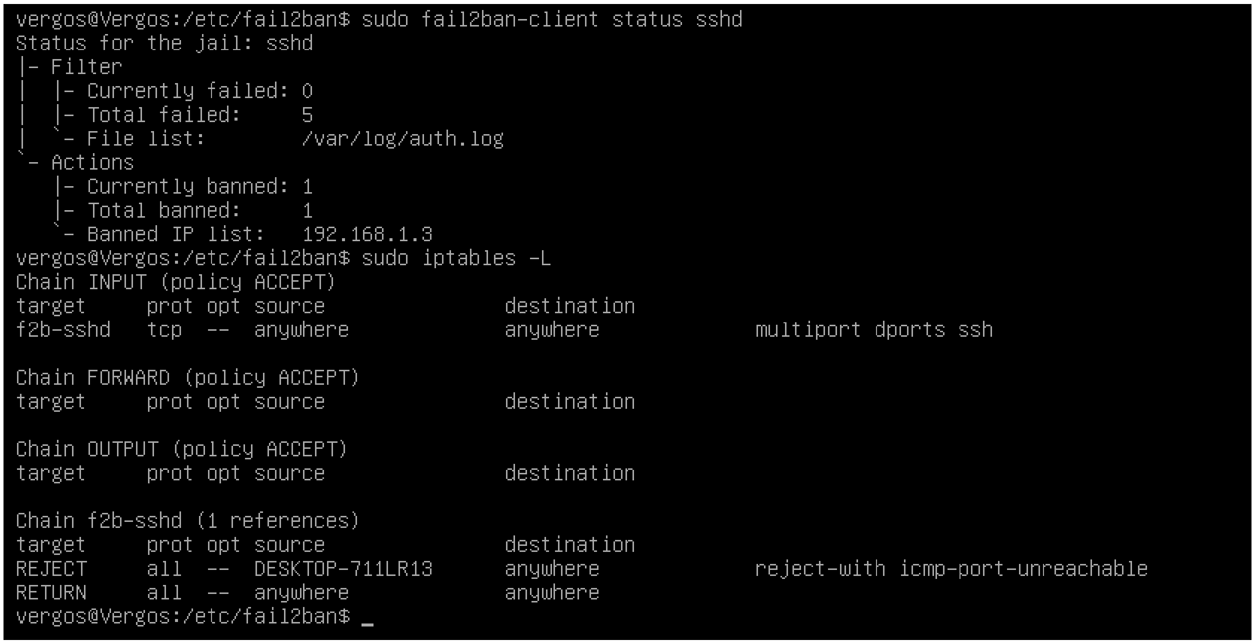
iii)

Έπειτα από 5 λανθασμένες προσπάθειες σύνδεσης:



```
C:\Users\Vergosss\.ssh>ssh vergos@192.168.1.7
vergos@192.168.1.7's password:
Permission denied, please try again.
vergos@192.168.1.7's password:
Permission denied, please try again.
vergos@192.168.1.7's password:
vergos@192.168.1.7: Permission denied (password).

C:\Users\Vergosss\.ssh>ssh vergos@192.168.1.7
vergos@192.168.1.7's password:
Permission denied, please try again.
vergos@192.168.1.7's password:
Permission denied, please try again.
vergos@192.168.1.7's password:
ssh_dispatch_run_fatal: Connection to 192.168.1.7 port 22: Connection timed out

C:\Users\Vergosss\.ssh>ssh vergos@192.168.1.7
ssh: connect to host 192.168.1.7 port 22: Connection timed out

C:\Users\Vergosss\.ssh>ssh vergos@192.168.1.7
ssh: connect to host 192.168.1.7 port 22: Connection timed out
```

η κατάσταση του jail για το ssh daemon και του firewall είναι η εξής:

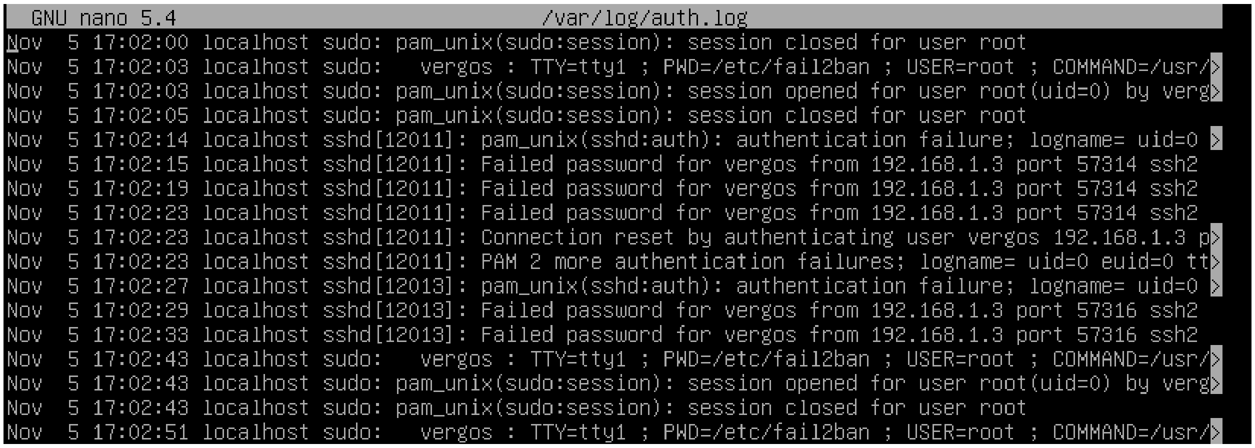


```
vergos@Vergos:/etc/fail2ban$ sudo fail2ban-client status sshd
Status for the jail: sshd
|- Filter
|  |- Currently failed: 0
|  |- Total failed:     5
|  `- File list:        /var/log/auth.log
`- Actions
   |- Currently banned: 1
   |- Total banned:     1
   `- Banned IP list:   192.168.1.3
vergos@Vergos:/etc/fail2ban$ sudo iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
f2b-sshd   tcp  --  anywhere             anywhere             multiport dports ssh

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination

Chain f2b-sshd (1 references)
target     prot opt source               destination
REJECT     all  --  DESKTOP-711LR13      anywhere             reject-with icmp-port-unreachable
RETURN     all  --  anywhere             anywhere
vergos@Vergos:/etc/fail2ban$ _
```

Βλέπουμε πως έχει banάρει το host με όνομα DESKTOP-711LR13 δηλαδή ο υπολογιστής από τον οποίο επιχειρώ την ssh σύνδεση δηλαδή ο 192.168.1.3

iv)

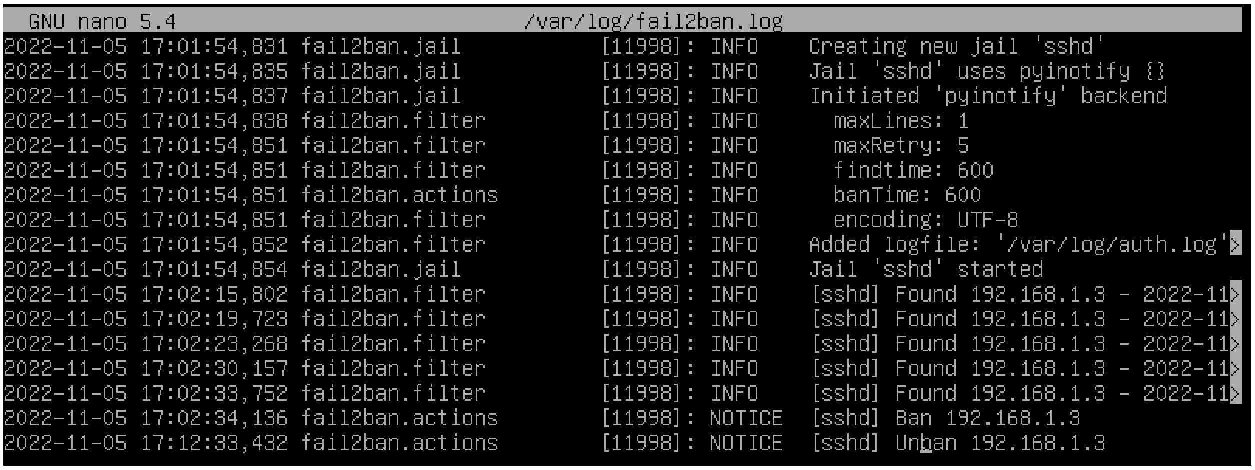
Οι συνδέσεις μέσω ssh καταγράφονται στο αρχείο /var/auth.log:



```
  GNU nano 5.4                        /var/log/auth.log
Nov  5 17:02:00 localhost sudo: pam_unix(sudo:session): session closed for user root
Nov  5 17:02:03 localhost sudo:   vergos : TTY=tty1 ; PWD=/etc/fail2ban ; USER=root ; COMMAND=/usr/>
Nov  5 17:02:03 localhost sudo: pam_unix(sudo:session): session opened for user root(uid=0) by verg>
Nov  5 17:02:05 localhost sudo: pam_unix(sudo:session): session closed for user root
Nov  5 17:02:14 localhost sshd[12011]: pam_unix(sshd:auth): authentication failure; logname= uid=0 >
Nov  5 17:02:15 localhost sshd[12011]: Failed password for vergos from 192.168.1.3 port 57314 ssh2
Nov  5 17:02:19 localhost sshd[12011]: Failed password for vergos from 192.168.1.3 port 57314 ssh2
Nov  5 17:02:23 localhost sshd[12011]: Failed password for vergos from 192.168.1.3 port 57314 ssh2
Nov  5 17:02:23 localhost sshd[12011]: Connection reset by authenticating user vergos 192.168.1.3 p>
Nov  5 17:02:23 localhost sshd[12011]: PAM 2 more authentication failures; logname= uid=0 euid=0 tt>
Nov  5 17:02:27 localhost sshd[12013]: pam_unix(sshd:auth): authentication failure; logname= uid=0 >
Nov  5 17:02:29 localhost sshd[12013]: Failed password for vergos from 192.168.1.3 port 57316 ssh2
Nov  5 17:02:33 localhost sshd[12013]: Failed password for vergos from 192.168.1.3 port 57316 ssh2
Nov  5 17:02:43 localhost sudo:   vergos : TTY=tty1 ; PWD=/etc/fail2ban ; USER=root ; COMMAND=/usr/>
Nov  5 17:02:43 localhost sudo: pam_unix(sudo:session): session opened for user root(uid=0) by verg>
Nov  5 17:02:43 localhost sudo: pam_unix(sudo:session): session closed for user root
Nov  5 17:02:51 localhost sudo:   vergos : TTY=tty1 ; PWD=/etc/fail2ban ; USER=root ; COMMAND=/usr/>
```

Η στήλη 5 δείχνει το είδος της δραστηριότητας(π.χ ssh) και η 7η στήλη δείχνει το συμβάν σχετιζόμενο με τη δραστηριότητα δηλαδή failed password for vergos from 192.168.1.3 port 57314 ssh2 για ανεπιτυχή σύνδεση.

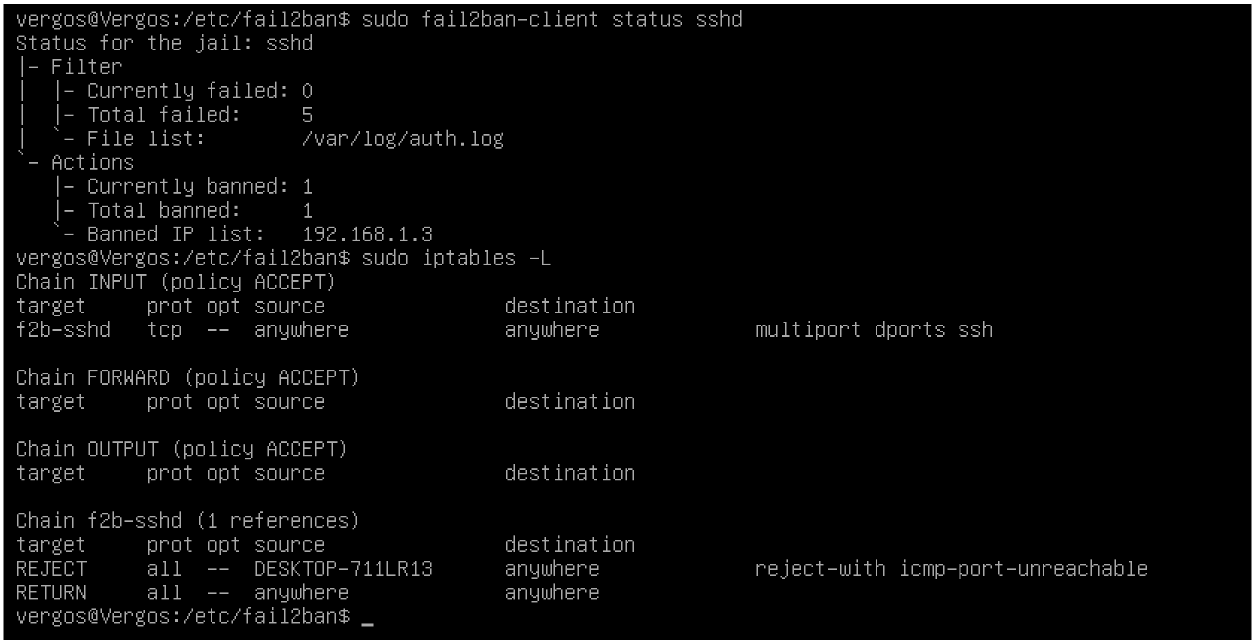
Επίσης στην παρακάτω εικόνα φαίνονται και οι ανεπιτυχείς συνδέσεις αλλά και ο αποκλεισμός(ban) της ip από το fail2ban:



```
  GNU nano 5.4                       /var/log/fail2ban.log
2022-11-05 17:01:54,831 fail2ban.jail           [11998]: INFO    Creating new jail 'sshd'
2022-11-05 17:01:54,835 fail2ban.jail           [11998]: INFO    Jail 'sshd' uses pyinotify {}
2022-11-05 17:01:54,837 fail2ban.jail           [11998]: INFO    Initiated 'pyinotify' backend
2022-11-05 17:01:54,838 fail2ban.filter         [11998]: INFO      maxLines: 1
2022-11-05 17:01:54,851 fail2ban.filter         [11998]: INFO      maxRetry: 5
2022-11-05 17:01:54,851 fail2ban.filter         [11998]: INFO      findtime: 600
2022-11-05 17:01:54,851 fail2ban.actions        [11998]: INFO      banTime: 600
2022-11-05 17:01:54,851 fail2ban.filter         [11998]: INFO      encoding: UTF-8
2022-11-05 17:01:54,852 fail2ban.filter         [11998]: INFO    Added logfile: '/var/log/auth.log'>
2022-11-05 17:01:54,854 fail2ban.jail           [11998]: INFO    Jail 'sshd' started
2022-11-05 17:02:15,802 fail2ban.filter         [11998]: INFO    [sshd] Found 192.168.1.3 - 2022-11>
2022-11-05 17:02:19,723 fail2ban.filter         [11998]: INFO    [sshd] Found 192.168.1.3 - 2022-11>
2022-11-05 17:02:23,268 fail2ban.filter         [11998]: INFO    [sshd] Found 192.168.1.3 - 2022-11>
2022-11-05 17:02:30,157 fail2ban.filter         [11998]: INFO    [sshd] Found 192.168.1.3 - 2022-11>
2022-11-05 17:02:33,752 fail2ban.filter         [11998]: INFO    [sshd] Found 192.168.1.3 - 2022-11>
2022-11-05 17:02:34,136 fail2ban.actions        [11998]: NOTICE  [sshd] Ban 192.168.1.3
2022-11-05 17:12:33,432 fail2ban.actions        [11998]: NOTICE  [sshd] Unban 192.168.1.3
```

v)

Βλέποντας την κατάσταση του firewall και του sshd jail παρατηρούμε ότι έχει banάρει το host με όνομα DESKTOP-711LR13 δηλαδή ο υπολογιστής από τον οποίο επιχειρώ την ssh σύνδεση δηλαδή ο 192.168.1.3

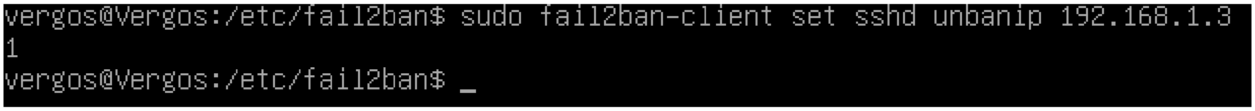


```
vergos@Vergos:/etc/fail2ban$ sudo fail2ban-client status sshd
Status for the jail: sshd
|- Filter
|  |- Currently failed: 0
|  |- Total failed:     5
|  `- File list:        /var/log/auth.log
`- Actions
   |- Currently banned: 1
   |- Total banned:     1
   `- Banned IP list:   192.168.1.3
vergos@Vergos:/etc/fail2ban$ sudo iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
f2b-sshd   tcp  --  anywhere             anywhere             multiport dports ssh

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination

Chain f2b-sshd (1 references)
target     prot opt source               destination
REJECT     all  --  DESKTOP-711LR13      anywhere             reject-with icmp-port-unreachable
RETURN     all  --  anywhere             anywhere
vergos@Vergos:/etc/fail2ban$ _
```

vi)

Για να κάνουμε unban μία ip εκτελούμε την εντολή:

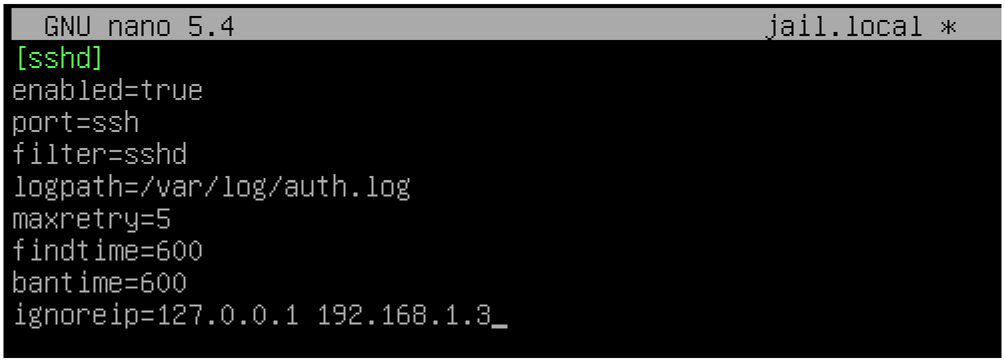
fail2ban-client set sshd unbanip 192.168.1.3



```
vergos@Vergos:/etc/fail2ban$ sudo fail2ban-client set sshd unbanip 192.168.1.3
1
vergos@Vergos:/etc/fail2ban$ _
```

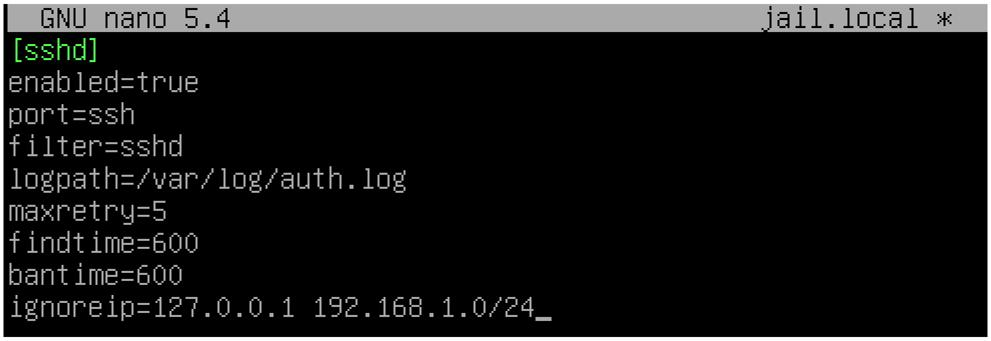
vii)

Στο αρχείο jail.local μπορούμε να προσθέσουμε τις ip, υποδίκτυα που δε θέλουμε να φιλτράρονται στη γραμμή ignoreip:



```
  GNU nano 5.4                                    jail.local *
[sshd]
enabled=true
port=ssh
filter=sshd
logpath=/var/log/auth.log
maxretry=5
findtime=600
bantime=600
ignoreip=127.0.0.1 192.168.1.3_
```

Και για υποδίκτυα(π.χ όλες τις ip από το LAN):

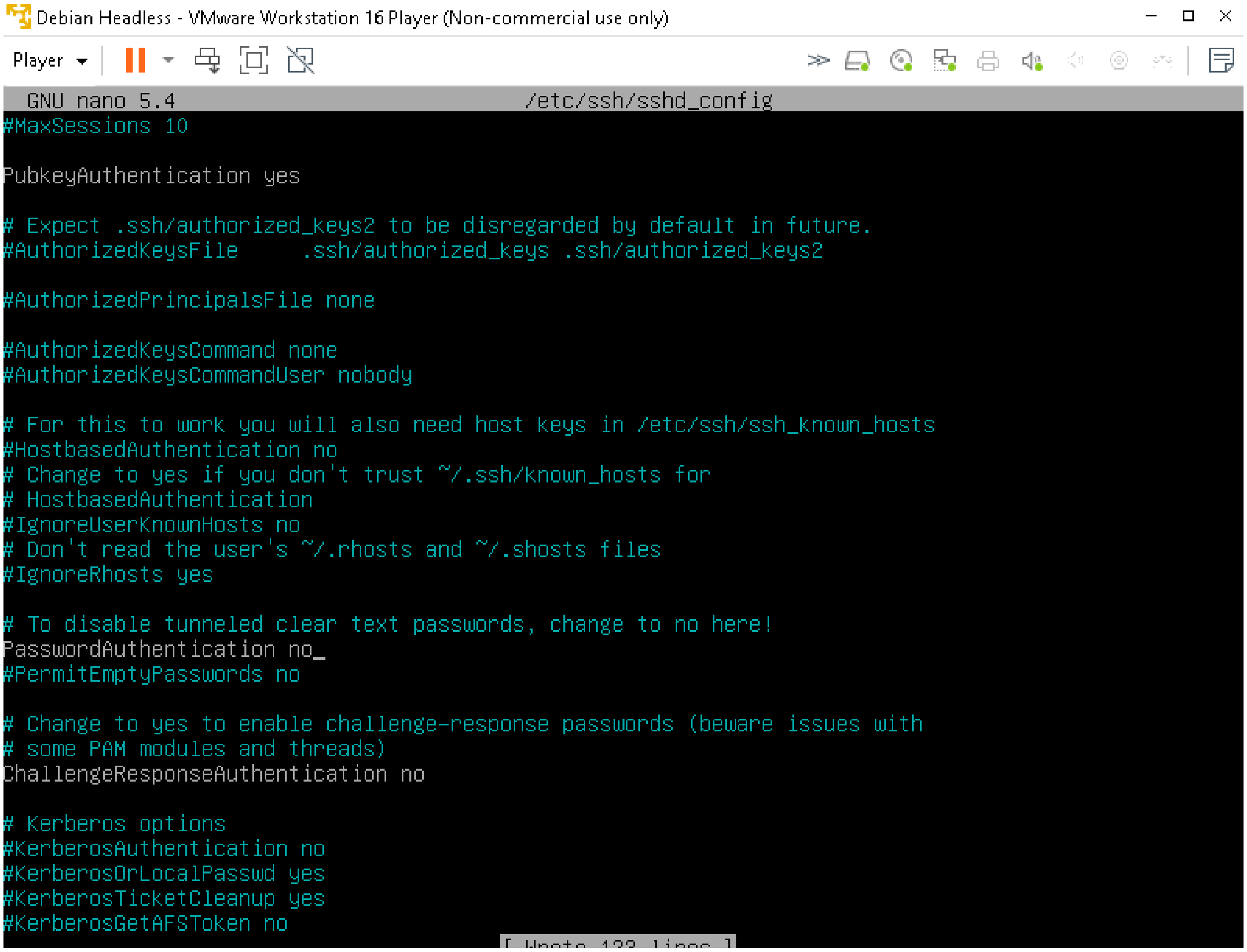


```
  GNU nano 5.4                                    jail.local *
[sshd]
enabled=true
port=ssh
filter=sshd
logpath=/var/log/auth.log
maxretry=5
findtime=600
bantime=600
ignoreip=127.0.0.1 192.168.1.0/24_
```

2) Χρήση Public Key Authentication

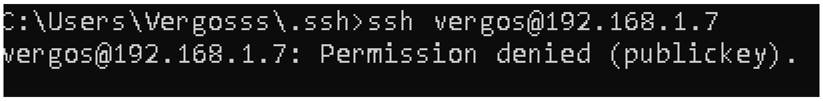
i)

Αρχικά προσπαθώ να συνδεθώ στον server χωρίς κάποιο κλειδί ενώ η πρόσβαση είναι επιτρεπτή μόνο με τη χρήση δημοσίου κλειδιού:


Debian Headless - VMware Workstation 16 Player (Non-commercial use only)
Player

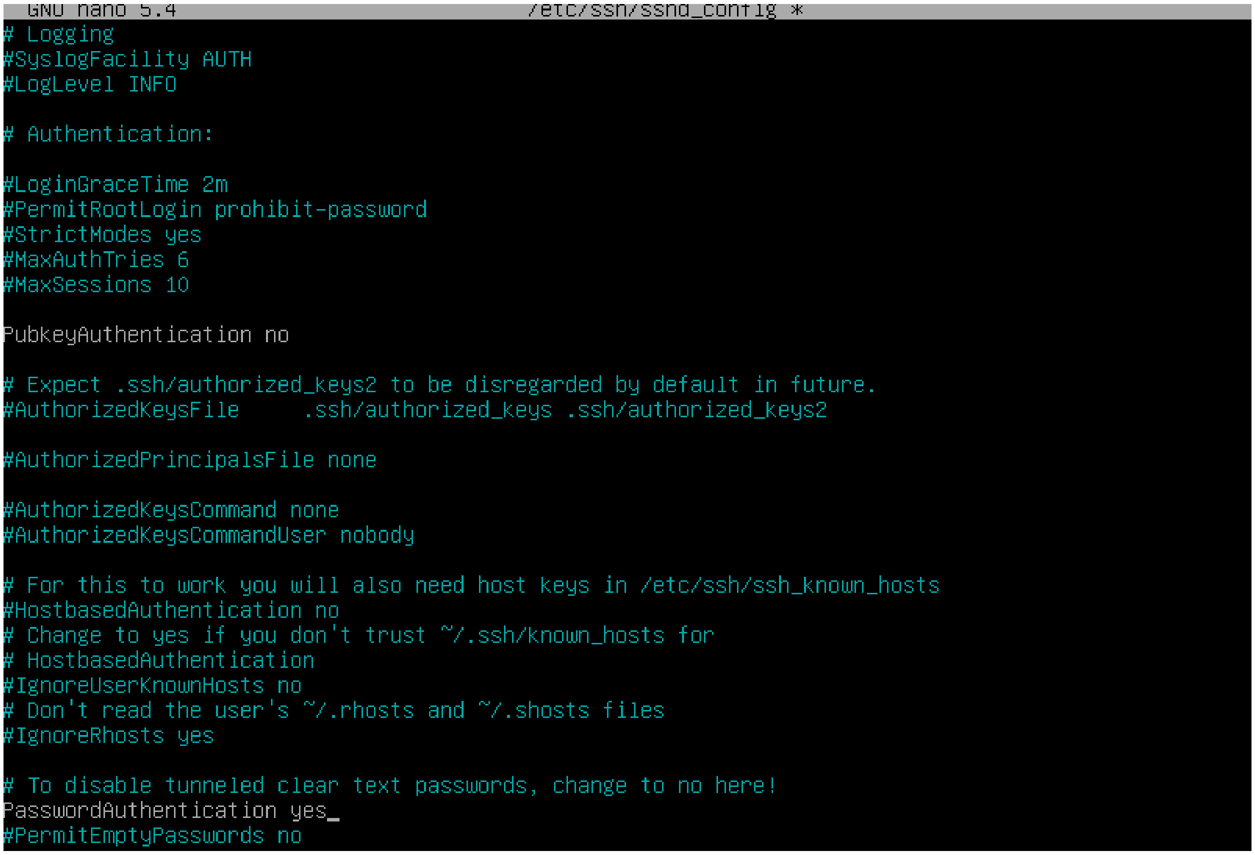
```
  GNU nano 5.4                         /etc/ssh/sshd_config
#MaxSessions 10

PubkeyAuthentication yes

# Expect .ssh/authorized_keys2 to be disregarded by default in future.
#AuthorizedKeysFile     .ssh/authorized_keys .ssh/authorized_keys2

#AuthorizedPrincipalsFile none

#AuthorizedKeysCommand none
#AuthorizedKeysCommandUser nobody

# For this to work you will also need host keys in /etc/ssh/ssh_known_hosts
#HostbasedAuthentication no
# Change to yes if you don't trust ~/.ssh/known_hosts for
# HostbasedAuthentication
#IgnoreUserKnownHosts no
# Don't read the user's ~/.rhosts and ~/.shosts files
#IgnoreRhosts yes

# To disable tunneled clear text passwords, change to no here!
PasswordAuthentication no_
#PermitEmptyPasswords no

# Change to yes to enable challenge-response passwords (beware issues with
# some PAM modules and threads)
ChallengeResponseAuthentication no

# Kerberos options
#KerberosAuthentication no
#KerberosOrLocalPasswd yes
#KerberosTicketCleanup yes
#KerberosGetAFSToken no
                                        [ Wrote 123 lines ]
```

Και προσπαθώ να συνδεθώ:



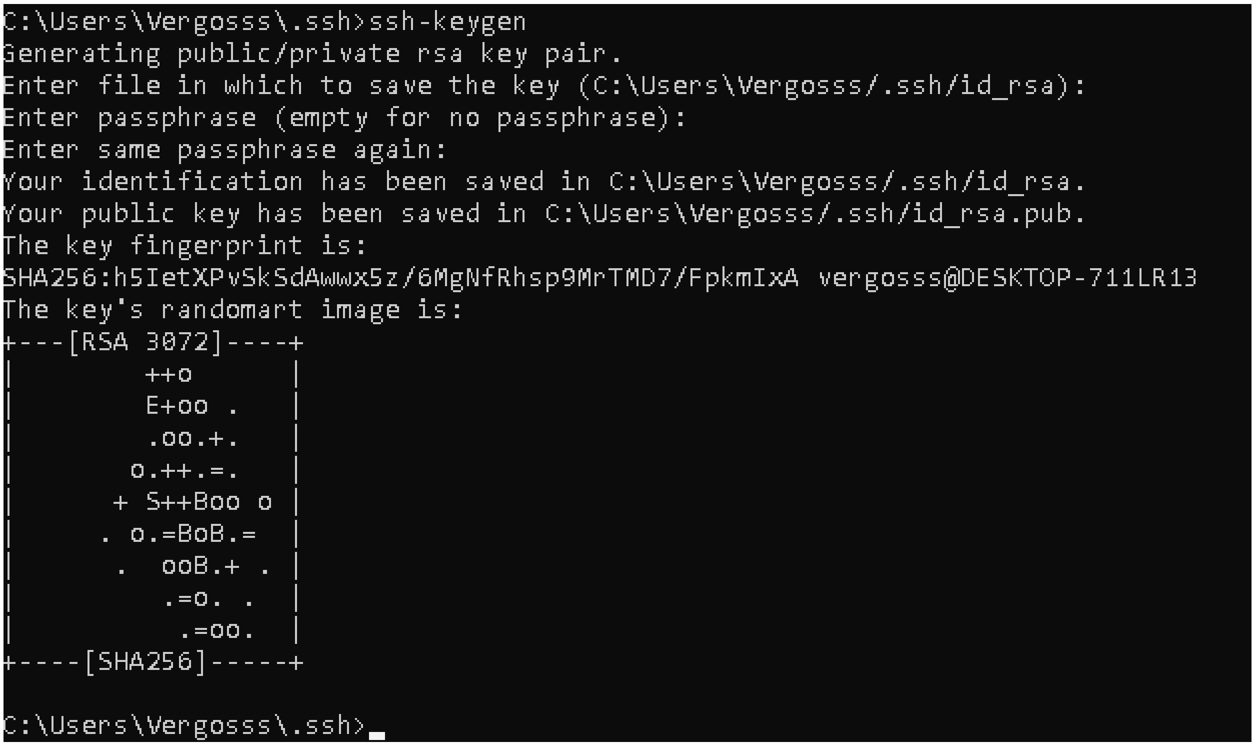
```
C:\Users\Vergosss\.ssh>ssh vergos@192.168.1.7
vergos@192.168.1.7: Permission denied (publickey).
```

Έπειτα προκειμένου να μπορώ να αντιγράψω το δημόσιο κλειδί στον server ενεργοποιώ πάλι την πρόσβαση με password και απενεργοποιώ την πρόσβαση με δημόσιο κλειδί:



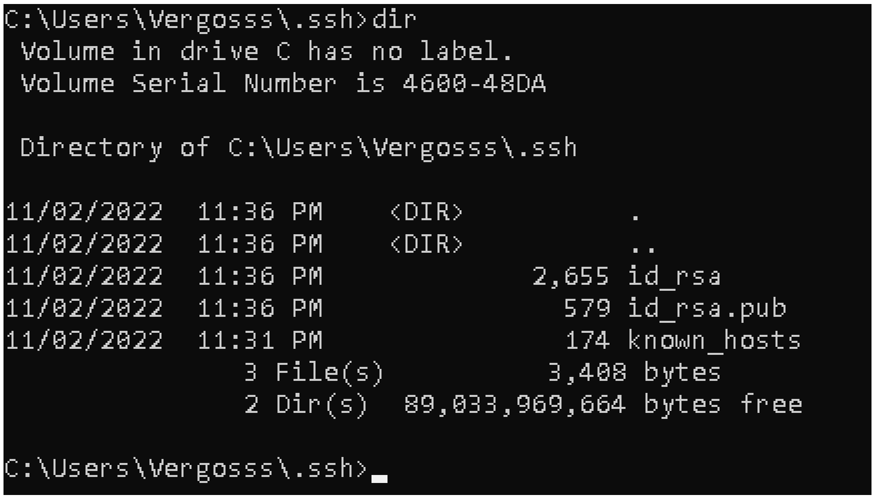
```
  GNU nano 5.4                              /etc/ssh/sshd_config *
# Logging
#SyslogFacility AUTH
#LogLevel INFO

# Authentication:

#LoginGraceTime 2m
#PermitRootLogin prohibit-password
#StrictModes yes
#MaxAuthTries 6
#MaxSessions 10

PubkeyAuthentication no

# Expect .ssh/authorized_keys2 to be disregarded by default in future.
#AuthorizedKeysFile     .ssh/authorized_keys .ssh/authorized_keys2

#AuthorizedPrincipalsFile none

#AuthorizedKeysCommand none
#AuthorizedKeysCommandUser nobody

# For this to work you will also need host keys in /etc/ssh/ssh_known_hosts
#HostbasedAuthentication no
# Change to yes if you don't trust ~/.ssh/known_hosts for
# HostbasedAuthentication
#IgnoreUserKnownHosts no
# Don't read the user's ~/.rhosts and ~/.shosts files
#IgnoreRhosts yes

# To disable tunneled clear text passwords, change to no here!
PasswordAuthentication yes_
#PermitEmptyPasswords no
```

Δημιουργώ τα ζεύγη δημοσίου και ιδιωτικού κλειδιού στον υπολογιστή:



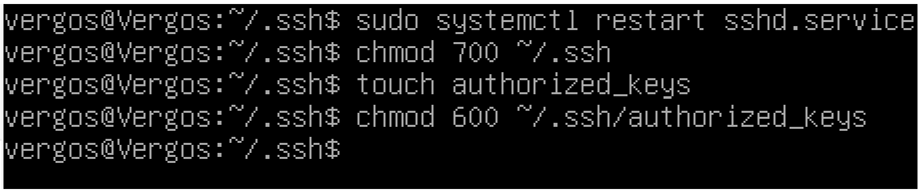
```
C:\Users\Vergosss\.ssh>ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (C:\Users\Vergosss/.ssh/id_rsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in C:\Users\Vergosss/.ssh/id_rsa.
Your public key has been saved in C:\Users\Vergosss/.ssh/id_rsa.pub.
The key fingerprint is:
SHA256:h5IetXPvSkSdAwwx5z/6MgNfRhsp9MrTMD7/FpkmIxA vergosss@DESKTOP-711LR13
The key's randomart image is:
+---[RSA 3072]----+
|        ++o      |
|        E+oo .   |
|        .oo.+.   |
|       o.++.=.   |
|      + S++Boo o |
|     . o.=BoB.=  |
|      .  ooB.+ . |
|         .=o. .  |
|          .=oo.  |
+----[SHA256]-----+

C:\Users\Vergosss\.ssh>
```

Στο παρακάτω στιγμιότυπο φαίνονται και τα δημιουργηθέντα αρχεία:



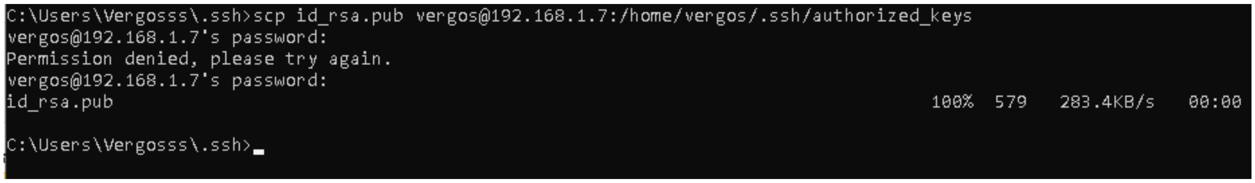
```
C:\Users\Vergosss\.ssh>dir
 Volume in drive C has no label.
 Volume Serial Number is 4600-48DA

 Directory of C:\Users\Vergosss\.ssh

11/02/2022  11:36 PM    <DIR>          .
11/02/2022  11:36 PM    <DIR>          ..
11/02/2022  11:36 PM             2,655 id_rsa
11/02/2022  11:36 PM               579 id_rsa.pub
11/02/2022  11:31 PM               174 known_hosts
               3 File(s)          3,408 bytes
               2 Dir(s)  89,033,969,664 bytes free

C:\Users\Vergosss\.ssh>
```

Δημιουργώ το αρχείο authorized_keys και αλλάζω τα δικαιώματα πρόσβασης στον φάκελο .ssh και στο αρχείο authorized_keys. Για όποιο κλειδί υπάρχει μέσα σε αυτό το αρχείο εάν κάποιος άλλος έχει το αντίστοιχο ιδιωτικό κλειδί θα μπορεί να συνδεθεί στον vm server:



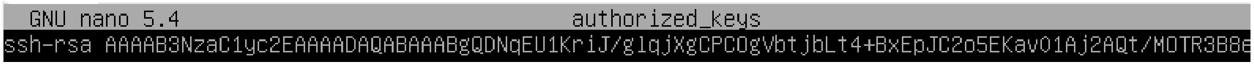
```
vergos@Vergos:~/.ssh$ sudo systemctl restart sshd.service
vergos@Vergos:~/.ssh$ chmod 700 ~/.ssh
vergos@Vergos:~/.ssh$ touch authorized_keys
vergos@Vergos:~/.ssh$ chmod 600 ~/.ssh/authorized_keys
vergos@Vergos:~/.ssh$
```

Αντιγράφω το δημόσιο κλειδί στον server που θέλω να συνδεθώ:



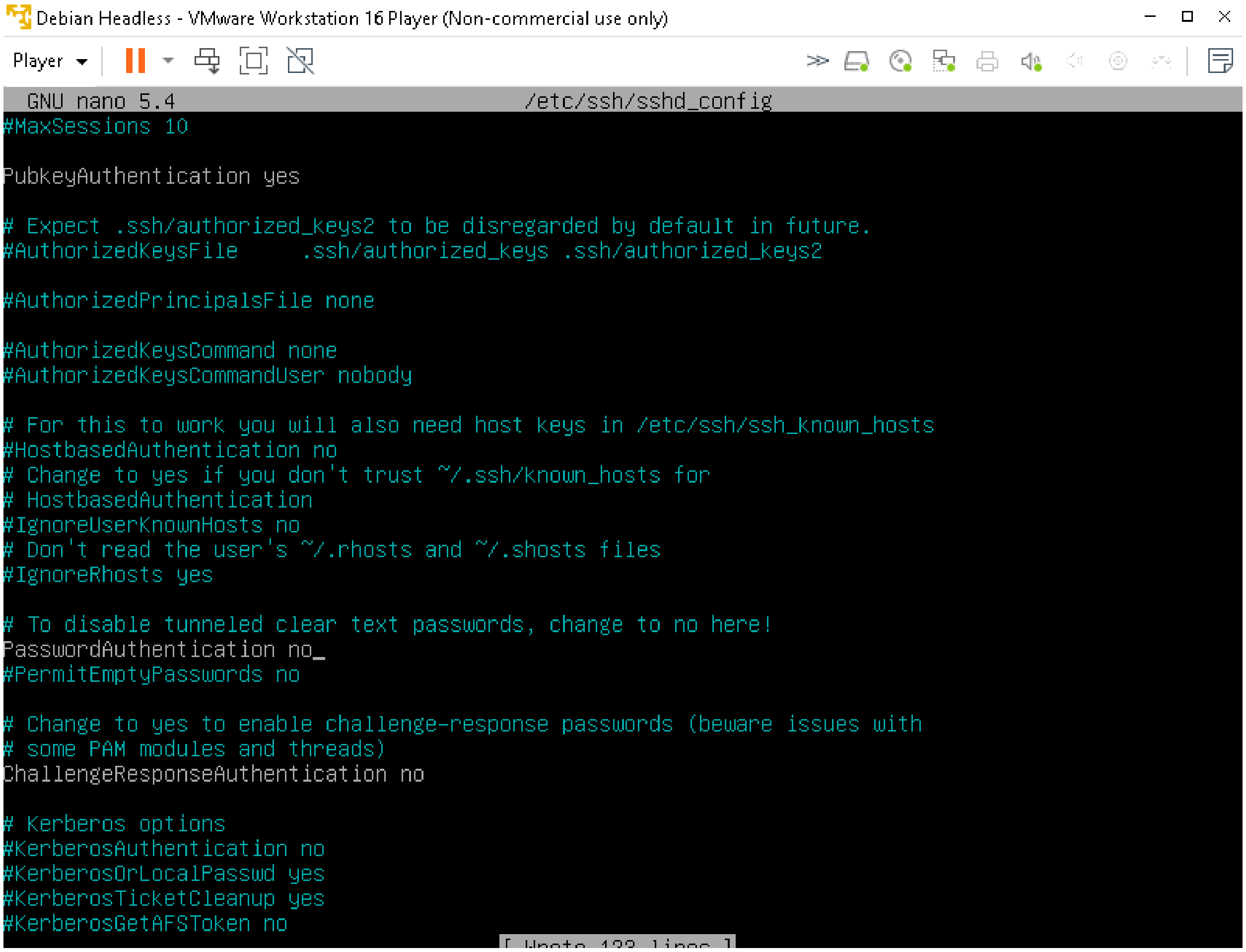
```
C:\Users\Vergosss\.ssh>scp id_rsa.pub vergos@192.168.1.7:/home/vergos/.ssh/authorized_keys
vergos@192.168.1.7's password:
Permission denied, please try again.
vergos@192.168.1.7's password:
id_rsa.pub                                                                    100%  579   283.4KB/s   00:00

C:\Users\Vergosss\.ssh>
```

Εδώ φαίνεται και ότι το κλειδί αντιγράφηκε επιτυχώς:



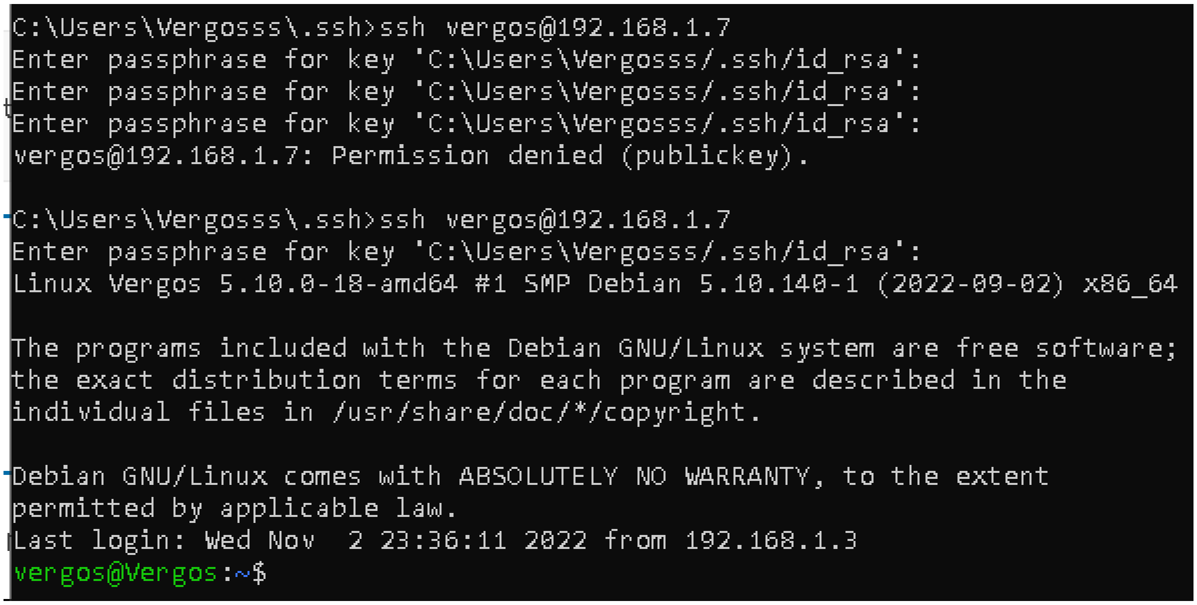
```
  GNU nano 5.4                                authorized_keys
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABgQDNqEU1KriJ/glqjXgCPCOgVbtjbLt4+BxEpJC2o5EKav01Aj2AQt/MOTR3B8e
```

Παραμετροποιώ κατάλληλα το sshd_config αρχείο ώστε η σύνδεση να γίνεται μόνο με δημόσιο κλειδί:


Debian Headless - VMware Workstation 16 Player (Non-commercial use only)
Player

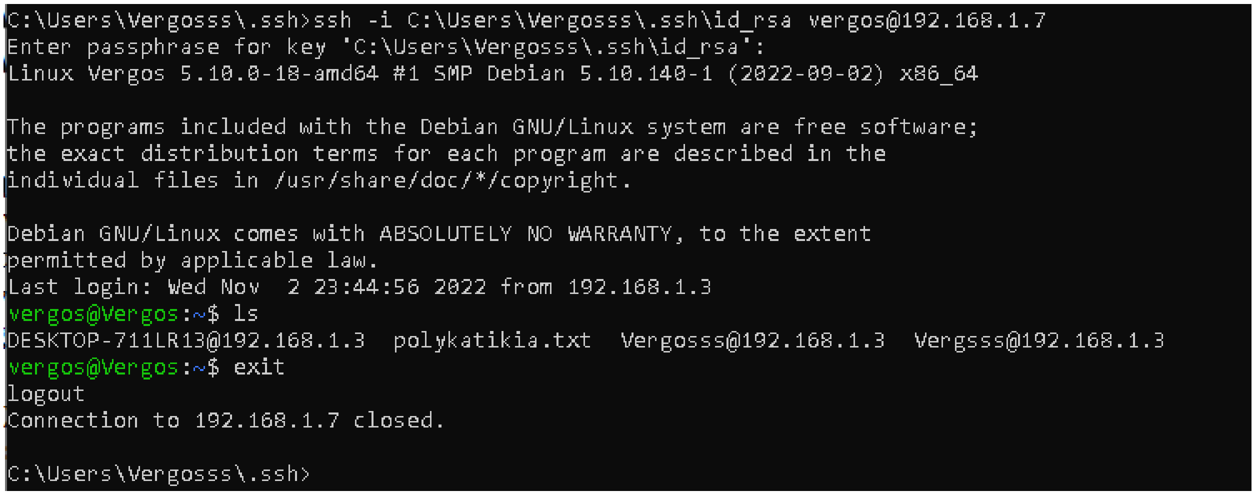
```
  GNU nano 5.4                                        /etc/ssh/sshd_config
#MaxSessions 10

PubkeyAuthentication yes

# Expect .ssh/authorized_keys2 to be disregarded by default in future.
#AuthorizedKeysFile     .ssh/authorized_keys .ssh/authorized_keys2

#AuthorizedPrincipalsFile none

#AuthorizedKeysCommand none
#AuthorizedKeysCommandUser nobody

# For this to work you will also need host keys in /etc/ssh/ssh_known_hosts
#HostbasedAuthentication no
# Change to yes if you don't trust ~/.ssh/known_hosts for
# HostbasedAuthentication
#IgnoreUserKnownHosts no
# Don't read the user's ~/.rhosts and ~/.shosts files
#IgnoreRhosts yes

# To disable tunneled clear text passwords, change to no here!
PasswordAuthentication no_
#PermitEmptyPasswords no

# Change to yes to enable challenge-response passwords (beware issues with
# some PAM modules and threads)
ChallengeResponseAuthentication no

# Kerberos options
#KerberosAuthentication no
#KerberosOrLocalPasswd yes
#KerberosTicketCleanup yes
#KerberosGetAFSToken no
                                        [ Wrote 123 lines ]
```

Επιτυχής σύνδεση στον server:



```
C:\Users\Vergosss\.ssh>ssh vergos@192.168.1.7
Enter passphrase for key 'C:\Users\Vergosss/.ssh/id_rsa':
Enter passphrase for key 'C:\Users\Vergosss/.ssh/id_rsa':
Enter passphrase for key 'C:\Users\Vergosss/.ssh/id_rsa':
vergos@192.168.1.7: Permission denied (publickey).

C:\Users\Vergosss\.ssh>ssh vergos@192.168.1.7
Enter passphrase for key 'C:\Users\Vergosss/.ssh/id_rsa':
Linux Vergos 5.10.0-18-amd64 #1 SMP Debian 5.10.140-1 (2022-09-02) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Wed Nov  2 23:36:11 2022 from 192.168.1.3
vergos@Vergos:~$
```

Ή

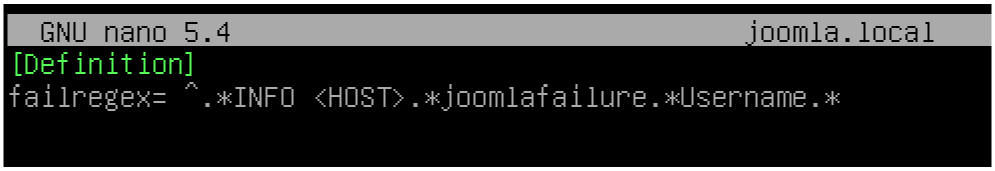


```
C:\Users\Vergosss\.ssh>ssh -i C:\Users\Vergosss\.ssh\id_rsa vergos@192.168.1.7
Enter passphrase for key 'C:\Users\Vergosss\.ssh\id_rsa':
Linux Vergos 5.10.0-18-amd64 #1 SMP Debian 5.10.140-1 (2022-09-02) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Wed Nov  2 23:44:56 2022 from 192.168.1.3
vergos@Vergos:~$ ls
DESKTOP-711LR13@192.168.1.3  polykatikia.txt  Vergosss@192.168.1.3  Vergsss@192.168.1.3
vergos@Vergos:~$ exit
logout
Connection to 192.168.1.7 closed.

C:\Users\Vergosss\.ssh>
```

3) Υλοποιήση νέων φίλτρων για χρήση στο πακέτο fail2ban

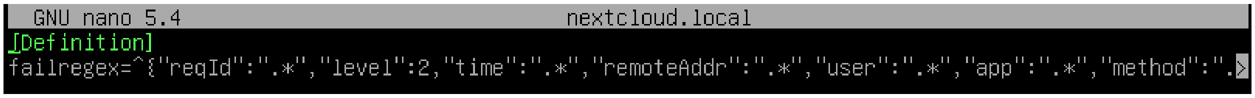
i)

Φίλτρο (κανονική έκφραση για log αρχεία της εφαρμογής joomla):

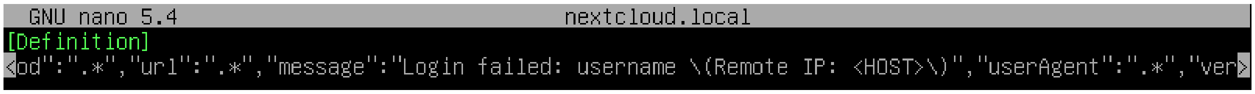


```
  GNU nano 5.4                                joomla.local
[Definition]
failregex= ^.*INFO <HOST>.*joomlafailure.*Username.*
```

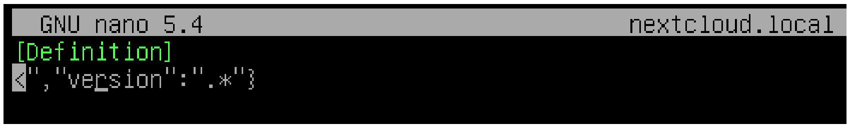
Φίλτρο(κανονική έκφραση για log αρχεία της εφαρμογής nextcloud):



```
  GNU nano 5.4                                nextcloud.local
[Definition]
failregex=^{"reqId":".*","level":2,"time":".*","remoteAddr":".*","user":".*","app":".*","method":".>
```



```
  GNU nano 5.4                                nextcloud.local
[Definition]
<od":".*","url":".*","message":"Login failed: username \(Remote IP: <HOST>\)","userAgent":".*","ver>
```

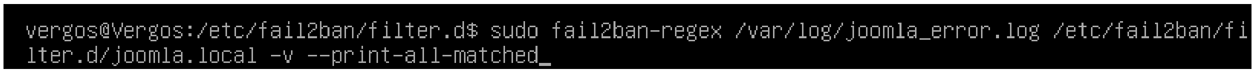


```
  GNU nano 5.4                                nextcloud.local
[Definition]
<","version":".*"}
```

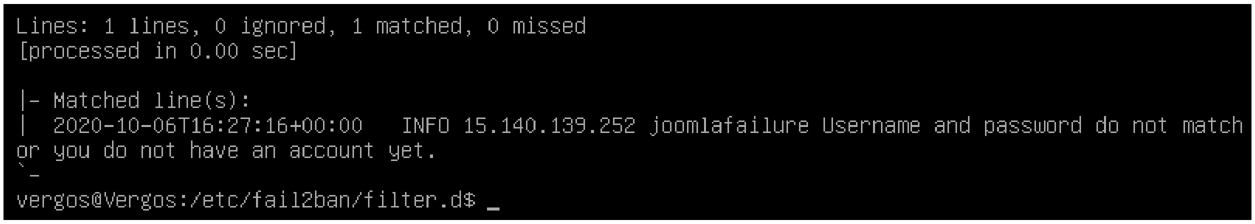
ii)

Τεστάρω τα φίλτρα μέσω της ακόλουθης εντολής fail2ban-regex <αρχείο καταγραφής> <αρχείο που περιέχει την κανονική έκφραση>:

Joomla:

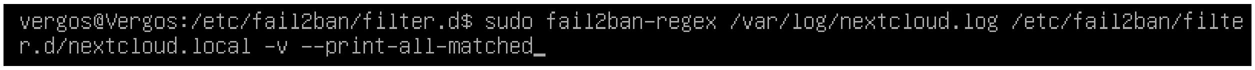


```
vergos@Vergos:/etc/fail2ban/filter.d$ sudo fail2ban-regex /var/log/joomla_error.log /etc/fail2ban/fi
lter.d/joomla.local -v --print-all-matched_
```

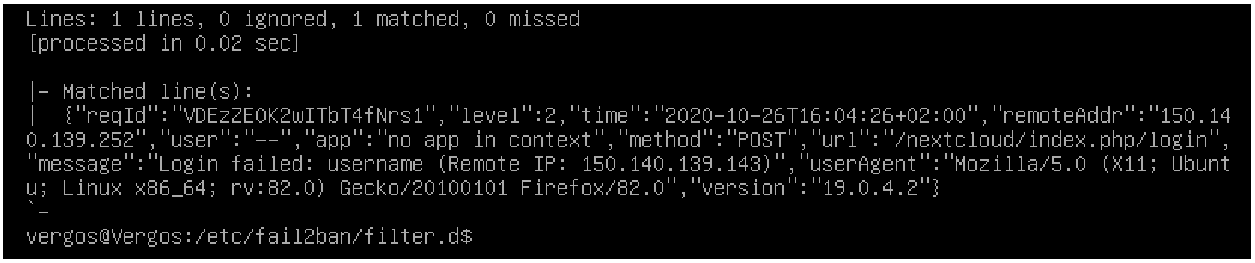


```
Lines: 1 lines, 0 ignored, 1 matched, 0 missed
[processed in 0.00 sec]

|- Matched line(s):
|  2020-10-06T16:27:16+00:00   INFO 15.140.139.252 joomlafailure Username and password do not match
or you do not have an account yet.
`-
vergos@Vergos:/etc/fail2ban/filter.d$ _
```

Nextcloud:



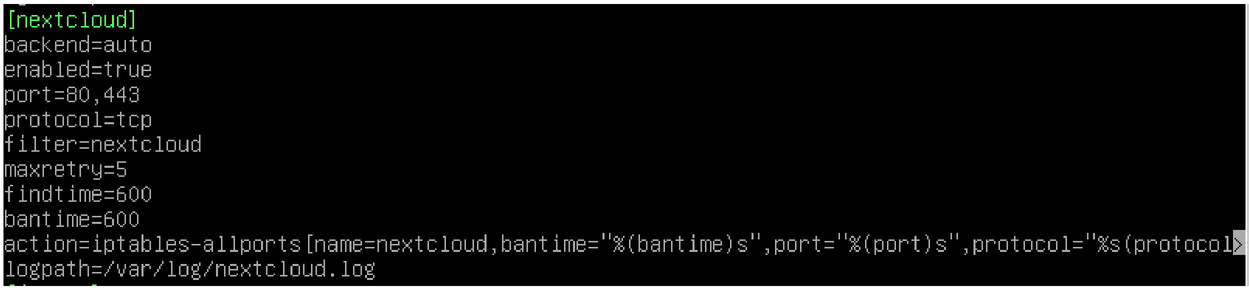
```
vergos@Vergos:/etc/fail2ban/filter.d$ sudo fail2ban-regex /var/log/nextcloud.log /etc/fail2ban/filte
r.d/nextcloud.local -v --print-all-matched_
```



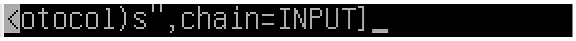
```
Lines: 1 lines, 0 ignored, 1 matched, 0 missed
[processed in 0.02 sec]

|- Matched line(s):
|  {"reqId":"VDEzZEOK2wITbT4fNrs1","level":2,"time":"2020-10-26T16:04:26+02:00","remoteAddr":"150.14
0.139.252","user":"--","app":"no app in context","method":"POST","url":"/nextcloud/index.php/login",
"message":"Login failed: username (Remote IP: 150.140.139.143)","userAgent":"Mozilla/5.0 (X11; Ubunt
u; Linux x86_64; rv:82.0) Gecko/20100101 Firefox/82.0","version":"19.0.4.2"}
`-
vergos@Vergos:/etc/fail2ban/filter.d$
```

iii)

Ορίζω ports, protocols, maxretries, bantime, findtime , iptables chains για το jail του nextcloud στο αρχείο jail.local:

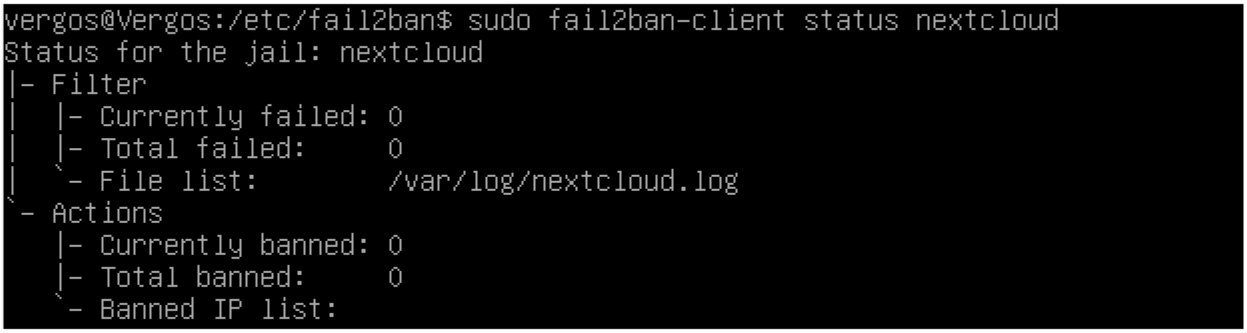


```
[nextcloud]
backend=auto
enabled=true
port=80,443
protocol=tcp
filter=nextcloud
maxretry=5
findtime=600
bantime=600
action=iptables-allports[name=nextcloud,bantime="%(bantime)s",port="%(port)s",protocol="%s(protocol>
logpath=/var/log/nextcloud.log
```



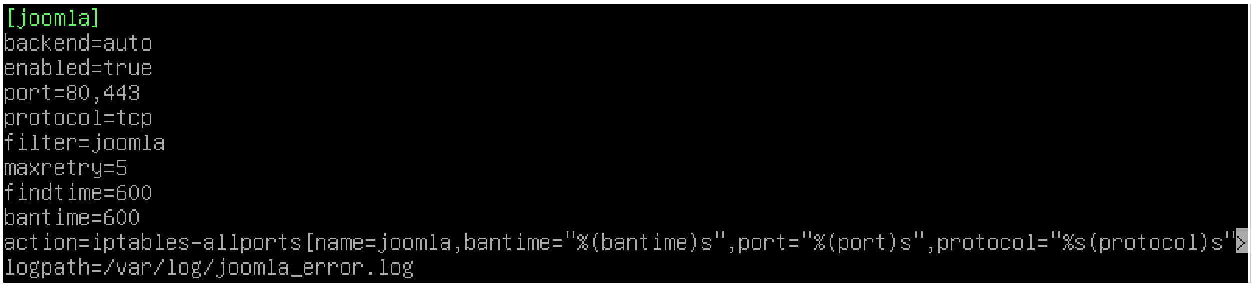
```
<otocol)s",chain=INPUT]_
```

Τσεκάρω την κατάσταση του jail:

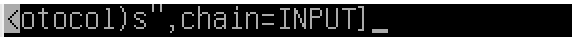


```
vergos@Vergos:/etc/fail2ban$ sudo fail2ban-client status nextcloud
Status for the jail: nextcloud
|- Filter
|  |- Currently failed: 0
|  |- Total failed:     0
|  `- File list:        /var/log/nextcloud.log
`- Actions
   |- Currently banned: 0
   |- Total banned:     0
   `- Banned IP list:
```

Ορίζω ports, protocols, maxretries, bantime, findtime , iptables chains για το jail του joomla στο αρχείο jail.local:

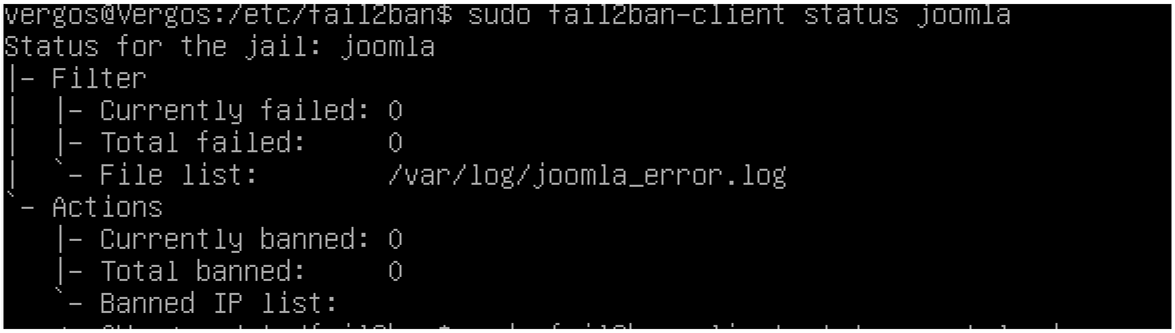


```
[joomla]
backend=auto
enabled=true
port=80,443
protocol=tcp
filter=joomla
maxretry=5
findtime=600
bantime=600
action=iptables-allports[name=joomla,bantime="%(bantime)s",port="%(port)s",protocol="%s(protocol)s">
logpath=/var/log/joomla_error.log
```



```
<otocol)s",chain=INPUT]_
```

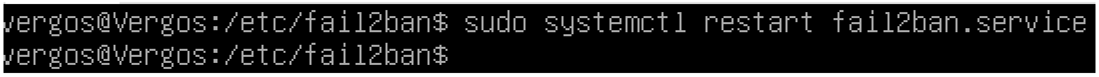
Τσεκάρω την κατάσταση του jail:



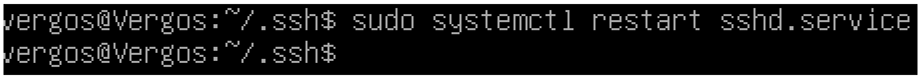
```
vergos@Vergos:/etc/fail2ban$ sudo fail2ban-client status joomla
Status for the jail: joomla
|- Filter
|  |- Currently failed: 0
|  |- Total failed:     0
|  `- File list:        /var/log/joomla_error.log
`- Actions
   |- Currently banned: 0
   |- Total banned:     0
   `- Banned IP list:
```

<u>Σημείωση</u> για τις ασκήσεις 1 και 2:

Μετά από οποιαδήποτε αλλαγή στα αρχεία jail.local και sshd_config για να λειτουργήσουν οι αλλαγές τρέχω τις ακόλουθες εντολές:



```
vergos@Vergos:/etc/fail2ban$ sudo systemctl restart fail2ban.service
vergos@Vergos:/etc/fail2ban$
```



```
vergos@Vergos:~/.ssh$ sudo systemctl restart sshd.service
vergos@Vergos:~/.ssh$
```