#

# This file controls the configuration of the audit daemon

# Configured according to CIS Benchmark

#

log\_file = /var/log/audit/audit.log

log\_format = RAW

log\_group = root

priority\_boost = 4

flush = INCREMENTAL

freq = 20

num\_logs = 5

disp\_qos = lossy

dispatcher = /sbin/audispd

name\_format = NONE

##name = mydomain

max\_log\_file = 6

max\_log\_file\_action = keep\_logs

space\_left = 75

space\_left\_action = email

action\_mail\_acct = root

admin\_space\_left = 50

admin\_space\_left\_action = halt

disk\_full\_action = SUSPEND

disk\_error\_action = SUSPEND

##tcp\_listen\_port =

tcp\_listen\_queue = 5

tcp\_max\_per\_addr = 1

##tcp\_client\_ports = 1024-65535

tcp\_client\_max\_idle = 0

enable\_krb5 = no

krb5\_principal = auditd

##krb5\_key\_file = /etc/audit/audit.key