Full credit is given to the above companies including the OS that this PDF file was generated!

Rocky Enterprise Linux 9.2 Manual Pages on command 'augenrules.8'

$ man augenrules.8

AUGENRULES(8) System Administration Utilities AUGENRULES(8)

NAME

augenrules - a script that merges component audit rule files

SYNOPSIS

augenrules [--check] [--load]

DESCRIPTION

augenrules is a script that merges all component audit rules files, found in the audit rules directory, /etc/audit/rules.d, placing the merged file in /etc/audit/audit.rules. Component audit rule files, must end in .rules in order to be processed. All other files in /etc/au?dit/rules.d are ignored.

The files are concatenated in order, based on their natural sort (see -v option of ls(1)) and stripped of empty and comment (#) lines.

The last processed -D directive without an option, if present, is al?ways emitted as the first line in the resultant file. Those with an op?tion are replicated in place. The last processed -b directive, if present, is always emitted as the second line in the resultant file. The last processed -f directive, if present, is always emitted as the third line in the resultant file. The last processed -e directive, if present, is always emitted as the last line in the resultant file.

The generated file is only copied to /etc/audit/audit.rules, if it dif?fers.

OPTIONS

--check

test if rules have changed and need updating without overwriting audit.rules.

--load load old or newly built rules into the kernel.

FILES

/etc/audit/rules.d/ /etc/audit/audit.rules

SEE ALSO

audit.rules(7), auditctl(8), auditd(8).

Red Hat Apr 2013 AUGENRULES(8)