
augenrules

Script qui fusionne les fichiers de règle d'audit

augenrules est un script qui fusionne tous les composants de règle d'audit dans `/etc/audit/rules.d` dans un fichier `/etc/audit/audit.rules`. Les fichiers de règle doivent se terminer par `.rules` pour être traités. Les fichiers sont concaténés dans l'ordre. Le fichier généré est copié dans `/etc/audit/audit.rules` seulement s'il diffère.

- La dernière directive `-D` traitée sans option, si présente, est toujours émise comme première ligne du fichier résultant.
- La dernière directive `-h` traitée, si présente, est toujours émise comme seconde ligne du fichier résultant.
- La dernière directive `-f` traitée, si présente, est toujours émise comme 3ème ligne
- La dernière directive `-e` traitée, si présente, est toujours émise comme dernière ligne.

OPTIONS

- check** Teste si les règles ont changées et doivent être mises à jours sans écrases les règles d'audit
- load** Charge les anciennes et les nouvelles règles dans le kernel