aureport

Outil de rapports des logs d'audit

aureport produit un sommaire des logs d'audit système.

OPTIONS

-au, –auth Affiche les tentative d'authentification

-a, –avc Affiche les messages avc

–comm afficher les commandes lancées

-cr, –crypto Affiche les évènements crypto

-f, –file Affiche les fichiers et sockets af_unix

–failed Ne sélectionne que les évènements échoués.

-h, –host Afficher les hôtes

-i, –interpret Interprète les entités numérique en texte.

-if, –input file | directory Utilise le fichier donné au lieu des logs

–input-logs Utilise l'emplacement des logs depuis auditd.conf comme entrées.

–integrité Affiche les évènements d'intégrité

-k, –key Affiche les clés des règles d'audit

-l, –login Affiche les logins

-m, –mods Affche les modifications de compte

-ma, –mac Affiche les évènements MAC

-n, –anomaly Affiche les évènement anormaux

–node node-name Ne sélectionne que les évènements venant du nœud spécifié

-nc, –no-config N'inclus pas les évènements CONFIG_CHANGE

-p, –pid Affiche les processus

-r, –response AFfiche les réponse aux évènements anormaux

-s, –syscall Affiche les syscall

–success Affiche seulement les évènements réussis

–summary Lance un sommaire qui donne un total des éléments du rapport principal

-t, –log Affiche un rapport du début et fin pour chaque log

–tty AFfiche les touches tty

-te, –end [end-date] [end-time] Recherche les évènement avant cette date/heure. mots clés permis : now, recent, today, yesterday, this-week, wwek-ago, this-month, this-year.

-tm, –terminal Affiche les terminaux

-ts, –start [start-date] [start-time] Affiche les évènements après cette date/heure. Les mots clé de -te sont permis.

-u, –user Affiche les utilisateurs

–virt Affiche les évènement de virtualisation

-x, –executable Affiche les exécutables