ausearch

Outil de requête de logs d'audit

OPTIONS

-a, –event audit-event-id Recherche un évènement basé sur l'id doné. Les messages commencent toujours par msg=audit(1116360555.329 :2401771, l'id étant le nombre après le ' :'.

–arch CPU Recherche les évènements basé sur une architecture CPU.

-c, –comm comm-name Recherche un évènement basé sur le nom de l'exécutable.

–debug Affiche les évènements mal-formés sur stderr

–checkpoint checkpoint-file checkpoint la sortie entre les invocation successive de ausearch de manière à ce que seuls les évènements qui n'ont pas été sortie sont affichés dans les invocations suivantes

-e, –exit exit-code-or-errno Recherche un évènement basé sur le code de sortie syscall donné

-f, –file filename Recherche un évènement basé sur le nom de fichier donné, ou socket af_unix

-ga, –gid-all all-group-id Recherche en évènement avec le gid ou gid effectif spécifié

-ge, –gid-effective effective-group-id Recherche en évènement avec le gid effectif spécifié

-gi, –gid group-id Recherche en évènement avec le gid spécifié

-hn, –host hostname Recherche en évènement avec le nom d'hôte spécifié

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

-if, –input filename | directory Utilise le fichier ou répertoire au lieu des logs

–input-logs Utilise l'emplacement des logs spécifié dans auditd.conf pour la recherche

–just-one Stop une fois le première évènement correspondant trouvé

-k, –key key-string Recherche en évènement basé sur la clé donnée

-l, –line-buffered Vide la sortie sur chaque ligne.

-m, –message message-type | comma-sep-message-type-list Recherche un évènement correspondant au type de message spécifié.

-n, –node node-name Recherche les évènements venant du ou des nœuds spécifiés.

-o, –object SE-Linux-context-string Recherche des évènements venant avec le tcontext donné

-p, –pid process-id Recherche un évènement avec le PID de processus donné

-pp, –ppid parent-process-id Recherche un évènement ayant le PID de processus parent donné

-r, –raw Sortie non formatée

-sc, –syscall syscall-name-or-value Recherche un évènement correspondant au syscall donné

-se, –context SE-Linux-context-string Recherche un évènement avec les scontext ou tcontext donné

–session Login-Session-ID Recherche un évènement avec l'ID de session donné

-su, –subject SE-Linux-context-string Recherche un évènement avec le scontext donné

-sv, –success success-value Recherche un évènement avec la valeur de succès donné (yes ou no)

-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.

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

-tm, –terminal terminal Recherche un évènement correspondant à la valeur terminal donnée

-ua, –uid-all all-user-id Recherche un évènement avec l'UID ou UID effectif donné

-ue, –uid-effective effective-user-id Recherche un évènement avec l'UID effectif donné

-ui, –uid user-id Recherche un évènement avec l'UID donné

-ul, –loginuid login-id Recherche un évènement avec le login id donné

-uu, –uuid guest-uuid Recherche un évènement avec l'uuid invité donné

-vm, –vm-name guest-name Recherche un évènement avec le nom de l'invité donné

-w, –word Chaîne de recherche à matcher

-x, –executable executable Recherche un évènement correspondant à l'exécutable donné

Codes de sortie

0 succès

1 Rien n'est trouvé, erreur d'argument, erreur d'accès fichier mineur

10 données checkpoint invalide

11 Erreur de traitement de checkpoint

12 Évènement checkpoint non trouvé dans le fichier de log