ausearch-expression

Format d'expression de recherche d'audit

Structure lexicale

Les espaces blancs sont ignorés. Les éléments suivants sont reconnus :

Ponctuation
**( ) **
opérateurs logiques
! && ||
Opérateurs de comparaison
< <= == > >= !== i= i != r= r !=
expressions régulières

Syntaxe

field comparison-operator value

field est une chaîne qui spécifie le premier champ avec ce nom dans l'enregistrement, ou \ suivi d'une chaîne, qui spécifie un champ virtuel avec le nom spécifié.

operator Spécifie la comparaison à effectuer

r= r != chaîne brute du champ (tel que stocké), et la compare à la valeur.

i= i != Chaîne interprétée du champs

< <= == > >= !== Opérateurs d'évaluation

\regexp string-or-regexp Dans ce cas spécial, l'enregistrement d'audit est pris comme une chaîne, et matché avec regexp-or-string, qui est une expression régulière étendue,.

Si E1 et E2 sont des expressions valides, alors ! E1, E1 && E2, et E1 || E2 sont des expressions valides également. Noter que ! field op value est interprétée comme !(field op value), et non pas (!field) op value.

Champs virtuels

\timestamp Valeur d'horodatage de l'évènement courant. Value doit avoir le format ts :<seconds>.<milli>.

\record_type La valeur est le type d'enregistrement courant.