sudoreplay

Rejouer les logs de session sudo

sudoreplay rejout ou liste les logs créés par sudo. Il peut jouer les sessions en temps réel, ou en ajustant la vitesse.

L'ID doivrait être une séquence à 6 chiffres et lettres majuscules, ou un motif matchant l'option iolog_file. Quand une commande est lancée via sudo avec log_output activée dans le fichier sudoers, la chaîne TSID=ID est loggée via syslog ou dans le fichier de log. L'ID peut également être déterminé en mode list.

En mode list, sudoreplay peut être utilisé pour trouver un ID de session basé sur des critères tels que l'utilisateur, le tty ou la commande lancée :

\n, \r Saute au prochain évènement, utile pour les longues pauses

' ' Met en pause la sortie, appuyer un n'importe quelle touche pour relancer

< Réduit la vitesse par 2

> Double la vitesse

OPTIONS

-d, –directory=dir Répertoire des logs de session au lieu du défaut /var/log/sudo-io

-f, –filter=[stdin|stdout,stderr,ttyin,ttyout] Sélection quels types E/S afficher.

-l, –list [expr] Active le mode liste. Dans ce mode, sudoreplay liste les sessions disponibles dans un format similaire au format de log sudo, trié par nom de fichier ou séquence de nombre. Si une expression de recherche est spécifiée, restreint les ID qui sont affichés. Une expression est composée des prédicats suivants :

command <pattern> Évalue à vrai si la commande match le motif spécifié

cwd <dir> Évalue à vrai si la commande a été lancée dans le répertoire spécifié

fromdate <date> Évalue à vrai si la commande a été lancée à ou après cette date

group <runas_group> Évalue à vrai si la commande a été lancée sous le groupe spécifié

runas <runas_user> Évalue à vrai si la commande a été lancée sous l'utilisateur spécifié

todate <date> Évalue à vrai si la commande a été lancée avant la date spécifiée

tty <tty> Évalue à vrai si la commande a été lancée dans le terminal spécifié

user <user> Évalue à vrai si la commande a été lancée par l'utilisateur spécifié

Les prédicats peuvent être combinées en utilisant les opérateurs and, or et !, ainsi que les parenthèses.

-m, –max-wait Spécifie une limite maximum d'attente entre les frappes de touche ou la sortie de données.

-s, –speed Spécifie le facteur de vitesse.

Format de date

La date et l'heure peuvent être spécifié de plusieurs manières : HH :MM :SS am MM/DD/CCYY timezone, HH :MM :SS am Month, Day Year timezone, CCYY-MM-DD HH :MM :SS, DD Month CCYY HH :MM :SS

Les dates suivantes sont valides :

now

tomorrow

yesterday il y a 24 heure

2 hours ago

next Friday

last week

a fortnight ago L'heure courante, mais il y a 14 jours

10 :01 am 9/17/2009

10 :01 am

10 10 heure du matin

9/17/2009

10 :01 am Sep 17, 2009

Exemples

Lister les sessions lancées par millert
sudoreplay -l user millert
Lister les sessions lancées par bob avec une commande contenant la chaîne vi
sudoreplay -l user bob command vi
Lister les sessions lancées par jeff qui match l'expression régulière
sudoreplay -l user jeff command '/bin/[a-z]*sh'
Lister les sessions lancées par jeff ou bob dans la console
sudoreplay -l (user jeff or user bob) tty console