auditd.conf

Fichier de configuration du service d'audit

local_events (bool) Spécifie si les évènements locaux sont inclus. Défaut : yes.

log_file Spécifie le chemin complet du fichier de log où les enregistrements d'audit sont stockés

write_logs [bool) Détermine si les logs sont stockés sur disque. Défaut : yes.

log_format Format des logs stockés sur disque : raw et enriched. enriched résoud les uid, gid, syscall, architecture, et adresse socket.

log_group Spécifie le groupe du fichier de log. Défaut : root

priority_boost Nombre non-négatif qui indique la priorité. Défaut 4.

flush none ne fait rien de spécial pour vides les enregistrements sur disque. incremental utilise freq pour déterminer la fréquence, incremental_async est similaire, mais de manière asynchrone pour de meilleurs performances. data conserve les données du disque synchronisés en permanence. sync conserve les données et les métadonnées pleinement synchronisés. Défaut : incremental_async

freq Nombre non-négatif indiquant le nombre d'enregistrement à écrire avant de les vider sur disque.

num_lgos Spécifie le nombre de fichiers de logs à conserver. < 2, la rotation de logs n'est pas effectuée. Doit être inférieur à 1000.

disp_qos Contrôle si la communication est bloquante/sans perte ou non-bloquante/avec perte entre auditd et le dispatcher. Il y a un tampon de 128K entre les 2, ce qui est suffisant dans la plupart des cas. (lossy ou lossless). Défaut : lossy

dispatcher Spécifie le dispatcher.

name_format Contrôle comment insérer les noms de nœud dans le flux d'évènements d'audit. none, hostname, fqd, numeric, et user. Défaut : none

name Nom à utiliser lorsque name_format = user

max_log_file Spécifie la taille max des fichiers de log. Une fois cette limite atteinte, il déclence une action de configuration

max_log_file_action Indique au système quelle action prendre quand le système a détecté que la limite de taille du fichier de log est atteinte.

action_mail_acct Adresse email ou alias. /usr/lib/sendmail doit exister dans la machine

space_left Valeur numérique, en Mo, indiquant quand effectuer une action lorsque l'espace disque vient à manquer

space_left_action Indique quelle action prendre quand l'espace disque restant est inférieur à space_left. (ignore, syslog, rotate, email, exec, suspend, single, ou halt)

admin_space_left Identique à space_left. Est considéré comme la dernière change de faire quelque chose avant de ne plus avoir d'espace disque.

admin_space_left_action Indique quelle action prendre quand l'espace disque restant est inférieur à admin_space_left

disk_full_action Indique quelle action prendre quand le système a détecté que la partition qui maintient les logs est pleine. (ignore, syslog, rotate, exec, suspend, single, et halt)

disk_error_action Indique quelle action prendre quand une erreur disque est détectée en écrivant des évènements d'audit sur disque.

tcp_listen_port Port tpc d'écoute des enregistrements d'audit des systèmes distants.

tcp_listen_queue Valeur numérique qui indique combien de connexions en cours sont permises. Défaut : 5

tcp_max_per_addr Valeur numérique indiquant combien de connection concurrentes de la même IP sont permises. Défaut : 1 (max 1024)

use_libwrap (bool) Utilise tcp_wrappers pour définir les machines autorisées à se connecter

tcp_client_ports 1 ou 2 valeurs numérique. Indique les ports clients permis pour les connexions entrante. Spécifier 1-1023 pour autoriser les port privilégiés

tcp_client_max_idle Délai en secondes d'inactivité d'un client avant que la connexion soit terminées. Défaut : 0 = désactive la vérification

enable_krb5 (bool) Utilise kerberos pour l'authentification et le chiffrement

krb5_principal Principal du serveur. Défaut : auditd.

krb5_key_file Emplacement de la clé du principal du client. Cette clé doit être possédée par root, en mode 0400. Défaut : /etc/audit/audit.key

distribute_network (bool) À yes, les évènements provenant du réseau sont distribués au dispatcher pour traitement. Défaut : no

Notes

- Dans un environneent CAPP, Le chemin d'audit est si important que l'accès aux ressources système doit être refusé si un chemin d'audit ne peut être créé. Dans cet environnement, il est suggéré que /var/log/audit soit dans sa propre partition.
- Le paramètre flush devrait être sync ou data
- space_left doit être être une valeur qui donne suffisamment de temps à un administrateur de réagir et de récupérer de l'espace disque. Cela peut impliquer aureport -t et le déplacement des anciens logs. Il est recommandé que space_left_action soit email.
- admin_space_left doit être l'espace disque nécessaire pour les actions administratives à enregistrer.
- disk_full_action est déclenchée quand il n'y a plus de place. Tous les accès devraient être terminés vu qu'il n'y a plus de capacité d'audit. Peut être définis à single ou halt
- disk_error_action devrait être syslog, sigle ou halt en fonction de la stratégie locale
- Spécifie ue seul port client permis peut poser problème pour le client souhaitant redémarrer le sous-système d'audit, vu qu'il n'est pas capable de recréer une connexion avec les même adresses d'hôte et ports tant que la connection est à l'état TIME_WAIT.