auditctl

Utilitaire de contrôle du système d'audit Linux

Options de configuration

-b backlog Définis le nombre max de tampon d'audit permit (défaut : 64). Si tous les tampons sont pleins, le flag d'erreur est consulté par le kernel.

–backlog_wait_time wait_time Définis de temps (défault : 60*Hz) que le kernel attend lorsque backlog_limit est atteind avant de mettre plus d'évènements d'audit en queue à transférer à auditd. Doit être supérieur ou égal à 0 et inférieur à 10 fois la valeur par défaut.

-c Continue à charger les règles malgré les erreurs. Génère un sommaire du résultat du chargement des règles

-D Supprime toutes les règles et watchs

-e [0..2] Définis le flag enable. 0 = désactivé, 1 = activé, 2 = bloqué en l'état actuel.

-f [0..2] Défpinis le mode failure. 0 = silencieux, 1 = printk, 2 = panic. Permet de déterminer comment le kernel gère les erreurs critiques.

-i Ignore les erreurs en lisant les règles depuis un fichier.

–loginuid-immutable Rend les loginuid inchangeables une fois définis.

-q mount-point.subtree Si vous avez un watch répertoire existant, et un montage déplacé ou bindé ailleurs dans le subtree rechargé, il faut indiquer au kernel que le subtree mounté est équivalent au répertoire regardé. Si le subtree est déjà monté au moment où le watch est émis, le subtree est automatiquement taggé pour surveilance.

-r rate Définis la limite des message par seconde. (0=pas de limite). Si ce taux est atteind, le flag failure est consulté

-R file Lit les règles dans un fichier.

-t Déclence les subtrees après une commande mount

Options de status

-l Liste toutes les règles, 1 par ligne. 2+ options peuvent être passées à cette commande. -k liste les règles qui matche une clé, ou -i pour interpreter a0 à a3 pour aider à déterminer les valeurs d'argument syscall.

-m text Envoie un message userspace dans le système d'audit. Ne peut être fait qu'avec la capability CAP_AUDIT_WRITE.

-s Reporte le status du sous-système d'audit

Options de règle

-a [list,action|action,list] Ajoute une règle à la fin de la liste avec l'action spécifié. Les champs peuvent être dans n'importe quel ordre. Les noms de liste valides, puis d'actions sont :

task Ajoute une règle à la liste par tâche. Utilisée seulement quand une tâche est créée (fork() ou clone())

exit Ajoute une règle à la liste de sortie syscall. Utilisée à la sortie d'un appel système pour déterminer si un évènement d'audit devrait être créé

user Ajoute une règle à a liste de filtre de message utilisateur. Utilisé par le kernel pour filtrer les évènements venant du userspace avant de les relayer à service d'audit.

exclude Ajoute une règle à la liste de filtre d'exclusion de type d'évènement. Cette liste est utilisée pour filtrer les évènement que l'on ne veut pas voir.

never Aucun enregistrement d'audit n'est généré.

always Alloue un contexte d'audit.

-A list,action Ajoute une règle au début de la liste

-C [f=f | f!=f] Construit une règle de comparaison inter-champ. Peut être spécifié plusieurs fois. Les 2 opérateurs supportés sont equel et not equal. Les champs valides sont : auid, uid, euid, suid, fsuid, obj_uid ; and gid, egid, sgid, fsgid, obj_gid

-d list,action Supprime une règle de la liste. La règle est supprimée seulement si les noms syscall matchent exactement.

-F [n=v | n!=v | n<v | n>v | n<=v | n>=v | n&v | n&=v] Construit un champs de règle : nom, opération, valeur. Peut être spécifié jusqu'à 64 fois. Chaque équation est combinée l'une avec l'autre pour déclencher un enregistrement d'audit. Il y a 8 opérateurs supportés : égal, non égal, inférieur à, supérieur à, inférieur ou égal à, supérieur ou égal à, mask de bit ou test de bit. Les champs qui prennent un uid peuvent utiliser le nom de l'utilisateur. Les champs valides sont :

a0, a1, a2, a3 Les 4 arguments d'un syscall. Noter que les arguments chaîne ne sont pas supportés.

arch Architecture CPU du syscall (uname -m)

auid ID original de l'utilisateur. raccourci de audit uid, parfois appelé loginuid

devmajor Numéro majeur de périphérique

devminor Numéro mineur de périphérique

dir Chemin complet d'un répertoire à regarder

egid gid effectif

euid uid effectif

exe Chemin absolu de l'application à laquelle cette règle s'applique. Uniquement dans une liste exit

exit Valeur de sortie d'un syscall

fsgid GID du système de fichier.

fsuid UID du système de fichier

filetype Type du fichier cible (file, dir, socket, link, character, block, ou fifo)

gid id du groupe

inode Numéro d'inode

key Autre manière de définir une clé filtre. voir -k

msgtype Utiliser pour matcher le type d'enregistrement de l'évènement. devrait être utilisé dans les listes d'exclusion ou utilisateur

obj_uid UID de l'objet

obj_gid GID de l'objet

obj_user Utilisateur SELinux de la ressource

obj_role Type SELinux de la ressource

obj_type Type SELinux de la ressource

obj_lev_low niveau inférieur SELinux de la ressource

obj_lev_high Niveau supérieur SELinux de la ressource

path Chemin complet du fichier à regarder. Ne peut être utiliser que dans la liste exit

perm Filtre de permissions pour les opérations de fichier. Voir -p Uniquement dans la liste exit

pers Numéro de personnalité OS

pid ID de processus

ppid ID du processus parent

subj_user Utilisateur SELinux du programme

subj_role role SELinux du programme

subj_type Type SELinux du programme

subj_sen Sensibilité SELinux du programme

subj_clr Autorisation SELinux du programme

sgid gid sauvé.

success Si la valeur de sortie est >=0, c'est true/yes (1), sinon false/no (0)

suid UID sauvé

uid id de l'utilisateur

-k key Définis une clé filtre dans une règle d'audite. C'est une chaîne arbitraire (max 31 octets) qui peut identifier de manière unique les enregistrements d'audit produits par une règle. Peut être spécifié plusieurs fois

-p [r|w|x|a] Décrit les types d'accès sur lesquels se déclence un watch de système de fichier.

-S [Syscall name or number|all] Si le syscall doné est fait par un programme, démarre un enregistrement d'audit. Peut être spécifié plusieurs fois

-w path Insert un watch pour un objet système de fichier au chemin spécifié.

-W path Suppmire un watch pour l'objet système de fichier.

Performances

Les règles syscall sont évaluées pour chaque syscall pour chaque programme. Avec 10 règles syscall, chaque programe dans le système est retardé durant un syscall jusqu'à ce que le système d'audit évalu chaque règle, ce qui peut impacter fortement les performances. Tenter de combiner autant de filtre, action, clé, et champs que possible sont identiques. Par exemple :
auditctl -a always,exit -S openat -F success=0
auditctl -a always,exit -S truncate -F success=0
peuvent être reécris en une seule règle :
auditctl -a always,exit -S openat -S truncate -F success=0
Également, tenter d'utiliser l'audit de système de fichier améliore les performances. Par exemple, pour capturer toutes les ouvertures échouées, mais seulement les fichiers dans /etc :
auditctl -a always,exit -S openat -S truncate -F dir=/etc -F success=0
Cela améliore les performances vu que le kernel n'évalue pas chaque syscall. C'est géré par le code d'audit de système de fichier.

Exemples

Voir tous les syscalls faits par un programme spécifique
auditctl -a always,exit -S all -F pid=1005
Vois les fichiers ouverts par un utilisateur spécifique
auditctl -a always,exit -S openat -F auid=510
Voir les appels openat échoués
auditctl -a always,exit -S openat -F success=0
Regarder les changements d'un fichier (2 manières exprimées)
auditctl -w /etc/shadow -p wa
auditctl -a always,exit -F path=/etc/shadow -F perm=wa
Regarder les changements, récursivement dans un répertoire (2 manières exprimées)
auditctl -w /etc/ -p wa
auditctl -a always,exit -F dir=/etc/ -F perm=wa
Voir si un admin accède aux fichier des autres utilisateurs :
auditctl -a always,exit -F dir=/home/ -F uid=0 -C auid!=obj_uid