



L'Audit et le contrôle au sein du mainframe IBM zAudit

Consul zAudit est l'outil d'audit d'état et d'audit événementiel pour un mainframe IBM avec RACF. Consul zAudit effectue l'analyse complète de l'intégrité du système ainsi que celle des événements de la sécurité. Il met en évidence les événements critiques et identifie les risques potentiels.

Les apports

- **Des rapports adaptables**
Vous ne recevrez ainsi que les informations pertinentes à vos yeux.
- **Des audits d'état et des analyses des événements**

Consul zAudit vous fournit les analyses de l'état de la sécurité du système ainsi que les analyses événementielles basées sur les journaux SMF (actifs ou archivés). Vous identifiez mieux les vides de sécurité et les risques encourus.

- **Réduit les coûts**
Il n'est pas besoin d'être un expert pour tirer profit de Consul InSight™ zAudit..

```
Trusted userids (may bypass security)          14 s elapsed, 7.9 s CPU
                                                18 Jan 2002 15:07

Pri Complex Trusted userids
10 DINO 1
Pri Reasons Userid Name RIP DfltGrp InstData
10 356 CRMAR02 ROB VAN HOBOKEN SYSPROG
Pri Cnt Audit concern
== 10 1 Can use Trojan attacks via the .profile of trusted user OHVS
== 10 1 Can use Trojan attacks via the .profile of trusted user CRMAR0B
== 10 1 Can use Trojan attacks via the homedirectory of trusted user CRMAR0B
== 10 4 Can submit jobs for trusted user
== 9 1 Can make HFS file APF-authorized, APF program can bypass security
== 9 1 User privileges and rules may be changed directly on disk
== 9 3 Security-relevant parameters may be changed
== 9 11 JCL that runs with high authority may be changed
== 9 72 May change APF program that can bypass security
== 8 1 Can alter the RMM control data set, thus gaining access to any tape.
== 8 1 Can change userid with set(re)uid or spawn
== 8 1 Can change APF program and hence bypass security
== 8 1 Superuser authority, can do anything in USS
== 7 4 May mark jobs as propagated from any user
== 6 1 Can dump all data sets, gaining access
== 6 1 Can dump and delete all data sets, gaining access
Command ==> Scroll==> CSB
HR a 24/015
Connected to remote server
```

Analyse simple

- Analyse automatique
- L'identification des changements portent sur la sécurité générale permet d'intervenir avant un éventuel problème qui en résulterait.
- Analyse de l'impact d'un changement sur le paramétrage
- "Trust analysis" pour comprendre quels identifiants ont un accès privilège à quelles ressources : par quel moyen et pourquoi.

Expertise

- zAudit apporte une expertise sur les derniers niveaux de zOS et les risques associés
- Un seul interface, un seul langage
- Expertise basée sur les vrais moyens de s'introduire dans un mainframe

Nombreux rapports simples et rapides à obtenir

- Affichages et rapports instantanés portant sur RACF, ACF2, SMF, z/OS et USS
- Analyse des tendances basée sur SMF
- Adaptation facile des états
- Distribution des états par Email

Consul zAudit RACF

zAudit analyse l'état général de la sécurité du système z/OS (identification des fichiers sensibles et de leurs protections, identification des programmes et SVC potentiellement dangereux etc... Présentation de rapports décrivant les failles par ordre d'importance.

Consul zAudit RACF s'appuie à la fois sur RACF et sur SMF, les exceptions sont isolées du reste et les rapports peuvent être présentés à la personne responsable d'un événement et pas seulement à l'administrateur.

zAudit a la faculté d'envoyer ses rapports par message électronique à un destinataire ou une liste de destinataires lorsqu'un incident survient. Le contrôle de la sécurité du mainframe, la détection de événements anormaux et la corrections des erreurs de définitions peuvent être réalisés par une même procédure.

zAudit RACF apporte également aux administrateurs la possibilité de contrôler simplement les définitions et d'identifier les problèmes dans Unix System Services.

Une fois collectées, les informations peuvent être mises en forme dans Consul zAudit RACF ou bien transférées vers Consul InSight™ pour être consultées avec celles des autres environnements.

Etic Software

28, rue de Voisins - 78430 - Louveciennes - Tel : 01 39 69 17 17 - Télécopie : 01 39 69 17 13 13
Email : sales@eticsoftware.com - support technique : support@eticsoftware.com - Web : www.eticsoftware.com