cilasoft

COMBATTRE LA FRAUDE
& VOUS METTRE EN CONFORMITÉ
AVEC LES RÈGLEMENTATIONS

EAM

LA SOLUTION D'ÉLÉVATION DE DROITS SUR IBM i

En permettant **d'augmenter temporairement les droits** d'un profil utilisateur en cas de besoin, EAM concourt à la **réduction du nombre de profils utilisateurs puissants** (*ALLOBJ, *SECADM, accès à la ligne de commande, etc.) sur un serveur IBM i. Enfin, l'activité des profils sous élévation de droits est loguée de façon à produire une **piste d'audit complète.**

EAM fournit au management la possibilité de contrôler l'activité des utilisateurs sur le serveur et donc de répondre aux exigences les plus contraignantes des règlementations telles que SOX, Bâle II, PCI-DSS, HIPAA, etc.

DESCRIPTION

Sous le contrôle total du responsable sécurité, EAM permet à des utilisateurs identifiés d'acquérir temporairement des droits supplémentaires, automatiquement ou à la demande. Ces droits peuvent être limités à une commande donnée, certains jours à certaines heures, à certaines adresses IP ou à d'autres paramètres.

Au-delà d'un mécanisme d'attribution de droits à la fois souple et rigoureux, EAM fournit également un outil de surveillance et de reporting complet des demandes et de l'utilisation des droits supplémentaires.
A partir des captures d'écran, de la joblog, des points d'exit et des journaux système et base de données, EAM récupère et logue intégralement l'activité de l'utilisateur, permettant ainsi un audit complet.

EAM propose différentes méthodes d'attribution de droits :

* *SWAP : l'utilisateur du job est permuté vers le profil cible et hérite de ses droits
* *ADOPT : l'utilisateur adopte les droits du profil cible
* *LOG : toute l'activité de l'utilisateur est loguée – les droits ne sont pas modifiés

Advanced Business Partner IBM

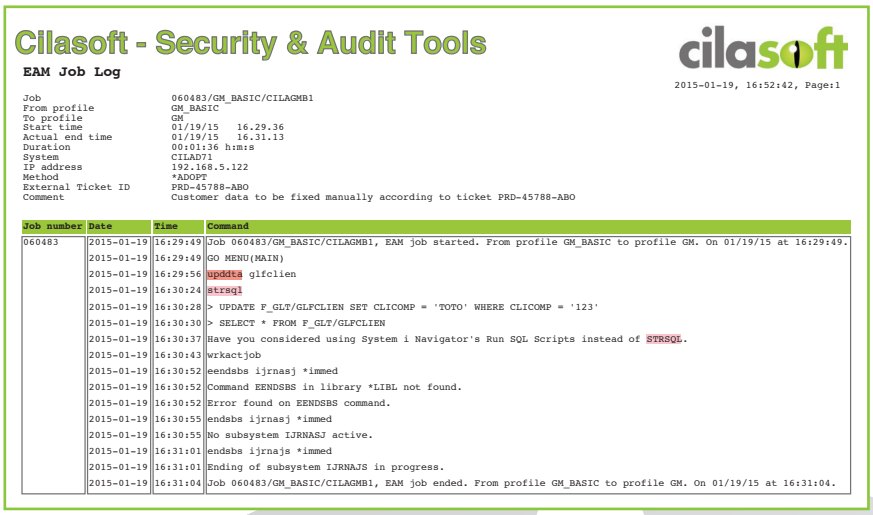
SOUPLE ET PERFORMANT

Avec **EAM**, vous pouvez par exemple :

* Autoriser la modification des valeurs système ou des attributs d'un profil sans attribuer le droit spécial *SECADM de façon permanente
* Permettre à un utilisateur d'hériter du droit spécial *AUDIT uniquement quand cela est nécessaire
* Fournir les droits nécessaires sur les données uniquement en cas de besoin pour modifier des fichiers de production (par DFU, STRSQL, ODBC, etc.)
* Loguer automatiquement l'activité de profils utilisateurs puissants
* Donner l'accès à la ligne de commande aux utilisateurs uniquement en cas de besoin

EAM

> “EAM s’adapte très facilement aux évolutions des besoins et exigences grâce à la souplesse de sa configuration et sa capacité à produire des rapports pertinents.”



Cilasoft - Security & Audit Tools

cilasoft

EAM Job Log

2015-01-19, 16:52:42, Page:1

Job	060483/GM_BASIC/CILAGMB1
From profile	GM_BASIC
To profile	GM
Start time	01/19/15 16.29.36
Actual end time	01/19/15 16.31.13
Duration	00:01:36 h:m:s
System	CILAD71
IP address	192.168.5.122
Method	*ADOPT
External Ticket ID	PRD-45788-ABO
Comment	Customer data to be fixed manually according to ticket PRD-45788-ABO

Job number	Date	Time	Command
060483	2015-01-19	16:29:49	Job 060483/GM_BASIC/CILAGMB1, EAM job started. From profile GM_BASIC to profile GM. On 01/19/15 at 16:29:49.
	2015-01-19	16:29:49	GO MENU(MAIN)
	2015-01-19	16:29:56	updata glfclien
	2015-01-19	16:30:24	strsql
	2015-01-19	16:30:28	> UPDATE F_GLT/GLFCLIEN SET CLICOMP = 'TOTO' WHERE CLICOMP = '123'
	2015-01-19	16:30:30	> SELECT * FROM F_GLT/GLFCLIEN
	2015-01-19	16:30:37	Have you considered using System i Navigator's Run SQL Scripts instead of STRSQL.
	2015-01-19	16:30:43	wrkactjob
	2015-01-19	16:30:52	eendsbs ijrnasj *immed
	2015-01-19	16:30:52	Command EENDSBS in library *LIBL not found.
	2015-01-19	16:30:52	Error found on EENDSBS command.
	2015-01-19	16:30:55	endsbs ijrnasj *immed
	2015-01-19	16:30:55	No subsystem IJRNASJ active.
	2015-01-19	16:31:01	endsbs ijrnajs *immed
	2015-01-19	16:31:01	Ending of subsystem IJRNAJS in progress.
	2015-01-19	16:31:04	Job 060483/GM_BASIC/CILAGMB1, EAM job ended. From profile GM_BASIC to profile GM. On 01/19/15 at 16:31:04.

ATOUTS

* Définition des règles d’autorisation indiquant la méthode (*SWAP, *ADOPT, *LOG) et le cadre d’utilisation (adresse IP, date et heure, travail, IASP, etc.)
* Définition des profils source et cible intégrant les profils de groupe, les groupes supplémentaires et des listes d’utilisateurs
* Mode urgence avec délégation de gestion des règles et piste d’audit complète
* Procédure de demande de droits simplifiée au maximum (valeurs par défaut, paramètres pré-remplis) et documentée
* Procédure d’acceptation des demandes de droits automatique ou manuelle
* Utilisation possible en mode 5250 ou en mode serveur pour les accès ODBC, JDBC, DRDA ou FTP
* Notification possible par e-mail, popup ou syslog pour les évènements EAM tels que démarrage, arrêt, temps autorisé dépassé, fin anormale d’une session
* Contrôle et/ou audit des commandes permettant de terminer inopinément une session EAM ou de masquer la joblog
* Contrôle de l’accès à la ligne de commande et de la soumission de travaux ; contrôle des travaux soumis
* Possibilité de réduire les droits d’un utilisateur si besoin
* Log de toutes les demandes et reporting avec des filtres adaptables
* Inclut les instructions SQL, les fonctions FTP et les commandes critiques dans la log de la session EAM
* Contrôle optionnel de ticket pour une interface avec une solution de HelpDesk
* Nombreux formats disponibles pour les rapports (PDF, XLS, CSV)
* Possibilité d’interface avec les principales consoles SIEM
* Et bien d’autres possibilités

VALEUR AJOUTÉE

* Satisfaire les utilisateurs demandeurs de droits par sa simplicité
* Satisfaire les responsables sécurité en réduisant le nombre de profils puissants
* Satisfaire les auditeurs par les possibilités d’alerte et de reporting
* Permettre la mise en place d’une véritable séparation des tâches
* Réduire significativement les erreurs humaines impactant la sécurité
* Restreindre l’accès aux données sensibles

cilasoft

www.cilasoft.com

Tél : +33 4 50 69 45 98 (EMEA)
Tél : +1 404 495 5912 (Amérique du Nord)

E-mail : sales@cilasoft.com

SUITE GLOBALE
D’AUDIT ET DE SÉCURITÉ SUR IBM i

QJRN/400
Audit système et base de données

CONTROLER
Contrôle d’accès

DVM
Audit des accès en lecture

CENTRAL
Consolidation et déploiement de données