



## Press Release

Contacts:

Guy Marmorat (France): +33 4 50 69 45 98

Bill Rice (USA): 801-521-0527

br@billricecommunications.com

### **Cilasoft lance Elevated Authority Manager sur IBM i**

*Cette nouvelle solution apporte une aide précieuse aux responsables informatiques désireux de gérer plus efficacement les utilisateurs disposant de droits élevés.*

Annecy, France, le 24 avril 2012 – Cilasoft, expert dans le domaine de la sécurité sur IBM i (AS/400) annonce le lancement de sa nouvelle solution baptisée « Elevated Authority Manager » (EAM) qui permet d'attribuer temporairement des droits supplémentaires à certains utilisateurs. EAM est de plus doté de fonctions de reporting et d'alertes très complètes permettant aux responsables informatiques de loguer toutes les actions effectuées par les utilisateurs durant les sessions où ils bénéficient de ces droits spéciaux.

EAM permet de réduire le nombre des profils puissants ayant en permanence des droits élevés et ainsi de mieux contrôler l'activité des utilisateurs dans l'environnement IBM i, enfin de mieux répondre aux exigences des réglementations, telles que, Sarbanes-Oxley (SOX), Payment Card Industry Data Security Standards (PCI-DSS), Health Insurance Portability and Accountability Act (HIPAA), etc. Grâce aux fonctionnalités de surveillance et de reporting, l'activité des utilisateurs est totalement auditée et loguée depuis différentes sources (joblog, journaux système et base de données, points d'exit).

Un utilisateur peut par exemple :

- Modifier des valeurs système sans pour autant avoir le droit spécial \*SECADM en permanence,
- Acquérir le droit spécial \*AUDIT uniquement quand il doit modifier les valeurs d'audit sur les objets sensibles,
- Obtenir les droits sur les données au moment où il doit les corriger dans les fichiers de production en utilisant DFU ou SQL

EAM propose deux méthodes d'attribution de droits pour une plus grande flexibilité : 1) SWAP : l'utilisateur acquiert des droits en permutant sur le profil cible – 2) ADOPT : l'utilisateur adopte les droits du profil cible - De plus, après sélection de la méthode, les responsables informatiques peuvent définir les règles sur la durée et/ou sur la commande spécifique autorisée.

Rocky Marquiss, Senior Programmer Analyst chez « Campbell County Government » à Gillette, Wyoming (USA) affirme : « – Nous avons remplacé un autre produit de Gestion des Droits par EAM car il propose plus de fonctionnalités de contrôle et d'audit. Nos utilisateurs avaient pour

*habitude de partager leurs identifiants quand ils avaient besoin de droits supplémentaires. Mais aujourd'hui, avec EAM intégré dans nos applications, si un utilisateur effectue un swap d'un profil, nous pouvons suivre qui a transféré les droits et savoir ce qu'il a effectué au cours de l'utilisation de ce profil. Ainsi, les utilisateurs savent désormais que leur activité est tracée ce qui évite certaines actions non souhaitables. » -*

### **Les bénéfices d'EAM:**

- Aide les administrateurs à répondre plus rapidement à des demandes de droits spécifiques
- Réduit le nombre d'utilisateurs puissants aux droits élevés
- Satisfait les auditeurs par les possibilités d'alertes et de reporting
- Fournit une meilleure séparation des tâches
- Réduit significativement les risques d'erreurs humaines
- Restreint l'accès aux données sensibles.

*« - Nous sommes ravis de renforcer la Suite de Sécurité Cilasoft avec Elevated Authority Manager. EAM est une solution qui se compose de fonctionnalités uniques et flexibles. Ce produit a déjà grandement séduit les utilisateurs de la plateforme IBM i. EAM apportera une aide considérable à tous nos clients souhaitant répondre plus efficacement à leurs exigences en matière de sécurité et de conformité », souligne Guy Marmorat, PDG de Cilasoft.*

### **PRINCIPALES FONCTIONNALITES :**

- Définition des règles avec sélection de la méthode (\*SWAP, \*ADOPT), de la durée, de la commande spécifique autorisée (ou de la ligne de commande), du contexte
- Mode urgence avec délégation de gestion des règles et avec piste d'audit
- La demande de droit est simplifiée au maximum
- Utilisation en mode 5250 et serveur (par exemple, une interface SQL externe telle que ODBC, JDBC pour modifier des données non accessibles autrement)
- Contrôle et/ou audit des commandes permettant de sortir inopinément de la session EAM ou de masquer l'historique du travail
- Alerte possible quand un évènement intervient (démarrage, arrêt, dépassement de durée, arrêt anormal, etc) via message 5250, e-mail, syslog, popup
- Règles sur les profils sources et cibles incluant les profils de groupe et groupes supplémentaires
- Les responsables informatiques peuvent réduire les droits ou les élever
- Gestion centralisée des travaux EAM
- Historique de toutes les demandes avec reporting
- Rapports personnalisables
- Configuration pré-définie et adaptable.

## **A propos de Cilasoft**

Cilasoft est leader dans les solutions logicielles d'audit, de compliance et de sécurité sur IBM i (AS/400). Les produits phares de sécurité, QJRN/400 et CONTROLLER, ont été initialement développés à la demande d'une direction générale d'une Administration suite à un audit du Fonds monétaire international. Après 10 ans de développement et d'utilisation sur le marché, les produits Cilasoft ont évolué en une Suite sophistiquée de solutions de sécurité, solutions qui sont à ce jour installées dans des entreprises dans plus de 60 pays. Cilasoft est certifié Advanced IBM Business Partner. Son siège social se situe au cœur des Alpes en France et ses produits sont commercialisés grâce à un large réseau de partenaires dans le monde. Pour plus d'information, visitez le site : [www.cilasoft.com](http://www.cilasoft.com)