

QJRN/400, LA BOITE NOIRE DE VOTRE System i



Vos données informatiques
sont votre patrimoine.
Pensez dès maintenant
à les protéger, les surveiller,
maîtriser leur évolution,
assurer leur confidentialité
et leur pertinence...

CONFORMITÉ

La réglementation internationale (SOX, HIPAA, BALE II, PCI, 21-CFR) impose aux sociétés de garantir la sécurité et l'intégrité de leurs données.

FRAUDE, SABOTAGE & DIVULGATION

Plus de 60% des actes de malveillance sont perpétrés par des éléments internes à l'entreprise.

Ils restent inexplicables dans la plupart des cas.

AUDIT INTERNE

Pour valider les procédures de contrôle interne réglementaires, les auditeurs demandent aujourd'hui la mise en place d'outils pour automatiser un processus d'audit continu.

SÉCURITÉ

Le contrôle de l'utilisation des profils « Officier de Sécurité » est une question récurrente à chaque audit.

Pouvoir limiter et auditer leurs interventions en production sans perturber les règles de sécurité existantes est un facteur important de réduction des risques.

La législation en matière de contrôle interne (Loi de Sécurité Financière, Sarbanes-Oxley, HIPAA, Bâle II, C-198, PCI, 21-CFR,...) se durcit et rend pénalement responsables les dirigeants et administrateurs des sociétés cotées et des organismes financiers, s'ils ne mettent pas en œuvre les moyens de sécuriser et d'auditer leur système d'informations. La responsabilité de la Direction Informatique peut également être mise en cause par délégation.

La suite QJRN/400 et CONTROLER met à votre disposition les solutions pour répondre à ces obligations.

Mise en œuvre complète en quelques jours !

QJRN/400, la solution d'audit sur IBM System i

AUDIT SYSTÈME

Ce module répond à toutes vos demandes d'audit en matière de sécurité, tentatives de connexion, gestion des valeurs système, bibliothèques et objets :

- Surveillance de profils sensibles (télémaintenance, prestataires)
- Audit des actions sur les fichiers spoules confidentiels...
- Interventions sur les profils, valeurs système, attributs de réseau, droits sur les objets sensibles
- Tentatives d'ouverture de session ou d'accès à des ressources non autorisées
- Suivi de l'activité hors heures ouvrables
- Contrôle d'intégrité des paramètres d'audit
- Contrôle des mises en production
- Accès à des objets sensibles (fichiers, options de menus)

AUDIT BASE DE DONNÉES

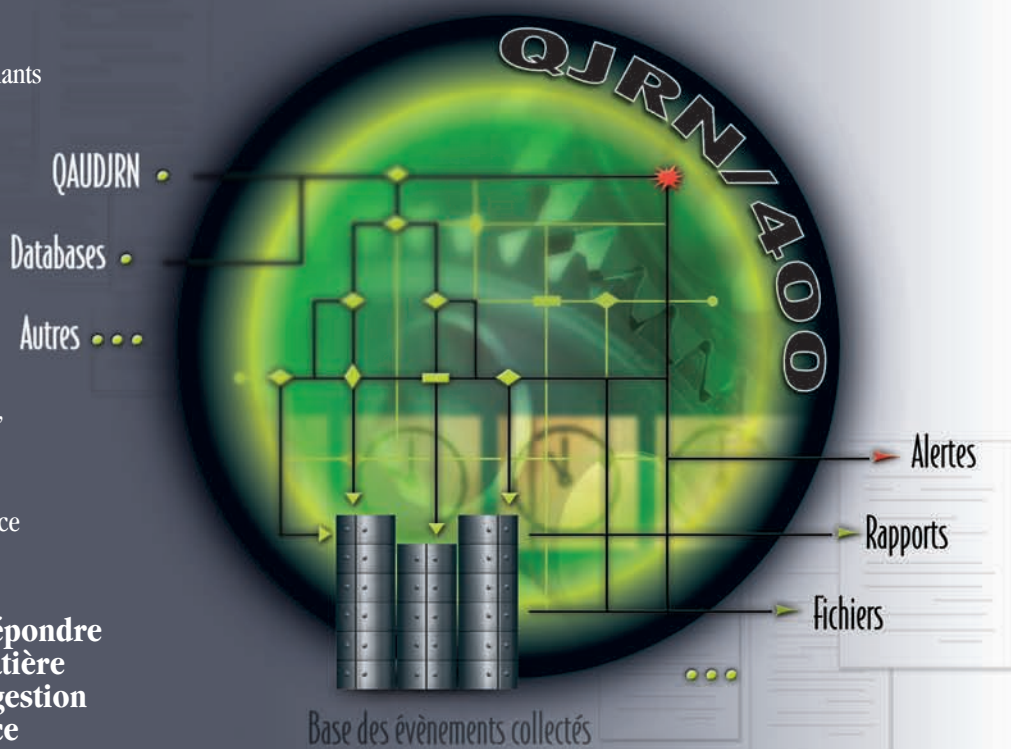
Ce module permet de générer des rapports détaillés sur toutes les modifications survenues dans vos données.

Vous pouvez facilement signaler et expliquer :

- Les interventions sur les habilitations
- Les modifications des données nominatives et confidentielles
- Les variations anormales des taux
- Les opérations sur des comptes dormants
- Les interventions sur les zones sensibles telles que RIB, conditions tarifaires, données nominatives, carte bancaire, plafond, limites de crédit...
- La détection de toutes les opérations effectuées hors application : DFU, SQL, upload Client Access, mais aussi par des programmes de type "bricolage" ou réputés d'utilisation dangereuse
- L'activité hors heures ouvrables
- Les modifications effectuées à distance sur les applications

QJRN/400 vous permet de répondre aux objectifs de COBIT en matière de contrôles de sécurité, de gestion des données et de surveillance des environnements de production.

Operateur	Date	Time	Job	User	Profile	Type	Statut	FCM	PROG	PER	ALL	JOB	SAV	SEC	SPR	STRY	AUD	SCN	Group
User Profile	05/01/2007	14:05:09	QPADEV004	ADMIN	ADMIN	CHG	ENABLED												
User Profile	05/01/2007	14:37:51	QPADEV004	ADMIN	CLASOFT	CRT	ENABLED	Y				Y							
User Profile	05/01/2007	15:01:33	QPADEV004	ADMIN	CLASOFT	CHG	ENABLED					Y							
User Profile	05/01/2007	15:10:19	SEC_CONSOL	ADMIN_JOE	USER_JOE	CHG	ENABLED												ADMIN_JOE
User Profile	05/01/2007	15:10:47	SEC_CONSOL	ADMIN_JOE	USER_JOE	CHG	ENABLED						Y	Y					Y
User Profile	05/01/2007	16:16:45	IT01001	ADMIN	QSEC_TMP	CRT	ENABLED			Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
User Profile	05/01/2007	16:30:08	IT01001	ADMIN	QSEC_TMP	CHG	DISABLED												
Delete	05/01/2007	16:47:22	IT01001	ADMIN	QSEC_TMP														



PRINCIPALES FONCTIONNALITÉS

Administration de la journalisation

Tous les journaux (système, base de données, défini par l'utilisateur) peuvent être déclarés et analysés par QJRN/400. Les journaux préexistants seront intégrés facilement. QJRN/400 prend aussi en charge la création d'environnements complets de journalisation et assure leur exploitation.

Chaque environnement possède son référentiel qui décrit les champs de toute la base de données journalisée. Ce référentiel est généré automatiquement, avec de nombreuses possibilités de personnalisation.

Parfaite compatibilité avec les logiciels de haute disponibilité

QJRN/400 cohabite parfaitement avec les principaux logiciels de haute disponibilité fonctionnant sur System i.

Gestionnaire de requêtes

Grâce à la conception originale et unique du système de requêtes, QJRN/400 analyse de manière très fine le contenu des journaux. La puissance des filtres permet de cibler de façon précise tout événement potentiellement frauduleux, tout accès aux informations sensibles. Grâce à ses possibilités de personnalisation, QJRN/400 restitue le contenu des récepteurs de façon claire, lisible, agréable et précise.

Automatisation du plan de surveillance

QJRN/400 allège la charge de travail générée par les processus de contrôle en automatisant totalement l'exécution des analyses adaptées à chaque type de contrôle : simple message OS/400 ou email pour les alertes sur des événements sensibles, rapports au format PDF ou Excel pour les rapports périodiques (journaliers, hebdomadaires, mensuels) directement mis à disposition des personnes adéquates par email ou FTP.

SÉLECTION DES INFORMATIONS SENSIBLES

QJRN/400 peut identifier des événements « sensibles » qui sont potentiellement suspects :

- Nombreuses possibilités de sélection avec les opérateurs classiques (=, >, <, Like, Range, List...) ou par programme spécifique, applicables sur tous les champs, en valeur absolue ou en variation (en valeur, en pourcentage ou spécifique aux dates).
- Listes de valeurs à sélectionner ou à omettre saisies ou alimentées par un programme ou par une requête antérieure.
- Sélections génériques telles que "opérations effectuées hors heures ouvrables", "opérations effectuées hors applicatif" (par comparaison à un référentiel des programmes).
- Sélections sur les profils (classe, groupe, droit spécial), programmes, travaux, systèmes, périodes.

LES DIFFÉRENTS MODES D'EXÉCUTION

- **Le mode normal** : les requêtes peuvent être exécutées à la demande (en batch ou en interactif) : on utilisera ce mode pour des investigations.
- **Le mode continu** : dans le cadre d'un plan de détection d'une fraude, ou pour la recherche d'un bug aléatoire dans l'applicatif, une requête en mode continu alertera un utilisateur final dès qu'un événement surveillé se produit ou déclenchera une action particulière.
- **Le mode automatique** : déclenché automatiquement lors du détachement des récepteurs, ce mode assure l'exhaustivité des informations collectées, qu'elles le soient à des fins statistiques ou de traçabilité dans le cadre de suivi qualité.
- **Le mode planifié** : permet d'extraire à une fréquence paramétrée (année, mois, jour, heure, minute) des informations sur la vie de votre applicatif ou de votre système.

LES MODES DE RESTITUTION

Quel que soit le mode utilisé pour extraire les données, QJRN/400 offre une grande variété de rapports : que votre analyse porte sur un événement précis, ou sur une période de plusieurs mois, vous pouvez rapidement générer des rapports répondant à vos besoins d'audit interne et externe (Clichés détaillés, historiques synthétiques, statistiques) aux formats PDF, Excel, Word, ou HTML et les distribuer par email ou sur un serveur FTP.

- **Les sorties écran** : claires et paramétrables, elles permettent de visualiser les modifications effectuées sur la sélection en cours.
- **Les sorties messages** : spécialement adaptées aux requêtes en mode continu, elles permettent d'avertir en temps réel de la survenance du bug tant recherché (message OS/400 au service informatique) ou d'une modification potentiellement suspecte d'une zone sensible (email au responsable des limites de crédit).
- **Les fichiers trace** : très utiles pour assurer la traçabilité de toutes les modifications sur des zones critiques dans un ou plusieurs fichiers selon des critères applicatifs définis comme clés (reconstitution de l'historique d'un dossier médical, d'un compte bancaire, d'un produit pharmaceutique). Ils sont facilement exploitables par Excel.
- **Les fichiers de préparation** : utilisés avec le mode automatique ils assurent la conservation des événements sensibles après l'épuration des récepteurs. Sur de gros volumes, ils servent de présélection qui sera exploitée par une ou plusieurs requêtes secondaires.

Modèles et Echanges multi-sites

QJRN/400 offre aux organisations multi-sites la possibilité de définir une politique de sécurité et un plan de surveillance homogène, et de le distribuer sur les sites distants, sans aucune ressaisie.

Des modèles d'audit sont disponibles pour de nombreux progiciels du marché : ils répondent à 95% des besoins en matière d'audit. La rapidité de mise en œuvre simplifie la mise en conformité.

ATOUTS

- Suivi efficace de toutes les vulnérabilités
- Nombreux formats disponibles pour les rapports
- Processus d'extraction des événements garantissant l'intégrité des données
- Pertinence des rapports par sélection des seuls événements sensibles
- Alertes en temps réel pour une meilleure réactivité
- Simplicité d'utilisation des requêtes par un non informaticien, permettant l'indépendance des auditeurs
- Interface unique pour l'audit base de données de toutes vos applications et pour l'audit système
- Distribution d'un plan d'audit homogène sur les sites distants
- Mise en œuvre rapide
- Modèles d'audit disponibles pour de nombreux progiciels

VALEUR AJOUTÉE

- Diminution du risque de malveillance
- Anticipation des litiges et diminution des risques de pertes financières
- Haut niveau d'automatisation
- Compatibilité avec les principaux logiciels de haute disponibilité
- Retour sur investissement rapide, en réduisant le coût de mise en conformité



QJRN/400 et **CONTROLER**
sont des produits



ZI Les Iles • 190 route des Sarves
74370 METZ-TESSY
FRANCE
Téléphone : +33 4 50 69 45 98
Télécopie : +33 4 50 69 45 99
Email : contact@cilasoft.com
Web : <http://www.cilasoft.fr>

CONTRÔLE D'ACCÈS

QJRN/400 peut être associé à notre solution **CONTROLER** pour constituer **une suite d'audit et de sécurité complète** : le contrôle d'accès et le suivi détaillé de tous les événements au travers de la même interface.



**LA SATISFACTION DE SAVOIR
CE QUI SE PASSE CHEZ SOI !**

VOTRE CONTACT