



Pour un Système d'Informations naturellement efficace ...



NEWSLETTER

N°5 - 5 juillet 2002

SOMMAIRE

" LA SECURITE LOGICIELLE "

EDITORIAL par Philippe MAGNE

Editorial

par Philippe MAGNE, CEO

L'approche services

par Olivier BONNET, DG

ARCAD- Skipper : Une autre vision de la Sécurité Logicielle.

par Alain GRILLET,
Directeur Activité
Services

La Sécurité

En matière de sécurité, on peut constater que si les entreprises sont très sensibles aux aspects matériels, elles le sont beaucoup moins sur la partie logicielle. Pourtant, l'indisponibilité engendrée par la mise en place d'une nouvelle version "buggée" est tout aussi préjudiciable (et quantifiable) que celle résultante d'une panne matérielle, même si elle est moins "spectaculaire". Ceci est d'autant plus dommageable qu'une part non négligeable de ces anomalies est due à des défauts d'installation qui ne se produiraient pas si les procédures de mise en production étaient automatisées.

La principale raison à cet état de fait, est sans doute que si assurer la sécurité d'un matériel consiste "simplement" à garantir sa haute disponibilité, il n'en va pas de même pour le logiciel qui lui subit nécessairement de nombreuses évolutions durant toute sa durée de vie pour répondre en permanence aux exigences de l'entreprise.

La finalité dans le domaine du logiciel ne consiste donc pas simplement à maintenir son état de bon fonctionnement mais à gérer au mieux cet état de "changement permanent", ce qui rend la tâche beaucoup plus délicate à maîtriser.

L'atteinte de cet objectif passe par la mise en place à la fois de méthodes (plans qualité logiciel, normes et standards), **mais également d'outils de gestion de configuration et de gestion des tests, tels qu'ARCAD-Skipper et ARCAD-Qualifier.** De nombreux clients ont d'ailleurs eu la démarche d'implémenter notre outillage pour accélérer l'implémentation de la méthodologie, et ils s'en félicitent. La sensibilité générale sur ce thème de la sécurité s'est malheureusement accentuée depuis le 11 Septembre dernier. Faut-il arriver au pire pour se préoccuper de sa sécurité ? Si cette question métaphysique vous hante, vous trouverez dans ce nouveau numéro de notre newsletter quantités d'articles qui, je l'espère, vous feront retrouver une certaine sérénité.

Bien cordialement,

Philippe MAGNE

FICHE PRATIQUE : Arcad-Skipper et la Sécurité Logicielle.

par **Michel MOUCHON**,
Directeur Technique

Ils nous ont fait confiance

Espace Partenaires

Evènements

Dans le prochain numéro...

L'APPROCHE SERVICES par Olivier BONNET

La haute disponibilité et la préservation du patrimoine applicatif

La plateforme iSeries se trouve à la croisée des évolutions technologiques. C'est à ce jour la seule plateforme d'intégration permettant de disposer de plusieurs systèmes d'exploitation. A ce titre, c'est une plateforme qui peut permettre de reconcentrer des systèmes répartis comme de réaliser un downsizing de Mainframe. Les applications appelées à tourner sur le iSeries sont de plus en plus critiques avec des besoins en qualité de services sans défaut. Parler de la haute disponibilité sur cette plateforme représente donc un enjeu réel.

Le mode Logiciel

Le fait de vouloir garantir un fonctionnement en mode haute disponibilité impose d'outiller les plateformes avec des solutions telles que la solution Mimix proposée par Geac Enterprise Solutions. Les fonctionnalités majeures sont les suivantes :

- q **Mise en cluster**
- q **Disponibilité des données**
- q **Redondance matérielle locale ou multi-sites**
- q **Equilibrage de charge**

ARCAD Software est en train de développer un module, Arcad for Mimix, qui va permettre de garantir une phase d'audit orientée haute disponibilité ainsi que la cohérence et l'intégrité des applications mises en production.

Cette démarche est directement dans la logique des Suites ARCAD Software. En effet, pour garantir de la haute disponibilité, il est impératif d'assurer la maîtrise du cycle d'évolution des applications en s'attachant à gérer au travers d'ARCAD-Skipper la gestion des composants ainsi que les références croisées inter-composants et inter-applicatifs.

L'intégrité des transactions

Pour garantir un fonctionnement en mode haute disponibilité, il est préférable de disposer d'applications intégrant la notion de transaction (contrôle de validation ou Commit Rollback) au moins sur les transactions qualifiées de critiques. Ceci permet de repartir d'un état stable cohérent sur l'ensemble des transactions gérées en cas de panne matérielle.

La Suite ARCAD-Observer va permettre de simplifier la recherche des points de commit en s'attachant à découvrir de façon outillée les différentes transactions intégrées à l'application. Ceci permet d'optimiser le temps nécessaire à la mise en conformité des applications.

Les services à valeur ajoutée

Dans ce contexte orienté haute disponibilité, ARCAD Software propose de participer aux phases d'audit haute disponibilité et de mise en place d'une gestion de versions seule garante de la cohérence des composants mis en production.

De plus, ARCAD Software propose de participer à la migration des applications critiques vers le mode transaction.

Quand on parle de " **Sécurité Logicielle** ", on pense essentiellement à la sécurité des données : procédure de sauvegarde, contrôle d'accès, cryptage, ... De nombreux acteurs apportent des réponses hardware ou software à ces problématiques.

Mais on oublie souvent que, malgré tous ces composants, les données du système d'informations peuvent devenir inexploitable si les applicatifs qui les gèrent comportent des anomalies ou sont rendus inutilisables par des montées de versions trop rapides ou des installations mal maîtrisées.

Depuis 1992, avec la suite ARCAD-Skipper, nous nous sommes intéressés à cette autre facette de la sécurité logicielle : fournir les solutions permettant d'assurer la haute disponibilité des applicatifs. Appuyé sur son référentiel, ARCAD-Skipper offre des éléments de sécurité durant tout le cycle de vie logiciel :

- q **Avant le développement, l'exhaustivité des analyses d'impact permet de valider l'étendue des actions à entreprendre.**
- q **En cours de modification d'un composant logiciel, la gestion de versions évite les pertes d'information ou les dysfonctionnements liés aux maintenances parallèles. Les contrôles d'intégrité évitent les erreurs de niveau.**
- q **Les tâches longues et rébarbatives (transferts des sources ou objets d'un environnement à un autre, recompilations,), sources d'erreurs, sont prises en charge par l'outil. Les équipes de développement se concentrent alors uniquement sur les phases pour lesquelles elles apportent une réelle valeur ajoutée.**
- q **Les mises en production ainsi que les distributions et installations sur sites distants des nouvelles versions sont également automatisées. Les différents niveaux d'information sont historisés (par version, par composant). Les fonctions de retour arrière (rollback) en cas d'incidents sont disponibles.**

Tous ces points, parmi de nombreux autres, concourent à l'obtention de systèmes d'informations toujours opérationnels.

Cette sécurisation des environnements logiciels s'accompagne alors d'un autre élément difficilement quantifiable mais hautement appréciable : la satisfaction des utilisateurs !

Pour assurer la sécurité des objets de vos applications gérés avec la suite **ARCAD-Skipper**, le produit intègre deux niveaux de sécurité :

- q **La Sécurité dite " logique " est celle qui régit la manipulation des composants dans les divers environnements,**
- q **La Sécurité " physique " qui correspond à la gestion des droits et de la propriété sur les sources et objets d'une application.**

La Sécurité logique

Ce que l'on appelle la " sécurité logique " dans ARCAD, c'est la capacité d'implémenter les règles de base relatives à la gestion des environnements. Ce sont elles qui garantiront la sécurité des

Contactez-nous

E-mail

Visitez
notre site web

Téléchargez
cette Newsletter
au format PDF

environnements, le respect des règles de mises en test et mises en production établies et l'intégrité du référentiel ARCAD.

Concrètement, elles permettent d'interdire l'accès en modification aux membres source en direct, via des outils autres que ceux d'Arcad comme STRSEU, dans l'environnement de référence et les environnements de test.

Ces règles vont régir les autorisations de transfert des composants entre les environnements et les autorisations de manipulation des composants à l'intérieur des environnements via les commandes ARCAD.

La Sécurité physique

Pour obtenir un niveau de sécurité maximal, il est indispensable de respecter la règle suivante :

Le propriétaire des objets de production doit être différent de celui des environnements de test et de développement

Ainsi, les développeurs et testeurs n'auront aucun droit sur l'utilisation des objets de production. Il est possible de définir dans ARCAD l'utilisateur propriétaire d'un environnement de référence, de test ou de développement. Ceci a pour effet de rendre cet utilisateur propriétaire des objets de l'environnement lors de leur remplacement. Si aucun utilisateur n'est indiqué, l'ancien propriétaire est reconduit lors des remplacements de composants alors que QPGMR est affecté lors des ajouts de composants.

En ce qui concerne la gestion des droits, aucun automatisme particulier, lié à la notion d'environnement n'existe. La philosophie générale est la non dégradation de l'existant, autrement dit, si un objet est remplacé, les droits précédemment affectés à cet objet sont conservés. ARCAD assure ici une garantie de non régression : tout ce qui avait été affecté est conservé.

Ils nous ont fait confiance ...

Bienvenue ce mois-ci à :

- **VP Bank**
- **LOGINOR**

ESPACE PARTENAIRE(S)



QJRN/400 : la boîte noire de votre IBM iSeries.

Si beaucoup de ressources sont affectées à la sécurisation des accès externes avec le développement des communications Internet (intrusion, firewall,...), à la sécurité des données (haute disponibilité, Arcad,...), le contrôle des accès internes reste le parent pauvre du plan de sécurité dans beaucoup de sociétés. Ce constat est paradoxal quand on sait que la fraude interne est généralement estimée à 80% du risque global de malveillance.

Il serait illusoire de prétendre que les plus belles procédures de sécurité ne comportent pas la moindre faille. C'est la détection précoce de ces lacunes qui permettra d'améliorer l'efficacité de ces procédures, mais aussi d'intervenir dans les processus pour limiter les conséquences d'opérations malveillantes ou anormales.

Tout plan de sécurité comporte des étapes de sécurité active (contrôle d'accès, protection des données), mais doit également comporter des étapes d'audit et de contrôle.

C'est à cette problématique que répond le logiciel QJRN/400 sur la plate-forme IBM iSeries : QJRN/400 fournit tant aux informaticiens qu'aux auditeurs, un outil simple d'administration de la journalisation, et des fonctions puissantes d'analyse du contenu de tous les journaux, qu'ils soient de type Système, Base de données ou Utilisateur.

Le module d'administration permet de créer entièrement des environnements de journalisation ou de reprendre des environnements existants. Toutes les opérations sur les journaux et récepteurs peuvent être prises en charge (création, détachement, démarrage, sauvegarde, suppression...). QJRN/400 est entièrement compatible avec les autres logiciels utilisant la journalisation comme ceux de haute disponibilité. De plus, QJRN/400 gardera la trace de toutes les opérations sur vos environnements, qu'ils soient administrés par QJRN/400 ou non.

La journalisation est une mine d'informations infalsifiables immensément riche pour qui peut l'exploiter, mais inorganisée et souvent très volumineuse.

Les requêtes sont dotées de sélections puissantes et précises permettant d'analyser cette matière et de la restituer sous des formes directement lisibles par des utilisateurs finaux comme les auditeurs. Elles permettent de zoomer sur un événement précis, d'élargir le champ d'investigation pour mieux comprendre le contexte d'une anomalie, voire de donner une vue statistique de l'utilisation d'une application.

Les requêtes peuvent répondre à tous types de besoin :

- q **Analyse ponctuelle (recherche d'un bug, de son contexte et de ses conséquences) : on utilisera alors le mode normal.**
- q **Surveillance permanente de certaines informations sensibles (limite de crédit, RIB, n° de Carte Bancaire, profils sensibles, fraude) : on utilisera le mode continu avec envoi immédiat d'un mail au chef de service.**
- q **Analyse exhaustive avec garantie de continuité dans le temps (opérations hors heures ouvrables ou hors applicatif, contrôle des objets mis en production, interventions des développeurs sur les données de production...) : on utilisera alors le mode automatique qui analyse les récepteurs détachés.**

La planification de requêtes prédéfinies et des tâches d'administration confiées à QJRN/400 constitue la base d'un plan d'audit automatisé. La grande facilité d'utilisation de QJRN/400 permet d'assurer l'indépendance des auditeurs vis à vis du service informatique tout en soulageant ce dernier de justifications fastidieuses et de plus en plus fréquentes.

QJRN/400 répond également aux exigences de traçabilité de l'information exigée par les chartes qualité.

Cilasoft, expert Arcad, est également partenaire QJRN/400.

Pour tout renseignement, consultez www.cilasoft.com/qjm400 ou contactez-nous à <mailto:info.qjm400@cilasoft.com>

Dans le prochain numéro...

Le prochain numéro de la **newsletter d'ARCAD Software** paraîtra au mois de septembre prochain.

Pour toute demande d'information ou questions relatives à cette newsletter, vous pouvez contacter : Stéphanie ZELKO, Service Marketing : szelko@arcadsoftware.com

N'hésitez pas à nous transmettre vos impressions, remarques et suggestions afin que nous puissions mieux encore répondre à vos attentes.

Si vous ne souhaitez plus recevoir d'informations de notre part : [cliquez ici](#)

Bien à vous,

L' équipe ARCAD Software.

[Haut de la page](#)