



Septembre 2000

etic news

génération mainframe

lettre d'information technique et commerciale consacrée aux grands systèmes IBM



SOMMAIRE

Editorial : du nouveau dans le mainframe

NOS PRODUITS :

Consul/RACF et Audit v2.6.0 annoncé pour octobre 2000.
Halo/SSO v 4.5 de Neon Systems : le sign-on unique NT - OS/390
Shadow AutoHTML for CICS/TS, de Neon Systems
Annonce de Megacrypt/MVS v4.2

ACTUALITE :

OS/390 v2r10
Le coup de gueule...

NOS CONSEILS

Le mode PADS de RACF
Des conseils RACF
SSL : le mainframe aussi est concerné
Qu'est-ce qu'un certificat ?
Beaucoup de bruit (pour rien ?) autour de LDAP
Kerberos, pour l'authentification et les droits d'accès
Ascii et FTP
Freewares

ONLINE

Editorial : du nouveau dans le mainframe

Le monde du mainframe bouge beaucoup ces temps-ci. Voici à notre avis les faits les plus marquants.

Nos fournisseurs habituels, IBM, HDS, Amdahl sont toujours là, mais HDS, délaissant les Trinium et autres Pilots, peu rentables pour lui, prend un virage stratégique avec sa future architecture « **Hercules** ». Constatant que l'hétérogénéité est la règle chez le client, HDS va proposer une machine hétérogène, à base de CMOS et de puces Intel. Hercules (livrable fin 2001) supportera donc plusieurs systèmes (sans doute OS/390, Unix et NT). HDS veut ainsi élargir son marché, mais risque d'y rencontrer une forte compétition.

Le problème de l'hétérogénéité se pose surtout pour les logiciels, particulièrement dans le monde web et client/serveur. IBM quant à lui a décidé de s'y attaquer par un autre biais, avec **Linux/390**. Linux, est multiplate-formes, indépendant des fournisseurs, plus répandu et plus connu que les systèmes propriétaires ; pour toutes ces raisons il aurait vocation à intégrer tous les applicatifs et à devenir le serveur web par excellence (le mainframe restant positionné comme serveur de données).

Bien que système Posix (comme USS), Linux n'appartenait pas vraiment à la culture IBM. Malgré ses atouts, il est encore largement distancé par les systèmes propriétaires ne serait-ce qu'au plan fiabilité et sécurité. Et WebSphere d'IBM, sous Linux ou sous OS/390, avec son approche « *cafétéria* » (*dixit le Gartner*), ne plaît pas à tout le monde.

Pour HDS comme pour IBM, ce sont deux paris sur le futur. Il n'est pas certain que les clients apprécient et aillent dans la direction espérée.

Du côté du **mainframe à 64 bits** (nom de code *Freeway*) on attend des annonces d'IBM peut-être au 3ème trimestre, les livraisons pouvant survenir en fin d'année ou en début 2001. Le signe avant-coureur qui, pour les techniciens, prouve que « cette fois, c'est pour bientôt » est le fait que HLASM r4 supportera des constantes d'adresses à 8 octets. On parle aussi d'une mesure plus fine des consommations CPU, permettant une meilleure facturation soft...

Soixante-quatre bits ou pas, on s'oriente pour la décennie vers une architecture idéale : le mainframe comme serveur de données, le PC avec browser pour l'interface client, et l'inévitable TCP/IP pour faire le lien. Le client léger, c'est une redéfinition du rôle du mainframe et du terminal : autrefois l'un était superactif et l'autre passif, à présent chacun est actif dans ce qu'il sait le mieux faire. Et les sites qui ont éludé l'étape intermédiaire du client-serveur s'en trouvent plutôt bien.

SNA est toujours là, mais il est clair qu'IBM fait porter ses efforts sur IP. Avez-vous encore chez vous beaucoup d'écrans 3270, des 3174, 3745 ou 3746 ? OSA-Express donne non seulement le moyen standard de se connecter au mainframe mais on suppose que dans quelques années ce sera un support d'accès aux données externes concurrent d'Escon ou de Ficon.

Ouverture et sécurité : deux exigences souvent difficiles à concilier, nous le savons bien puisque nous vendons des produits qui touchent aux deux domaines. Nous essayons dans ce numéro de clarifier certains termes, liés à ce paradoxe de « l'ouverture dans la sécurité », des termes que vous rencontrez de plus en plus, et pas seulement dans les brochures des vendeurs : SSL, certificat, LDAP...

Nous participons à la croissance globale du nombre de Mips mainframe. En effet, notre P/390 de 5 Mips va être remplacé par un magnifique Multiprise 3000, modèle 7060, de 60 Mips...

Thierry FALISSARD

NOS PRODUITS

La nouvelle version de Consul/RACF et Audit v2.6.0 est annoncée pour octobre 2000.

Le **Coup de pouce de Carla**, version de juin 2000, augmenté de nouvelles requêtes, est disponible sur notre site web. Tout ce que vous rêviez de faire avec RACF (et Consul), sans pouvoir y parvenir...

Nous avons réalisé récemment, pour un client Consul, en Carla et en REXX, un développement consistant à générer des états de sécurité personnalisés destinés à des administrateurs RACF. Ces états sont envoyés dans la messagerie, le nom+prénom tiré de RACF étant transformé pour devenir prénom.nom@domain.fr par un exec REXX (qui rajoute aussi les en-têtes attendus par SMTP).

Ventes récentes de Consul : AXA.

Halo/SSO v 4.5 de Neon Systems : le sign-on unique NT - OS/390

Disons-le tout net, les produits de *single sign-on* ont souvent mauvaise réputation. L'avantage supposé (on se signe une seule fois pour accéder ensuite à toutes les plates-formes) est effacé par les coûts du produit (coûts de gestion comme d'achat), et souvent son manque de fiabilité et de sécurité. Et en pratique, il est illusoire de parvenir à un userid/password unique sur **tous** les systèmes.

Neon a cherché à traiter le problème dans son aspect le plus courant. La plupart des entreprises exploitent une infrastructure informatique à bases de serveurs NT et de mainframe(s) OS/390. La connexion au(x) mainframe(s) survient après le sign-on NT. Il serait intéressant de synchroniser sur NT et sur OS/390 les événements suivants : changements de mots de passe ; activation ou suspension (revoke-resume en termes RACF) ; suppression de userid.

C'est exactement ce que fait Halo/SSO. Les userids peuvent être les mêmes sur NT et OS/390, ou « mappés » par une table de correspondance. Les mots de passe peuvent être les mêmes ou peuvent être différents (si on demande à Halo de générer des PassTickets RACF).

La version 4.1 de Halo/SSO imposait l'emploi de SNA Server côté NT, le *host account cache* de NT servant à stocker les userids/passwords. Il fallait avoir même userid/password sur tous les MVS, en contrepartie les changements de mots de passe étaient propagés partout par le point focal SNA Server (avec des scripts de sign-on).

Avec la v 4.5, SNA Server est toujours supporté mais n'est plus nécessaire. La synchronisation des users et mots de passe est réalisée par une API Halo. Le logon au mainframe devient transparent. Les changements de mots de passe sur une plate-forme sont répercutés sur toutes les autres. Halo met en place dynamiquement sur OS/390 les exits de sécurité nécessaires (interception des commandes et identification des users). Pour se signer sur une application OS/390, un PassTicket peut être produit par Halo/SSO.

La technologie de communication en mode client/serveur est la même que pour Shadow/Direct. Côté MVS, le suivi depuis ISPF est comme d'habitude très complet (une interface web destinée à l'administrateur existe aussi).

Shadow AutoHTML for CICS/TS, de Neon Systems

Ils l'avaient fait pour IMS, ils le font à présent pour CICS. Avec ce nouveau composant de Shadow, vous pourrez **accéder à vos transactions CICS depuis le web**, sans reprogrammation ni codage particulier, ni customisation, ni modification BMS, par un mapping qui est externe au CICS. Comme toujours, la robustesse et la performance devraient être au rendez-vous, et la mise en place très rapide. On attend pour bientôt l'annonce définitive (Shadow AutoHTML CICS à ce jour est en bêta-test).

Annnonce de Megacrypt/MVS v4.2 pour octobre 2000

Outre les algorithmes symétriques DES, triple-DES, et Blowfish, la v4.2 supportera l'algorithme asymétrique **EIGamal** (utilisé aussi par PGP, parallèlement à RSA). Cela signifie concrètement que deux sites mainframes n'auront plus besoin de se communiquer des informations secrètes (les clés de chiffrement) : seules les clés publiques, transmises une fois pour toutes, suffiront pour tous les échanges ultérieurs. Une taille de clé de 1024 jusqu'à 2048 bits sera proposée. Les clés publiques PGP seront supportées.

Prévus aussi dans la v4.2 : un support limité de PGP v6 (possibilité de chiffrer sur MVS et de déchiffrer par PGP hors MVS) ; les algorithmes de hashing MD5 et SHA, un utilitaire de gestion des clés (les clés sont stockées dans la base RACF pour plus de sécurité).

ACTUALITE

OS/390 v2r10

Alors que v2r9 était une release mineure, v2r10 est riche en apports, en attendant la suivante (v2r11 ou même v3 ?) qui, elle, sera une release majeure (avec sans doute les 64 bits).

La v2r10 comporte de nombreux apports liés à la sécurité et aux systèmes ouverts qui concernent RACF, VTAM, USS, LE, PSF, Sysplex, SMS, JES, ISPF, SDSF, OSA/SF, etc., apports que vous trouverez dans le release guide GC28-1725-09. Elle nécessite une machine « moderne » : les pré-CMOS ou CMOS Rx1 de première génération ne conviennent pas.

Pour nous limiter à la sécurité, notons l'authentification à la mode Kerberos (en relation avec RACF, LDAP et USS), le filtrage par nom de certificat, des améliorations dans le mode PADS (un meilleur diagnostic), dans FTP et dans TCP/IP (notion de zone de sécurité=groupe d'adresses IP). Si les termes qui précèdent vous effraient, voyez ci-dessous nos explications.

La v2r10 peut coexister avec v2r6 et au-delà. La version qui suivra (en 2001) requerra au moins des machines G5 (9672 xx6), au grand dam des sites qui ont acheté des CMOS moins récents... Dans ce cadre, la v2r10 peut être vue comme une version à atteindre pour stabiliser votre environnement au moins quelques années (si vous ne passez pas aux G5 tout de suite).

Le coup de gueule...

C'est une tendance malade, IBM aime changer les noms de ses produits. Paradoxalement, un nouveau nom dénote rarement quelque chose de vraiment nouveau, mais plutôt une velléité de marketing, voire un certain embarras pour positionner un composant (OMVS, OE, USS...) ou une offre (Websphere). Le client s'y perd, et ne reconnaît plus dans *SecureWay Security Server for OS/390*, *eNetwork* (ou est-ce *SecureWay*?) *Communications Server* ou *Infoprint Server* ce qui s'appelait auparavant (depuis 10 ou 20 ans) RACF, VTAM ou PSF. Les noms courts font trop technique et ne font pas assez rêver : parlez de *dasd* et vous êtes un dinosaure, *Enterprise Storage Server* est autrement dans l'air du temps !

Le résultat est maintenant que les produits ont souvent deux noms, un long qui fait plaisir aux gens du marketing, et le nom d'origine, plus court (appelé par les Anglo-saxons TLA, *three-letter acronym*, voire YABA, *yet another bloody acronym*). Dans ses annonces IBM se sent d'ailleurs obligé de rappeler entre parenthèses le nom court, pour que le client et les techniciens puissent comprendre.

Cette « novlangue » de Big Blue veut imposer l'idée que les produits sont toujours au goût du jour et ne vieillissent jamais. N'allez pas leur rappeler que RACF date de 1976, c'est-à-dire du siècle dernier (presque), et que c'est dans les années 60 que le mainframe tel que nous le connaissons a été conçu...

NOS CONSEILS

Le mode PADS de RACF

Le mode PADS (*program access to datasets*) de RACF permet de protéger un fichier en donnant accès à certains users au moyen d'un programme spécifique (qui sans doute filtrera les données intelligemment – il ne faut pas que ce soit un programme à tout faire tel que IEBGENER ou IDCAMS).

Il suffit d'établir une access-list conditionnelle par une commande telle que :

```
PERMIT dsname ID(userid) ACCESS(read) WHEN(PROGRAM(pgm1))
```

Pour que cela fonctionne, il faut que tout module chargé dans l'espace-adresse soit *controlled*, c'est-à-dire connu de RACF (on peut utiliser un profil générique « * » dans la classe PROGRAM) ; la raison est qu'on ne peut faire confiance a priori à n'importe quel programme qui se trouve en mémoire. Dès qu'un programme non connu de RACF est chargé, un dirty bit (TCBNCTL) est positionné et le PADS ne fonctionne plus (abend S913 à l'open du fichier). Sous TSO, un logoff / logon est alors nécessaire (ou une invocation par TSOEXEC).

La mise en place du PADS peut être pénible (le moindre programme oublié fait tout échouer). Nous avons publié un REXX qui définit le programme « * » pour toutes les bibliothèques de la link-list. Dans la v2r10 d'OS/390, IBM propose un « PADS allégé » qui permet d'ignorer le dirty bit (via l'exit ICHRCX02). Le goodie RACTRACE d'IBM est précieux pour déboguer les problèmes de PADS (pour repérer le programme qui a tout fait échouer).

PADS est souvent requis pour USS (daemons et programmes serveurs) et aussi... pour notre produit Consul/RACF. En effet, le mode d'administration décentralisée de Consul (mis en oeuvre depuis ISPF ou Windows) repose sur un filtrage PADS de la base RACF lié aux droits de l'administrateur (pour qu'il ne voit que les objets RACF de son domaine).

Des conseils RACF

Plutôt que de définir un profil avec un uacc READ, UPDATE, etc., définissez-le en uacc(NONE) et faites un PERMIT en READ, UPDATE, etc. au bénéfice d'un user générique **ID(*)**. L'intérêt est que vous protégez le profil contre un accès effectué par un user non défini à RACF (UADS, NJE, started task non associée à un userid, etc.).

Comment repérer et détruire des userids qui ne servent plus ? L'idéal serait d'être synchronisé avec une base du personnel, mais ce n'est pas toujours possible. Si vous disposez de Consul/RACF, une simple requête vous permettra de générer les commandes RACF adéquates, et éventuellement de détruire les fichiers des users concernés. Sinon, vous pouvez passer un job tel que le suivant :

```
//STEP1      EXEC PGM=IKJEFT01,DYNAMNBR=20
//SYSTSPRT DD SYSOUT=*
//SYSTSIN   DD *
  SR CLASS(USER) AGE(180) CLIST('DELUSER  ')
```

Des commandes DELUSER seront générées dans un fichier userid.EXEC.RACF.CLIST pour tous les userids non connectés depuis plus de 180 jours.

Des erreurs à ne pas faire avec RACF :

- définir un profil * dans la classe PROGRAM avec uacc(none) ; votre prochain IPL risque d'être, disons... héroïque ;
- définir un profil ** dans la classe FACILITY : cela a un impact sur JES, qui, cherchant des profils NJE.node, trouve ce générique « butoir » et suppose alors que les signons NJE ou RJE sont contrôlés par RACF.

SSL : le mainframe aussi est concerné

SSL (Secure Sockets Layer) est une couche sécuritaire au-dessus de TCP/IP destinée à créer une connexion sécurisée. SSL, inventé par Netscape, a une forte connotation *web* : il est invoqué quand vous faites des achats sur Internet (serveurs https), pour saisir des mots de passe ou des numéros de carte bancaire ; mais en fait SSL permet de protéger n'importe quelle connexion TCP/IP, par exemple un TN3270 pour faire du TSO ou du CICS. Avec SSL v2, le serveur est authentifié, avec SSL v3, le client peut également l'être.

SSL est standard en OS/390 depuis la v2r6. SSL est un protocole cryptographique qui requiert une clé publique signée, ce qu'on appelle un *certificat*.

Qu'est-ce qu'un certificat ?

Les algorithmes à clé publique permettent de mettre en oeuvre des fonctions de sécurité (authentification, confidentialité, intégrité) sans partage de secret (mot de passe, clé de chiffrement). Pour que cela fonctionne, il suffit que les partenaires se communiquent leurs clés publiques (non secrètes). Il faut cependant qu'ils aient la certitude que la clé publique appartient bien à l'interlocuteur qui se présente, et non pas à un autre, sinon la porte est ouverte à différentes attaques (*man in the middle*).

C'est le rôle du certificat, qui fournit la clé publique accompagnée d'une signature. Le certificat obéit à une norme (X509 v3) et est délivré par une « autorité certifiante » (qui signe avec sa clé privée). On aboutit ainsi à une hiérarchie de certification, avec souvent en haut de la hiérarchie une société spécialisée (Verisign, Thawte, en France CertPlus) dont les certificats sont automatiquement reconnus par les browsers du marché.

On peut aussi s'auto-certifier (pour des tests, ou dans un intranet), le certificat n'a pas alors une valeur forte.

RACF sait faire l'association entre un certificat et un userid (commande RACDCERT), ce qui évite de saisir un userid/password. Sous OS/390, les certificats sont créés sous OMVS par des utilitaires spécifiques (*mkkf* ou *gskkyman*).

Nous parlerons pas ici des PKI (*public-key infrastructures*), car il nous faudrait d'abord parler de LDAP...

Beaucoup de bruit (pour rien ?) autour de LDAP

LDAP (Lightweight Directory Access Protocol) est un protocole qui donne accès à travers le réseau à des données stockées dans une structure de répertoire en arbre, selon différents critères d'accès. Il

pourrait donc servir d'interface à un répertoire du personnel, un annuaire téléphonique, une liste de ressources réseau, une base de certificats digitaux (pour une PKI). Par exemple, les clés publiques PGP sont stockées sur différents serveurs LDAP (tel que ldap://pgp.surfnet.nl:11370).

LDAP est récent sur l'environnement OS/390. Le serveur LDAP avec LDAP v3 (et un *backend store* qui est DB2 ou RACF) n'apparaît qu'avec OS/390 v2r8.

LDAP, avec RACF comme *backend store*, permet d'authentifier un user (en vérifiant le mot de passe) depuis différentes plates-formes et ainsi de faire du SSO (bien que LDAP ne puisse être considéré comme un outil de SSO). Les produits de SSO qui existent sur le marché utilisent rarement LDAP mais vont l'intégrer petit à petit. Via LDAP, on peut retrouver des informations sur les users et les groupes, ajouter, modifier ou détruire des users ou des groupes (mais non d'autres types de profils).

LDAP peut donc être, dans le cas d'OS/390, une interface ouverte sur RACF, qui ne remplace pas RACF, mais permet de faire de l'authentification et de l'administration depuis un système autre qu'OS/390. Il y a bien d'autres applications envisageables, outre la sécurité. Les sites très hétérogènes trouveront bénéfice à avoir des répertoires centralisés et ouverts.

Kerberos, pour l'authentification et les droits d'accès

Kerberos, bien sûr, est dans la mythologie antique Cerbère, le chien à trois têtes qui gardait les Enfers. De nos jours, Kerberos garde cet Enfer qu'est l'informatique distribuée... Les trois têtes sont en général un utilisateur, un serveur de ressources et le serveur central Kerberos qui gère les droits d'accès, authentifie utilisateurs et applications, et distribue des « tickets » non rejouables valables quelques heures.

Créé au MIT pour résoudre le problème de l'administration des clés, Kerberos met en œuvre des procédés symétriques à base de DES assez complexes. S'il fallait le refaire aujourd'hui, on utiliserait sans doute des protocoles asymétriques (à base de RSA ou ElGamal).

Windows 2000 supporte Kerberos comme protocole d'authentification. OS/390 v2r10 peut devenir un serveur Kerberos, en lien étroit avec RACF (nouveau type de segment « KERB »). On peut donc imaginer un client non OS/390 (par exemple Windows 2000) qui s'authentifie sur OS/390 et obtient des « tickets ».

Ainsi les moyens d'authentification sur OS/390 sont de plus en plus nombreux : mot de passe classique (le plus simple mais le moins sûr), PassTicket, serveur LDAP, certificat digital, Kerberos, sans compter les solutions non IBM (SecurId).

Ascii et FTP

Un lecteur attentif nous a fait remarquer une inexactitude dans le numéro précédent d'etic news, où nous affirmions dans « Nos conseils FTP » que Iso 8859-1 était le code page Ascii.

En fait, ISO 8859 est l'extension à 8 bits du code US-ASCII (ISO 646) à 7 bits. ISO 8859-1 (qui date des années 80) est le jeu de caractères d'Europe de l'Ouest, qui correspond aux principales langues occidentales (on l'appelle aussi "Latin1").

Windows, VMS et presque tous les Unix supportent ISO 8859-1 ; MS-DOS et l'EBCDIC d'IBM sont des exceptions notables.

Il y a une dizaine d'autres ISO 8859-x, par exemple ISO 8859-15 introduit l'Euro (€) codé x'A4'. A ce propos, avez-vous remarqué sous ISPF l'option "Enable EURO sign" des settings ? L'Euro est x'9F' en EBCDIC (x'5A' pour les pays nordiques). Sous Word, on l'obtient avec rien moins que 5 touches (ALT 0 1 2 8)...

Freewares

MXI 2.2a de Rob Scott, version de juillet 2000, a des fonctions étendues (CDE, TCB, CHP...) qui le font de plus en plus ressembler aux moniteurs du marché (notamment RESOLVE) : www.secltd.co.uk/mxi_download.htm.

Share offre des dizaines de présentations techniques (cliquer sur « sessions »), une véritable mine d'informations très actuelles : www.share.org/proceedings/sh94/share00w.htm.

Une autre mine est bien sûr le site de **Xephon**, avec toutes les parutions de MVS Update de 1987 à 1997 : www.xephon.com/mvsupdate.html.

Notre **RACF password cracker**, qui a soulevé une polémique sur le forum RACF fin mai, est disponible : <http://os390-mvs.hypermart.net/cracker.htm>. Un cracker à prendre avec un grain de sel...

ONLINE

Un ambitieux portail S/390, avec surtout un moteur de recherche sur des centaines de sites mainframe (ceux d'IBM bien sûr, mais aussi notre site) : www.search390.com.

Si vous ignorez tout de SSL, Fortify vous dévoile les possibilités de votre browser : <https://www.fortify.net/sslcheck.html>.

L'authentification sur le web : une bonne description sur www.wwnet.net/~janc/auth.html (« a Guide to Web Authentication Alternatives »).

Notre site web hébergé sur OS/390 : r1-etic.francenet.net.

Et toujours nos produits :

- **Rexxtools** : www.open-softtech.com
- **Consul** : www.consul.com
- **Neon Systems** : www.neonsys.com
- **Link Manage** : www.linkmanage.be

Bulletin d'abonnement gratuit à envoyer ou à faxer à **etic**

Société

Adresse

Nom

Votre fonction

etic news est une lettre d'information technique et commerciale à parution périodique.

La rédaction ne garantit pas l'exactitude absolue ni le caractère exhaustif des informations publiées.

Toute reproduction, partielle ou totale, est strictement *encouragée*.

etic software,

26 rue Marceau,

92137 ISSY-les-Moulineaux Cedex

Tél : 01 46 48 69 69 Fax : 01 46 48 45 73

www.eticsoftware.com

E-mail :

sales@eticsoftware.com