NoToS

SSO & EIM
Le Single Sign On dans les mondes IBM et Microsoft

Résumé :

- La gestion des mots de passe est un des talons d'Achille de la Sécurité Informatique
- Pour simplifier cette gestion, **NoToS** propose le Pack EIM. Cet ensemble de services met en œuvre l'EIM d'IBM qui permet de disposer d'un seul identifiant pour un ensemble de serveurs et de logiciels (SSO). Il s'adresse à des réseaux à base d'AS/400 (iSeries, i5) et de Microsoft Active Directory
- Ce Pack EIM s'appui sur des produits livrés en standard par IBM et Microsoft, donc gratuits !

Dans ce document :

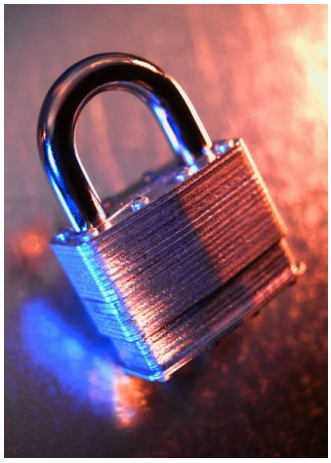
Sécurité et mot de passe

L'essentiel de la Sécurité de nos Systèmes d'Information s'appuie sur des **mots de passe** associés à des comptes utilisateur. C'est dire si la gestion de ces mots de passe est fondamentale. Mais cette gestion est complexe, en voici quelques exemples :

- Pour chaque utilisateur, les mots de passe à mémoriser sont nombreux, souvent un par serveur ou par application
- Les stratégies sont souvent contraignantes : fréquence de modification élevée allant jusqu'à une fois par mois, pas de caractères répétitifs, impossibilité de choisir un mot de passe déjà utilisé…
- Démotivation des utilisateurs qui en arrivent à écrire le mot de passe sur un Post It, au mieux collé sous le clavier
- Gestion de ces mots de passe par le Service Informatique qui impose le sésame et qui le mémorise dans un classeur ou dans un fichier Excel...
- Enfin, pour être tranquille, le mot de passe est définitif et le même partout, on se retrouve, alors, rapidement dans la situation où tout le monde connait le mot de passe de tout le monde.

Pour tous les Systèmes d'Information basés sur Microsoft Active Directory pour les réseaux Windows et sur un ou plusieurs AS/400 (iSeries, i5), IBM a défini EIM (Enterprise Identity Mapping). Cette architecture s'appuie d'une part sur l'organisation en place (Active Directory) et d'autre part sur des fonctions standard de l'OS/400 V5. Aucune licence n'est à acquérir !

Avec EIM, la gestion des mots de passe est simplifiée car elle ne s'appuie que sur ceux stockés dans l'Active Directory : un seul mot de passe par utilisateur quel que soit le nombre et l'hétérogénéité des serveurs concernés !



EIM : un seul mot de passe pour votre connexion Windows, pour tous vos AS/400 et pour bien d'autres logiciels...

Dominique GAYTE

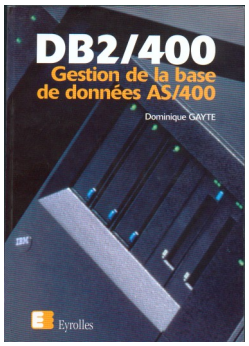
Dominique GAYTE, fondateur de **NoToS,** intervient sur l'Informatique des PME/PMI depuis près de 20 ans.

Il est expert en IBM AS/400 et en ses successeurs iSeries et i5 (il a publié plusieurs livres aux éditions Eyrolles sur le sujet) et il est spécialiste des nouvelles technologies.

Fort de ces diverses compétences, il s'est orienté vers la Sécurité des Systèmes d'Information.

Il est titulaire d'un Doctorat en sciences et d'un DESS en Informatique.

Il est certifié par IBM et Microsoft sur plusieurs technologies.



Dans le Pack EIM, la formations du Service Informatique et l'assistance à la réalisation des procédures essentielles vous assure de l'autonomie de vos équipes.

Principes de l'EIM

L'EIM s'appuie sur deux entités du réseau :

- le standard Kerberos, implémenté dans l'Active Directory
- et sur un contrôleur EIM (EIM Domain Controleur) installé dans un AS/400.

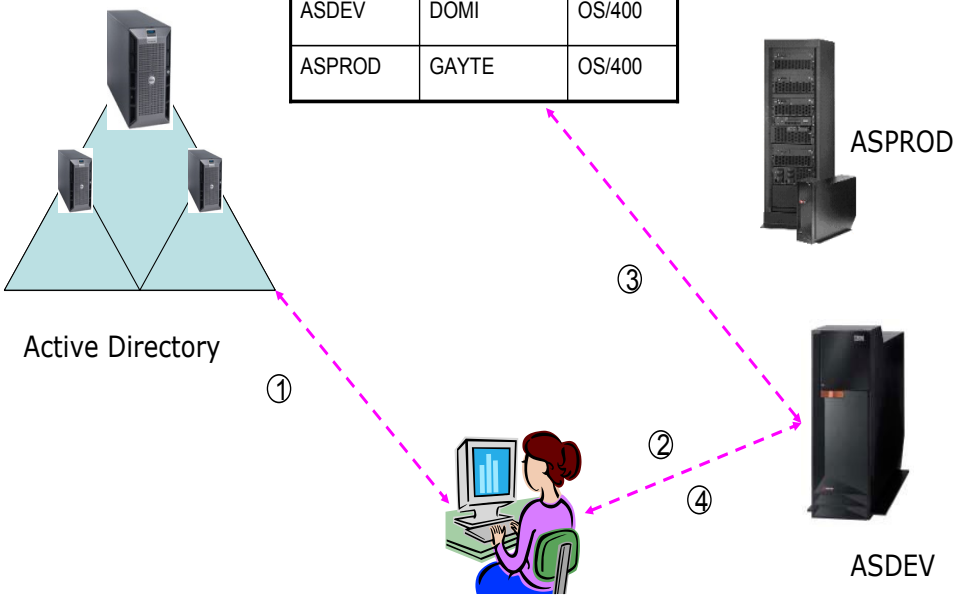
Les mots de passe ne sont présents, en standard, que dans l'Active Directory. Ils peuvent être désactivés sur tous les AS/400 concernés.

L'utilisateur, lors de son ouverture de session Windows, se connecte au domaine à l'aide de son identifiant Windows et du mot de passe associé. Lorsqu'une application, telle que l'émulation écran de iSeries Access for Windows (Client Access Express) démarre, elle demande un « jeton » à l'Active Directory (Kerberos). Ce jeton est présenté au serveur sur lequel on souhaite se connecter. Celui-ci demande au contrôleur EIM quel est le profil utilisateur à utiliser. Si la connexion est autorisée, la session est directement ouverte avec le bon profil utilisateur. Dans le cas de la figure ci-dessous, le nom de connexion au domaine est DGAYTE, et la session AS/400 sur le système ASDEV est automatiquement ouverte sous le profil DOMI.

Les utilisateurs ne maintiennent que le mot de passe de l'Active Directory selon les contraintes imposées à ce niveau : durée de validité, complexité...

La gestion des mots de passe est le talon d'Achille de la Sécurité Informatique !

Contrôleur EIM		
Serveur	Identifiant	Type
AD	DGAYTE	Kerberos
ASDEV	DOMI	OS/400
ASPROD	GAYTE	OS/400



Questions/réponses

Question : Faut-il apporter des modifications importantes à mon Active Directory ?

Réponse : non. Les actions à réaliser sur l'Active Directory sont superficielles, elles consistent à créer quelques comptes pour définir chaque serveur et chaque application concernés.

Question : Quels logiciels dois-je acquérir pour mettre en place EIM ?

Réponse : aucun, à condition d'avoir un Active Directory et un OS/400 en V5. Des restrictions peuvent être liées à la version de l'OS/400. La V5R3 est conseillée, la V5R2 est le minimum supporté. Active Directory est un composant de Windows Server (2000 ou 2003).

Question : Mes comptes Windows et AS/400 sont différents, est ce un problème ?

Réponse : non. Le contrôleur EIM fait le lien entre le compte Windows et les profils sur chaque AS/400 (voir figure de la page précédente). Ainsi, la connexion Windows peut de faire avec le compte DGAYTE, puis l'ouverture sur ASDEV s'effectuera automatiquement sous le profil DOMI et celle sur ASPROD sous GAYTE.

Question : Toute cette architecture est basée sur Active Directory. Que se passe t'il en cas d'arrêt de ce service ?

Réponse : les caches de Windows permettent de fonctionner pendant un temps limité. Nous fournissons une organisation et un mode opératoire qui permettent de continuer l'activité AS/400, même en cas de défaillance de l'AD.

Question : Quels sont les produits qui supportent le SSO ?

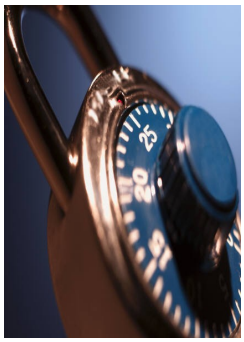
Réponse : tout d'abord pour l'EIM, il s'agit des produits IBM : iSeries Access for Windows (Client Access Express), iSeries Navigator et NetServer pour l'AS/400, mais aussi Z/OS (RACF) et AIX. Lotus Notes participe au SSO car il sait directement se synchroniser avec le mot de passe Windows. Enfin, il existe d'autres principes autorisant un SSO à partir des informations de l'AD. Il est ainsi possible de se connecter avec Linux , Windows NT et autres… Notre phase d'analyse permet d'identifier toutes les applications qui pourraient être concernées et tous les protocoles à mettre en œuvre.

Question : Est-ce que mes collaborateurs seront autonomes en cas de problèmes ?

Réponse : oui. Le Pack EIM, proposé par NoToS, intègre une phase de formation afin que vos collaborateurs maitrisent tous les aspects de l'EIM et du SSO. De plus, nous vous assistons pour la mise en place d'un ensemble de procédures (sauvegarde, passage en mode dégradé (sans SSO), création d'un utilisateur, déploiement d'un poste client…).

Question : Pourquoi faut-il une phase d'analyse ?

Réponse : pour pouvoir fonctionner correctement, les applications et les serveurs concernés par l'EIM doivent être configurés de manière précise. Les versions des systèmes d'exploitation (Serveur Microsoft, OS/400, Windows) et des logiciels (Client Access Express) doivent être vérifiées afin de prévenir toute incompatibilité. La configuration des différentes fonctions de TCP/IP (tout ce qui concerne le nommage, notamment) doit être vérifiée.



Le Pack EIM : un ensemble de prestations pour bénéficier d'un SSO « clé en main »

Aucune licence n'est à acquérir. Tous les produits nécessaires sont livrés en standard !

IBM AS/400, iSeries et maintenant i5 : plusieurs noms pour un système départemental assurant une des meilleures sécurité du marché

NoToS

32, chemin Notre Dame
34160 BEAULIEU

Téléphone : 04 67 86 09 08
Portable : 06 30 17 02 55
Messagerie : dgayte@notos.fr

www.notos.fr

Le Pack EIM

Le déploiement complet de votre SSO

Solution clé en main comprenant :

- **L'analyse de l'organisation en place et la vérification des pré-requis**
- **La mise en œuvre de l'EIM pour un AS/400**
- **La création des comptes dans l'Active Directory**
- **La formation du Service Informatique**
- **La configuration des postes clients types et le transfert de compétence**
- **L'assistance à la mise en place des procédures essentielles (sauvegardes, mode dégradé, création d'utilisateurs…)**
- **Tests et recette**

NoToS c'est aussi :

- toutes les prestations autour de l'**AS/400** (iSeries) :
  - Audit et conseil
  - Formation
  - Développement
- La fourniture et la mise en œuvre de solutions **Microsoft**
  - Serveurs : 2003 serveur, 2003 SBS, SQL Server, Exchange…
  - Bureautique (Office 2007)
  - Intranet (SharePoint)
  - Gestion de la Relation Client (Dynamics CRM)
  - Décisionnel (BI) autour de SQL Server 2005

Microsoft Spécialiste PME

IBM Partenaire Commercial