Solutions de gestion de la sécurité
Livre blanc

Tivoli software

L'intégration de la gestion des identités et des accès avec l'authentification unique
Objectif : Renforcer la politique de sécurité et améliorer la productivité des utilisateurs

Avril 2006

ON DEMAND BUSINESS™

Sommaire

Présentation

Beaucoup d'entreprises recherchent une solution complète de gestion des identités incluant un service d'authentification unique. IBM vous aide dans cette démarche et vous propose ses logiciels leader sur le marché : IBM Tivoli® Identity Manager et IBM Tivoli Access Manager for Enterprise Single Sign-On.

- *IIBM Tivoli Identity Manager* est une solution de gestion des identités et des habilitations automatisant le processus (workflow) de gestion des comptes utilisateurs, depuis leur création jusqu'à leur suppression. IBM Tivoli Identity Manager augmente ainsi l'efficacité des utilisateurs et des équipes de support, en particulier il réduit le nombre d'appels au « Help Desk », simplifie la production des rapports pour les audits et permet d'être conforme aux législations en matière d'accès et d'autorisations à des applications.
- *IBM Tivoli Access Manager for Enterprise Single Sign-On* permet aux entreprises de renforcer leur politique de gestion des identités, des habilitations et des accès en offrant un service d'authentification unique à la fois simple et puissant. En outre, IBM Tivoli Access Manager for Enterprise Single Sign-On permet aux entreprises d'augmenter leur productivité en limitant l'implication des utilisateurs sur le sujet toujours difficile des mots de passe ; il les aide également à réduire le coût des appels au support pour réinitialiser les mots de passe et renforce de fait la sécurité au niveau des postes de travail.
  Ce produit est une aide indéniable pour combattre et éliminer le phénomène bien connu en entreprise de « gestion laxiste ou peu rigoureuse » des mots de passe par les utilisateurs (Post It sur l'écran, mot de passe dits faibles, réutilisation rapide des mêmes chaînes de caractères, etc.).
- *L'adaptateur d'allocation des comptes IBM Tivoli Access Manager for Enterprise Single Sign-On Provisioning Adapter* permet aux entreprises d'intégrer les deux sujets : la gestion de l'identité et celle de l'authentification. Cet adaptateur étend les fonctionnalités d'IBM Tivoli Access Manager for Enterprise Single Sign-On en intégrant directement les informations d'identification depuis IBM Tivoli Identity Manager vers IBM Tivoli Access Manager for Enterprise Single Sign-On. L'intégration de ces deux logiciels évite aux utilisateurs finaux de s'identifier ou même de voir ou de connaître les informations nécessaires pour accéder aux applications (login, mots de passe). Ces derniers sont en effet choisis automatiquement en fonction des politiques de sécurité, configurés et renseignés automatiquement via le produit IBM Tivoli Identity Manager lors de la création du compte utilisateur.

Ce livre blanc propose une description de l'adaptateur IBM Tivoli Access Manager for Enterprise Single Sign-On Provisioning Adapter. Il décrit les étapes de son intégration à IBM Tivoli Identity Manager et à IBM Tivoli Access Manager for Enterprise Single Sign-On. Par ailleurs, il propose une description du déploiement et de l'administration de l'adaptateur.

En quelques mots

Une solution qui s'adapte aux entreprises de toutes tailles

Faire confiance à une solution d'authentification unique et éprouvée

Le logiciel IBM Tivoli Access Manager for Enterprise Single Sign-On est une solution d'entreprise d'authentification unique, leader sur le marché, et s'appuyant sur la technologie Passlogix. Plus de deux millions d'utilisateurs et 200 sites clients, dont le plus grand site de déploiement actuel au monde, utilisent les technologies de Passlogix. En effet, les services postaux des Etats-Unis ont eu recours à ce logiciel afin de déployer, en seulement huit mois, l'authentification unique pour 7 000 applications et 165 000 utilisateurs.

IBM Tivoli Access Manager for Enterprise Single Sign-On supporte de manière sécurisée :

- Tout type de méthode d'authentification des utilisateurs (connexion Microsoft Windows, cartes à puce, données biométriques, jetons, etc.)
- Tout type d'application d'entreprise (client/serveur, Java, Web, site central, développement interne)
- Tout type d'infrastructure d'entreprise : répertoire, base de données, partage de fichiers en réseau, etc.
- Tout type d'accès : par poste de travail fixe ou mobile, hors ligne, kiosques ou postes de travail partagés (utilisé par exemple dans le monde hospitalier).

IBM Tivoli Access Manager for Enterprise Single Sign-On est destiné à compléter IBM Tivoli Access Manager for e-business. IBM Tivoli Access Manager for Enterprise Single Sign-On offre la fonction d'authentification unique en rejouant de manière automatique et sécurisée les informations d'identification à la place de l'utilisateur. IBM Tivoli Access Manager for e-business supporte de nombreuses méthodes d'authentification pour le Web et va en particulier prendre en charge la gestion des accès en fonction des rôles et des groupes des utilisateurs. Point intéressant : Les deux produits partagent le même annuaire pour que l'utilisateur ne soit identifié qu'une seule fois.

En quelques mots

L'authentification unique de l'utilisateur dès sa prise de fonction

Automatiser l'allocation et la suppression des comptes tout en facilitant les audits

Dans de nombreuses entreprises, qu'elles soient grandes ou petites, les utilisateurs doivent gérer parfois eux-mêmes des dizaines d'identifiants et de mots de passe pour accéder à leurs applications. Cette gestion nécessite très souvent de choisir, saisir et surtout mémoriser toutes les informations d'identification – parfois complexes – pour chaque application ou système d'exploitation. De plus, lors de l'arrivée d'un nouvel employé dans l'entreprise, cette charge de travail augmente encore d'un facteur non négligeable, sans oublier les situations ou l'employé doit changer de droits lors de modifications de responsabilité ou de fonction.

Si une entreprise utilise l'adaptateur IBM Tivoli Access Manager for Enterprise Single Sign-On Provisioning Adapter, l'allocation et la suppression des informations d'identification pour les différentes applications sont automatisées entre IBM Tivoli Identity Manager et IBM Tivoli Access Manager for Enterprise Single Sign-On. Ainsi, il n'est plus nécessaire de demander aux utilisateurs finaux de saisir eux-mêmes les informations d'identification dans IBM Tivoli Access Manager for Enterprise Single Sign-On. Ce sont les administrateurs qui créent, éditent et suppriment les informations d'identification des utilisateurs à l'aide d'IBM Tivoli Identity Manager. Les utilisateurs finaux peuvent donc bénéficier de l'authentification unique très rapidement et n'ont plus à mémoriser leurs informations d'identification, ce qui garantit ainsi une sécurité plus élevée.

Lorsqu'un utilisateur final n'a plus besoin d'accéder aux systèmes, l'intégration permet à IBM Tivoli Identity Manager d'interdire l'accès de cet utilisateur aux applications et systèmes et également de supprimer automatiquement les informations d'identification gérées au niveau d'IBM Tivoli Access Manager for Enterprise Single Sign-On.
La maîtrise du bon niveau d'accès augmente la sécurité et la conformité et permet de démontrer le respect des règles internes aux auditeurs.

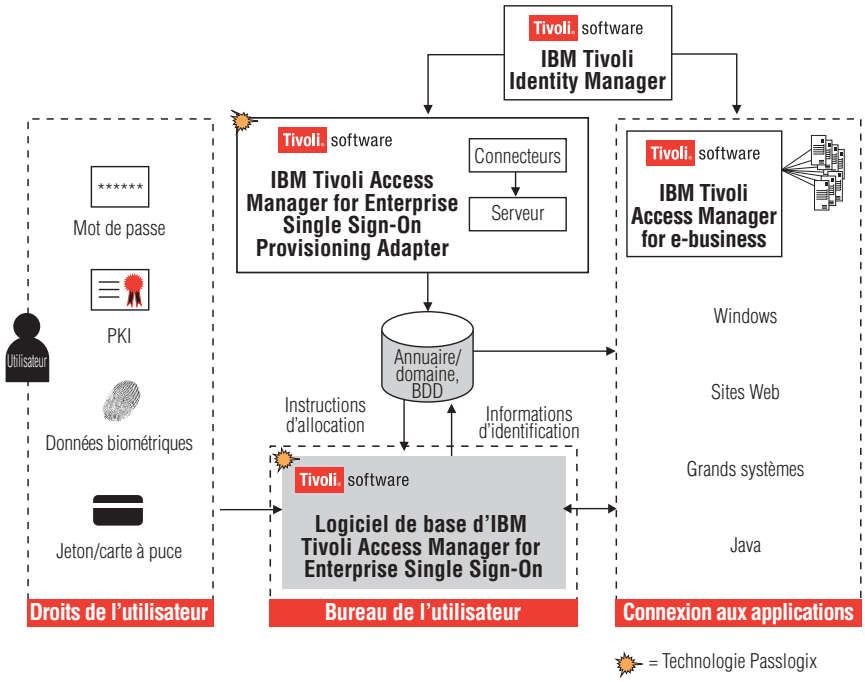
En outre, IBM Tivoli Access Manager for Enterprise Single Sign-On Provisioning Adapter apporte aux administrateurs un meilleur niveau de pilotage. Par exemple, lorsque les mots de passe des applications sont réinitialisés via IBM Tivoli Identity Manager, ceux de Tivoli Access Manager for Enterprise Single Sign-On le sont aussi, ce qui garantit leur validité permanente. Par ailleurs, les capacités d'audit et de création de rapports exploitent maintenant les informations sur les usages stockées dans IBM Tivoli Access Manager for Enterprise Single Sign-On. Les administrateurs peuvent par ailleurs utiliser l'adaptateur afin de consulter une liste de tous les utilisateurs ayant accès à une application ou, à l'inverse, consulter la liste de toutes les applications auxquelles un utilisateur a accès.

Comprendre les principales fonctionnalités du logiciel

Lorsque IBM Tivoli Access Manager for Enterprise Single Sign-On Provisioning Adapter reçoit des demandes d'IBM Tivoli Identity Manager, il informe les agents d'IBM Tivoli Access Manager for Enterprise Single Sign-On afin que ces derniers exécutent les changements, les ajouts ou les suppressions à faire sur les différentes configurations d'applications :

- en normalisant les instructions dans un format compris par Tivoli Access Manager for Enterprise Single Sign-On.
- en mettant à jour les informations de l'utilisateur concerné.

Lorsque IBM Tivoli Access Manager for Enterprise Single Sign-On se synchronise avec la base de données ou l'annuaire approprié, il lit et traite les demandes en mettant à jour son cache local d'informations d'identification. En fonction des demandes reçues, IBM Tivoli Access Manager for Enterprise Single Sign-On ajoute, modifie ou supprime les informations d'identification dans le cache local de l'utilisateur concerné. Enfin, IBM Tivoli Access Manager for Enterprise Single Sign-On synchronise à nouveau les informations d'identification avec la base de données ou l'annuaire de l'utilisateur concerné.



Architecture de l'application IBM Tivoli Access Manager for Enterprise Single Sign-On Provisioning Adapter

L'adaptateur IBM Tivoli Access Manager for Enterprise Single Sign-On Provisioning Adapter se compose d'un serveur, d'une console, d'une interface CLI et d'un connecteur.

- Le serveur reçoit les informations d'allocation des comptes via une interface Web. Il communique ces informations aux clients d'IBM Tivoli Access Manager for Enterprise Single Sign-On en mettant à jour les référentiels des applications.
- La console est l'interface graphique d'administration Web pour communiquer avec le serveur.
- L'interface de ligne de commande permet aux applications et aux administrateurs de communiquer avec le serveur.
- Le connecteur réalise l'intégration entre le serveur et IBM Tivoli Identity Manager via l'interface de ligne de commande. Le connecteur est une bibliothèque Java qui est mise en œuvre comme une extension workflow et qui peut s'intégrer à n'importe quelle opération d'allocation d'IBM Tivoli Identity Manager. Les administrateurs peuvent donc, via l'interface d'IBM Tivoli Identity Manager, ajouter, éditer ou supprimer les informations d'identification des applications pour les utilisateurs finaux. Le connecteur fonctionne sur n'importe quelle plateforme sur laquelle est installé IBM Tivoli Identity Manager.

En quelques mots

Intégrer l'application en fonction de votre déploiement d'IBM Tivoli Identity Manager

Comment intégrer identité et authentification unique

Le connecteur d'IBM Tivoli Access Manager for Enterprise Single Sign-On Provisioning Adapter fonctionne impérativement sur un PC sous Windows. Il est toutefois possible de procéder à l'intégration de deux façons :

- Si IBM Tivoli Identity Manager est également installé sur un PC sous Windows, il est possible d'utiliser une bibliothèque locale de classes, fournie avec le produit, afin de communiquer avec IBM Tivoli Access Manager for Enterprise Single Sign-On Provisioning Adapter.
- Si IBM Tivoli Identity Manager est installé sur un PC sans Windows, avec prise en charge d'un client Java, il suffit d'installer un client RMI *(Remote Method Invocation)* qui appellera à distance le connecteur.

Le connecteur met actuellement à disposition les opérations suivantes :

- ChangePasslogixPassword (changement du mot de passe)
- AddPasslogixCredential (ajout des informations d'identification)
- DeletePasslogixCredential (suppression des informations d'identification)
- ModifyPasslogixCredential (modification des informations d'identification)

Respectez les étapes qui suivent afin d'activer l'intégration :

1. Activez le service de demande d'allocation des ressources d'IBM Tivoli Identity Manager.
2. Copiez le connecteur approprié dans le répertoire d'IBM Tivoli Identity Manager.
3. Référencez ensuite le connecteur dans IBM Tivoli Identity Manager.
4. Créez un fichier de configuration pour ce connecteur. Ce fichier doit indiquer l'URL et les informations d'identification qui permettent d'accéder au serveur d'IBM Tivoli Access Manager for Enterprise Single Sign-On Provisioning Adapter.
5. Mettez à jour le schéma de données d'IBM Tivoli Identity Manager.
6. Si vous utilisez le connecteur RMI, démarrez le serveur RMI qui détectera les requêtes du client RMI.
7. Etendez l'interface regroupant les opérations IBM Tivoli Identity Manager afin de pouvoir appeler Tivoli Access Manager for Enterprise Single Sign-On Provisioning Adapter.
8. Configurez les services d'IBM Tivoli Identity Manager pour synchronisation avec IBM Tivoli Access Manager for Enterprise Single Sign-On Provisioning Adapter.

En quelques mots

Envoyer des requêtes d'allocation des comptes de façon transparente

Une fois la dernière étape réalisée, les demandes d'allocation des comptes transmettent de façon transparente les requêtes à l'adaptateur par une ligne de commande avec les arguments corrects. Cette intégration permet à IBM Tivoli Identity Manager de synchroniser les informations d'identification gérées par IBM Tivoli Access Manager for Enterprise Single Sign-On avec celles des différentes applications.

Piloter avec une console d'administration simple

L'adaptateur IBM Tivoli Access Manager for Enterprise Single Sign-On Provisioning Adapter est administré via une simple console Web. Cette console accepte les demandes externes d'allocation des comptes et les transmet à IBM Tivoli Access Manager for Enterprise Single Sign-On pour traitement. Ce dernier traite ensuite ces demandes en ajoutant, modifiant ou supprimant les propriétés identifiant les utilisateurs.

Cette console d'administration permet aussi aux équipes de générer des rapports sur les créations de nouveaux comptes, les réinitialisations de mots de passe et les suppressions d'accès à un compte.

Les fonctionnalités de base d'IBM Tivoli Access Manager for Enterprise Single Sign-On Provisioning Adapter peuvent être exécutées et administrées via la console, mais aussi via une source externe, comme la console d'administration de Tivoli Identity Manager. Elles peuvent également être administrées en mode manuel via l'interface ligne de commande.

En quelques mots

Générer des rapports pour les vérifications de conformité (audits)

Faciliter les audits grâce à des fonctions de consignation des événements et de création de rapports

IBM Tivoli Access Manager for Enterprise Single Sign-On Provisioning Adapter peut détecter, enregistrer et produire des rapports sur des événements spécifiques sur demande de l'administrateur. Le logiciel peut générer plusieurs rapports d'audit comme par exemple :

- la liste de tous les utilisateurs qui ont une application spécifique configurée dans IBM Tivoli Access Manager for Enterprise Single Sign-On ;
- la liste de toutes les applications configurées dans IBM Tivoli Access Manager for Enterprise Single Sign-On pour un utilisateur spécifique ;
- la liste de toutes les requêtes d'allocation des comptes ;
- la liste des ressources applicatives utilisées par les utilisateurs.

Pour analyser le journal des événements, exportez-le simplement dans un fichier CSV puis importez ce fichier dans n'importe quel outil d'analyse capable de lire ce format.

Conclusion

Avec IBM Tivoli Identity Manager, Tivoli Access Manager for Enterprise Single Sign-On et Tivoli Access Manager for Enterprise Single Sign-On Provisioning Adapter, les administrateurs peuvent pré-remplir ou supprimer les informations d'identification des utilisateurs stockées dans Tivoli Access Manager for Enterprise Single Sign-On. De cette manière, les utilisateurs n'ont jamais à modifier ou même à connaître les informations d'identification de leurs applications.

L'intégration de Tivoli Identity Manager et de Tivoli Access Manager for Enterprise Single Sign-On via Tivoli Access Manager for Enterprise Single Sign-On Provisioning Adapter aide les entreprises à :

- augmenter leur productivité en évitant aux utilisateurs finaux de connaître leurs mots de passe ;
- renforcer la sécurité et faciliter le respect de la conformité aux règles de sécurité en supprimant automatiquement les droits d'accès et les informations d'identification lorsque l'utilisateur final n'en a plus l'utilité ;
- diminuer de manière conséquente les coûts de support liés aux mots de passe en évitant aux utilisateurs de saisir manuellement leurs informations d'identification lorsque ces informations doivent être réinitialisées ou fournies sur requête ;
- réduire les coûts en permettant aux employés de réinitialiser eux-mêmes leurs propres mots de passe.

Les logiciels Tivoli d'IBM

Grâce aux logiciels Tivoli d'IBM, les entreprises peuvent gérer de manière efficace et rentable les ressources, les tâches et les processus informatiques pour répondre à des exigences économiques en permanente évolution et offrir une gestion des services informatiques flexible et réactive, tout en réduisant les coûts. Les produits Tivoli couvrent les domaines de la sécurité, de la disponibilité, du stockage, de la conformité, des performances, de la gestion de configuration, de l'exploitation et de la gestion du cycle de vie des applications informatiques. Ils bénéficient de la qualité de support, de la recherche et des services IBM.

Pour plus d'informations

IBM Tivoli Access Manager for Enterprise Single Sign-On Provisioning Adapter intègre IBM Tivoli Identity Manager et Tivoli Access Manager for Enterprise Single Sign-On afin de simplifier et de sécuriser les processus d'identification et d'allocation des comptes pour les utilisateurs finaux. Ce logiciel aide les utilisateurs à avancer dans leur démarche de gestion des identités et de respect de la conformité.

Pour en savoir plus sur IBM Tivoli Access Manager for Enterprise Single Sign-On, appelez votre agent commercial ou votre partenaire commercial IBM, ou bien consultez le site **ibm.com**/tivoli

IBM Corporation
Software Group
Route 100
Somers, NY 10589
U.S.A.

Produit aux Etats-Unis d'Amérique
4-06

GC28-8425-FRA-00