

Gérer efficacement les identités pour accroître la productivité des administrateurs et des utilisateurs, tout en facilitant les initiatives de conformité.



Points forts

- Centralise et automatise les tâches répétitives de gestion du cycle de vie des identités pour accroître la productivité, applique des règles de sécurité de façon cohérente et simplifie les processus d'audit
- Applique des règles d'évaluation de façon cohérente, centralise la collecte des données d'audit et permet la connexion unique dans l'entreprise
- Rationalise la gestion des identités dans les limites organisationnelles et de l'entreprise, à l'aide de produits et services de fédération d'identités

Les tâches coûteuses en temps associées à la gestion d'identités détournent constamment les administrateurs et le personnel informatique de votre entreprise d'initiatives à haute valeur ajoutée, en faveur de l'innovation.

Par exemple, les accords de niveau de service (SLA), les exigences légales et les règles internes peuvent solliciter très fortement les processus de gestion des identités d'utilisateur. Vous devez effectuer un suivi du cycle de vie de chaque identité d'utilisateur : Quand le compte a-t-il été créé ? Quand l'utilisateur a-t-il eu accès à chaque service ou application au sein de votre entreprise ? Qui a approuvé la

création du compte ? Quelle modification le compte a-t-il subi ? La collecte manuelle de ces informations et d'autres types de données sur tous les nœuds finals gérés par votre équipe peut nécessiter beaucoup de temps et de ressources. Sans un certain niveau d'automatisation et de répétabilité, la collecte des informations d'identité devient un nouveau projet chaque fois que des rapports s'avèrent nécessaires pour des audits internes et externes.

Pensez également aux gains de productivité possibles en matière de gestion de mots de passe et de création de comptes. Compte tenu qu'un pourcentage élevé des appels au



centre d'assistance concerne la réinitialisation de mots de passe, il a été estimé que la réinitialisation manuelle des mots de passe représente jusqu'à 40 % des coûts d'assistance.* Outre le temps utilisé par les administrateurs, qui pourraient sinon se concentrer sur des activités plus stratégiques, les utilisateurs qui demandent une réinitialisation de leur mot de passe n'ont pas accès aux ressources nécessaires pour être productifs. Lorsque des utilisateurs sont dans l'attente d'un nouveau compte, un approvisionnement rapide est essentiel à la productivité.

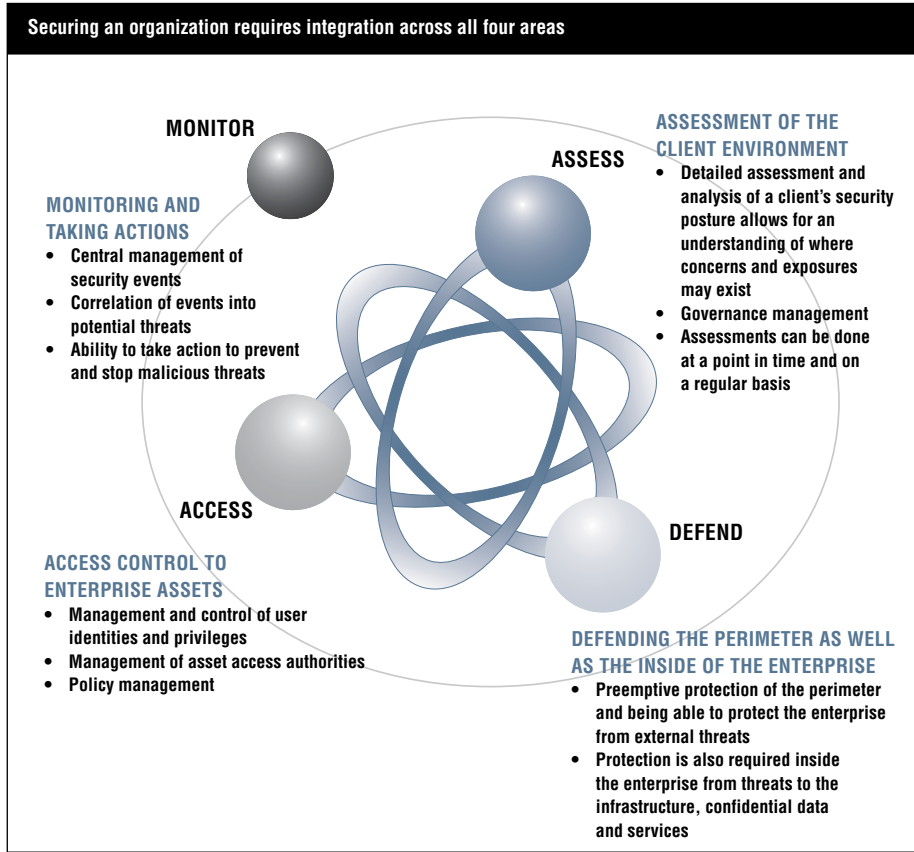
Pour aider à optimiser les efforts de sécurité, de productivité, d'audit et de conformité, IBM propose une large gamme de solutions de gestion d'identités (systèmes, logiciels et services, plus financement) qui aident les entreprises à maîtriser les menaces informatiques. La gestion centralisée et rationalisée des identités est l'un des nombreux composants des solutions de sécurité IBM, qui aident les clients à mettre en place des stratégies efficaces de gestion des

risques afin de gérer et sécuriser les informations et les technologies de leur entreprise, d'anticiper les vulnérabilités et les risques et de maintenir un accès rapide aux informations. Les solutions de sécurité IBM aident les entreprises à adapter la technologie à leurs priorités et à rediriger les ressources susceptibles d'être affectées à la résolution des problèmes de sécurité vers des initiatives qui augmentent la valeur novatrice, stratégique et substantielle de leur activité.

Les chapitres suivants décrivent comment les solutions IBM aident les entreprises à gérer et automatiser de façon centralisée la gestion du cycle de vie des identités, à accéder à une fédération des identités et des contrôles dans l'entreprise, depuis le système central jusqu'au poste de travail.

Rationaliser l'approvisionnement d'identités et permettre une maintenance par l'utilisateur

L'administration manuelle des identités entraîne fréquemment des opérations



vos besoins d'entreprise. Les moteurs d'approvisionnement et de workflow intégrés à IBM Tivoli® Identity Manager permettent de rationaliser la soumission et l'approbation des demandes d'utilisateur et d'appliquer vos règles de sécurité de manière cohérente. Conjointement à vos plates-formes existantes, sur des environnements mainframe et distribués, Tivoli Identity Manager vous aide à centraliser la définition des utilisateurs et l'approvisionnement de services utilisateur afin de minimiser les erreurs et les incohérences.

Tout en centralisant l'administration pour exécuter vos meilleures pratiques de manière cohérente, le logiciel propose également un modèle d'administration souple, de sorte que vous pouvez déléguer des privilèges administratifs de façon appropriée. Les gestionnaires de groupes utilisés pour l'accès peuvent contrôler leurs propres groupes et le serveur central de Tivoli Identity Manager synchronise leurs modifications et vérifie les éventuelles non-conformités.

lentes et incohérentes. Il est facile pour un administrateur de manquer une attribution groupée, notamment lorsqu'il doit gérer de nombreux comptes dont les privilèges changent très souvent. De nombreuses entreprises considèrent également qu'elles possèdent trop de comptes orphelins, un sous-produit issu

d'une administration manuelle et qui engendre un risque inutile.

Pour vous aider à relever ces défis, IBM propose des outils et services de gestion du cycle de vie des identités qui permettent d'automatiser les tâches répétitives conformément à

Enrichir les solutions en puisant dans les composants de base des identités

Pour aider les sociétés dans l'intégration de leurs annuaires et leurs besoins en workflow, IBM propose IBM Tivoli Directory Server et IBM Tivoli Directory Integrator. Ces produits se combinent souvent avec les autres solutions de gestion des identités décrites dans ce document pour fournir une base extensible, basée sur des normes, pour stocker et synchroniser les diverses sources de données d'identité utilisateur au sein de votre entreprise. Grâce à Tivoli Directory Server et Tivoli Directory Integrator, vous pouvez gérer les identités de manière cohérente et avec une grande souplesse. De plus, Tivoli Directory Integrator permet une intégration au niveau de l'objet de données au-delà des identités utilisateur. Son architecture Java™ ouverte et son ensemble complet de gestionnaires de technologie vous aident à rationaliser et atténuer le risque lié à l'intégration de données personnalisées préparées à l'avance.

Par ailleurs, Tivoli Identity Manager comprend des fonctions de maintenance personnelle qui permettent aux utilisateurs finals de réinitialiser et de synchroniser eux-mêmes leurs mots de passe, conformément à vos règles. Par conséquent, le produit vous aide à optimiser la sécurité et votre personnel informatique est libéré des fonctions administratives pour se consacrer à des activités plus stratégiques.

Tivoli Identity Manager vous aide également à réduire le temps nécessaire pour répondre aux demandes d'audits et à la consultation manuelle des règles. S'appuyant sur ses pistes d'audit centralisées dans vos systèmes d'information clés, il peut rapidement créer des rapports standard centralisés concernant des règles de sécurité, des droits d'accès actuels ou des événements d'audit. Vous pouvez utiliser ces informations non seulement pour répondre à des audits, mais aussi pour adopter une approche de conformité plus proactive.

Les solutions IBM d'Identity and Access Management Services offrent une assistance en implémentant, en déployant et en gérant des solutions de gestion d'identités intégrées. Si vous avez besoin d'identifier les carences de vos processus de gestion d'identités actuels, de trouver un hôte pour des services d'approvisionnement, d'identification et de rapport, ou tout

autre service associé, les solutions IBM d'Identity and Access Management Services vous assistent dans toutes les phases de la gestion du cycle de vie des identités. Quelques exemples :

- Stratégie et évaluation d'identités
- Vérification d'identités
- Gestion du cycle de vie des identités
- Service d'annuaires
- Gestion d'accès
- Solutions d'authentification performantes

Les solutions IBM d'Identity and Access Management Services s'appuient non seulement sur des solutions IBM efficaces, mais également sur les principales technologies des partenaires commerciaux IBM, afin de fournir les fonctions de gestion d'identités dont votre entreprise a besoin.

Faciliter l'audit et offrir une connexion unique

Si la gestion du cycle de vie des identités est importante pour un accès efficace basé sur des rôles, IBM propose également des solutions de contrôle d'accès éprouvées qui vous aident à appliquer les droits d'accès, les règles de mot de passe et les règles de gestion d'informations que vous avez définies. Ces solutions facilitent les efforts de conformité, en maintenant des pistes d'audit centralisées pour les demandes d'accès, tout en permettant à vos administrateurs et aux utilisateurs d'être plus productifs.

IBM Tivoli Access Manager for e-business fournit un point d'autorisation unique pour les applications Web et vous aide à surmonter les difficultés de l'implémentation de règles de sécurité sur une large gamme de ressources Web et d'application. Ainsi, avec cohérence, vous fournissez à vos collaborateurs, partenaires, fournisseurs et clients un accès basé sur des rôles aux informations et aux services dont ils ont besoin.

Pour aider à rationaliser les efforts et répondre aux demandes d'audit, Tivoli Access Manager for e-business centralise la collecte et les rapports relatifs aux audits, journaux, statistiques et d'autres informations sur une entreprise répartie. De plus, il rédige des enregistrements d'audit au format XML standard, facilement analysables pour extraire les informations dont vous ou vos auditeurs ont besoin.

Le logiciel Tivoli Access Manager prend en charge plusieurs techniques d'authentification efficaces. En combinaison avec IBM Tivoli Federated Identity Manager, Tivoli Access Manager for e-business est fourni avec 30 rapports prêts à utiliser pour couvrir les domaines les plus utiles aux utilisateurs.

Du point de vue de vos utilisateurs finals, le logiciel de contrôle d'accès d'IBM propose un mécanisme d'accès cohérent, qui permet d'augmenter la productivité. Tivoli Access Manager for e-business offre aux utilisateurs finals la capacité d'utiliser une identité unique pour accéder à de nombreuses ressources par la prise en charge

Les solutions de gestion d'identités IBM comprennent :

Gestion du cycle de vie des identités

- Tivoli Identity Manager
- Tivoli Identity Manager Express

Contrôle d'accès

- Tivoli Access Manager for e-business
- Tivoli Access Manager for Operating Systems
- Tivoli Access Manager for Enterprise Single Sign-On

Fédération d'identités

- Tivoli Federated Identity Manager
- Tivoli Federated Identity Manager Business Gateway

IBM Identity and Access Management Services

du protocole SPNEGO (Simple and Protected GSSAPI Negotiation Mechanism).

IBM Tivoli Access Manager for Enterprise Single Sign-On permet aux utilisateurs de se connecter une seule fois pour accéder aux applications et services de votre entreprise. Le besoin d'effectuer uniquement un suivi d'une seule identité et d'un seul mot de passe simplifie non seulement la vie de l'utilisateur, mais aide également à réduire la perte de mots de passe (et la perte associée de productivité pour les utilisateurs et le personnel informatique) et à minimiser les vulnérabilités de sécurité liées aux mots de passe conservés dans des endroits non sécurisés.

IBM Identity and Access Management Services peut vous aider à concevoir, implémenter, déployer et gérer des solutions de contrôle d'accès. Par exemple, IBM Identity and Access Management Services peut vous aider à définir et traiter vos exigences en matière de connexion unique, d'authentification (y compris authentification multifactorielle) et d'accès physique et logique.

Partager l'authentification des utilisateurs et attribuer des informations entre des personnes autorisées et des applications de services Web

Aujourd'hui, les entreprises souhaitent toujours plus partager les informations d'identité avec des personnes autorisées, telles que des partenaires extérieurs ou des unités commerciales internes. Les entreprises qui procèdent ainsi améliorent et simplifient grandement la vie des utilisateurs. Ce concept, appelé fédération d'identités, permet également d'optimiser la sécurité pour la plupart des services d'entreprise complexes, tout en minimisant le besoin de gestion de sécurité par votre département informatique.

Tivoli Federated Identity Manager vous permet d'utiliser les normes de fédération les plus répandues, pour fournir un accès aux identités d'utilisateur gérées par une entreprise autorisée. Ainsi, vous pouvez plus facilement développer des services tiers à proposer à d'autres entreprises et vous permettez à vos propres utilisateurs de bénéficier



des services tiers, sans les contraindre à naviguer entre des sites de fédération. Au sein d'une entreprise, Tivoli Federated Identity Manager vous aide à sécuriser les transactions utilisant la technologie de services Web et SOA sur des environnements centraux et répartis. Pour les petites et moyennes entreprises, IBM Tivoli Federated Identity Manager Business Gateway est le point de départ idéal pour mettre en place une solution de connexion unique fédérée.

Avec le logiciel Tivoli Federated Identity Manager, vous pouvez accorder un accès basé sur des rôles à vos utilisateurs et leur permettre de passer moins de temps à se connecter à différents environnements ou unités, et être ainsi plus productifs. Vous pouvez également utiliser IBM Identity and Access Management Services pour développer et/ou implémenter la solution de fédération d'identités qui est adaptée à votre entreprise.

Pour en savoir plus

Pour en savoir plus sur la manière dont votre entreprise peut utiliser les solutions de sécurité IBM afin de mieux gérer les identités d'utilisateur et ainsi augmenter la sécurité et la productivité, ou bien pour trouver le point de départ des solutions de sécurité IBM qui correspond le mieux à votre entreprise, contactez votre représentant ou partenaire commercial IBM ou visitez le site ibm.com/itsolutions/security

A propos des solutions IBM pour faciliter la gouvernance informatique et la gestion des risques

IBM permet aux départements informatiques de prendre en charge la gouvernance et la gestion des risques en adaptant les règles, processus et projets informatiques aux objectifs de l'entreprise. Les entreprises peuvent s'appuyer sur les services, les logiciels et les équipements IBM pour planifier, exécuter et gérer des initiatives de gestion de services informatiques, de récupération et de sécurité au sein de l'entreprise. Des entreprises de toutes tailles peuvent bénéficier des solutions IBM souples et modulaires, couvrant la gestion d'entreprise, le déploiement informatique et les opérations informatiques et s'appuyant sur une expérience client étendue, les meilleures pratiques et une technologie basée sur des normes ouvertes. IBM aide les clients à implémenter les bonnes solutions informatiques pour obtenir des résultats commerciaux rapides et devenir des partenaires stratégiques dans le développement d'activité. Pour en savoir plus sur la gestion des risques et la gouvernance IBM, visitez le site ibm.com/itsolutions/governance

© Copyright IBM Corporation 2007

IBM Corporation
Route 100
Somers, NY 10589
Etats-Unis

Produit aux Etats-Unis

3-07

Tous droits réservés

IBM, le logo IBM et Tivoli sont des marques d'International Business Machines Corporation aux Etats-Unis et/ou dans certains autres pays.

Java et toutes les marques incluant Java sont des marques de Sun Microsystems, Inc. aux Etats-Unis et/ou dans certains autres pays.

Les autres noms de sociétés, de produits ou de services peuvent appartenir à des tiers.

Exclusion de garantie : Il revient au client de garantir la conformité aux exigences légales. Il est de l'unique responsabilité du client d'obtenir des conseils auprès de juristes compétents quant à l'identification et l'interprétation de toute loi et exigence réglementaire pertinente, susceptible d'affecter l'entreprise du client et toutes les mesures que le lecteur pourrait être amené à prendre pour se conformer auxdites lois. IBM ne fournit ni conseil, ni représentation, ni attestation légale sur le fait que ses produits ou services garantiront que le client est en conformité avec toute loi ou réglementation pertinente.

*Maxine Holt, analyste en recherche, Butler Group, citation dans René Millman, "Avoiding an Identity Crisis," SC Magazine, 5 avril 2006.

scmagazine.com/uk/news/article/551843