Tivoli software

IBM Tivoli Access Manager for Enterprise Single Sign-On

En quelques mots

- Simplifie la tâche des utilisateurs en les déchargeant de l'obligation de mémoriser et de gérer informations d'identification : noms d'utilisateur, mots de passe, …
- Renforce la sécurité et évite la gestion laxiste des mots de passe.
- Diminue les coûts de support en réduisant le nombre d'appels liés à la réinitialisation des mots de passe.
- Répond aux exigences des réglementations en supprimant les accès inutiles et en gérant les données d'identification via une intégration étroite avec IBM Tivoli Identity Manager.
- Enrichit les fonctions d'autorisation et de gestion des droits de Tivoli Access Manager for e-business pour les applications Web en traitant l'identification unique entièrement au niveau du client.
- Complète les fonctions de Tivoli Access Manager for e-business en proposant des adaptateurs pour : les kiosques, les postes de travail partagés, les dispositifs d'authentification forte ou à niveaux multiples, l'automatisation de l'allocation des comptes et la réinitialisation des mots de passe à partir du poste de travail.
- Consolide et produit des rapports d'audit démontrant la conformité avec les règles de confidentialité et de sécurité.

Avec l'authentification unique, venez à bout du casse-tête des mots de passe

Le nombre et la complexité des connexions qu'un employé doit gérer chaque jour représentent une source de mécontentement et une perte de productivité croissantes. Dans la plupart des entreprises, les employés doivent mémoriser entre cinq et trente mots de passe, dont certains doivent être modifiés tous les mois. Le temps perdu à saisir, modifier, inscrire, oublier et réinitialiser les mots de passe semble mineur, mais il s'accumule au fil des jours et finit par représenter une part non négligeable du temps de travail des employés. De plus, lorsqu'un employé ne peut pas accéder à une application, il ne peut plus travailler, finit par perdre son temps et bloque souvent le travail de ses collègues.

D'autre part, le choix et la gestion laxistes des mots de passe par les employés représentent aujourd'hui un des principaux points faibles de la sécurité des entreprises. En effet, il arrive souvent que les employés notent leurs mots de passe dans des lieux peu sûrs, utilisent des mots de passe du type « mot_de_passe » ou bien communiquent leur mot de passe à des collègues pour parer au plus pressé ou débloquer une situation.

C'est pourquoi les entreprises souhaitent aujourd'hui déployer facilement une solution d'authentification unique simple, rapide pour l'ensemble de leurs applications tout en garantissant un maximum de sécurité et de productivité.

Le logiciel IBM Tivoli® Access Manager for Enterprise Single Sign-On, solution d'entreprise basée sur la technologie Passlogix®, leader sur le marché, répond parfaitement à ce besoin : les employés s'identifient une seule fois, puis le logiciel détecte tous les demandes d'identification liés au mot de passe et y réagit en automatisant chacune des tâches de gestion associées : connexion, choix, modification et réinitialisation du mot de passe.

Que vous soyez en train de déployer une solution d'authentification forte, de gérer des problèmes de conformité, de mettre en œuvre une solution de gestion des identités pour toute l'entreprise ou bien si, tout simplement, vous vous concentrez sur l'authentification unique pour un groupe d'utilisateurs, la suite IBM Tivoli Access Manager for Enterprise Single Sign-On peut répondre aux besoins de votre entreprise et satisfaire vos exigences techniques. IBM Tivoli Access Manager for Enterprise Single Sign-On vous aide à mettre en place une authentification unique pour vos applications, quel que soit leur environnement d'exécution :

- Microsoft® Windows®
- Client/serveur
- Web
- Java™
- Emulateurs d'hôtes : IBM AS/400® (5250), IBM OS/390® (3270) et UNIX® (telnet)
- Applications développées en interne
- Applications sur grands systèmes

Gérez vos mots de passe en toute sécurité
IBM Tivoli Access Manager for Enterprise Single Sign-On automatise la gestion des mots de passe et permet de réduire la vulnérabilité du système d'information. Trop souvent encore, les employés choisissent rapidement des mots de passe simples et n'hésitent pas à les écrire sur du papier ou coller parfois des Post It sur leurs machines.

Ce logiciel est conçu pour vous aider à mettre en place des politiques strictes de gestion de mots de passe, même si les applications utilisées au quotidien ne disposent pas de ce genre d'option. Vous pouvez par exemple paramétrer les longueurs minimale et maximale des chaînes de caractères de mots de passe, autoriser ou restreindre l'utilisation des caractères alphabétiques, numériques, spéciaux. Vous pouvez également restreindre l'utilisation des minuscules ou des majuscules, ou encore de certains caractères en début ou en fin de mot de passe. Enfin, il est possible d'exiger un changement de mot de passe à des fréquences fixées, etc.

Lors des interactions entre les différentes applications de votre entreprise (Web, client-serveurs, mainframe, applications réseau) IBM Tivoli Access Manager for Enterprise Single Sign-On peut détecter ou déclencher les changements de mot de passe nécessaires. Le logiciel peut aussi soulager les utilisateurs de la création, de la saisie et de la mémorisation des mots de passe (en leur permettant cependant à tout instant d'accéder à leurs mots de passe via des moyens appropriés si besoin est).

Que vos mots de passe et données soient stockés dans votre annuaire d'entreprise ou tout autre référentiel, en local sur vos disques ou sur un serveur, leur protection et leur intégrité sont assurées à tout instant. IBM Tivoli Access Manager for Enterprise Single Sign-On utilise des techniques de cryptographie parmi les plus avancées du marché, incluant les algorithmes de type DES (Triple Data Encryption Standard) et AES (Advanced Encryption Standard). La capacité du logiciel à s'adapter aux standards FIPS 140-2 (Federal Information Processing Standard) permet aux institutions financières ou médicales, aux administrations publiques et autres organisations de respecter rigoureusement les règles de confidentialité et de sécurité décrites dans ce standard.

IBM Tivoli Access Manager for Enterprise Single Sign-On est à la fois simple et efficace
Dans un environnement client/serveur ou à base de terminaux, IBM Tivoli Access Manager for Enterprise Single Sign-On assure l'authentification unique rapide en utilisant peu de ressources système. Le logiciel peut se connecter à n'importe quelle application, intercepter les demandes d'authentification ou rejouer de manière automatique les informations de connexion et cela, dans un délai inférieur à la seconde dans la plupart des cas.

De plus, le logiciel occupe peu d'espace mémoire (moins de 2,5 Mo) et ne consomme des ressources client ou réseau qu'en cas de demande de connexion, approche particulièrement intéressante pour les environnements client-serveur, Citrix, Sun et Windows Terminal Services.

Un déploiement et une gestion simplifiés
La mise en œuvre d'IBM Tivoli Access Manager for Enterprise Single Sign-On est facilitée par sa console d'administration intuitive, robuste et dotée d'assistants graphique. Cette console permet également d'intégrer le produit aux référentiels de type annuaire d'entreprise.

Votre administrateur réseau peut procéder au déploiement du logiciel côté client à partir d'un poste unique en utilisant IBM Tivoli Configuration Manager ou tout autre système de télédistribution, sans avoir à ajouter ni le matériel, ni de logiciel au réseau, et sans faire intervenir les utilisateurs lors du processus d'installation.

La console simplifie l'administration en reconnaissant et en configurant automatiquement les applications pour la connexion, avec intervention minimale de l'administrateur. A partir de la console d'administration (disponible depuis une console .NET ou depuis une console de gestion Windows MMC snap-in), les assistants graphiques guident l'administrateur dans la configuration, le déploiement et l'administration. IBM Tivoli Access Manager for Enterprise Single Sign-On est fourni avec des configurations type pour les applications de base. La console d'administration est également capable de configurer automatiquement le logiciel pour des applications qu'il n'a jamais rencontrées. En résumé, quelle que soit l'application sur laquelle on souhaite mettre en place l'authentification unique, aucun développement spécifique n'est nécessaire – tout se fait par paramétrage.

Lorsque le logiciel est installé, vous pouvez utiliser la console d'administration pour gérer les utilisateurs individuellement, par rôle ou bien par groupe. La console vous guide également dans la définition des politiques de gestion des mots de passe, des préférences utilisateur, des règles de ré-authentification.

L'élaboration de rapports d'activités est facilitée par la console d'administration. Elle vous permet de gérer l'enregistrement et la trace des événements et des activités : connexions utilisateurs, changements de mot de passe, authentification, choix ou modification des règles ou des politiques, etc. IBM Tivoli Access Manager for Enterprise Single Sign-On peut consigner ces activités dans un fichier XML, dans Windows Event Viewer ou bien via la méthode de votre choix en utilisant l'API de gestion des événements. Ainsi, vous pouvez générer des rapports d'audits sur les événements et l'activité des utilisateurs.

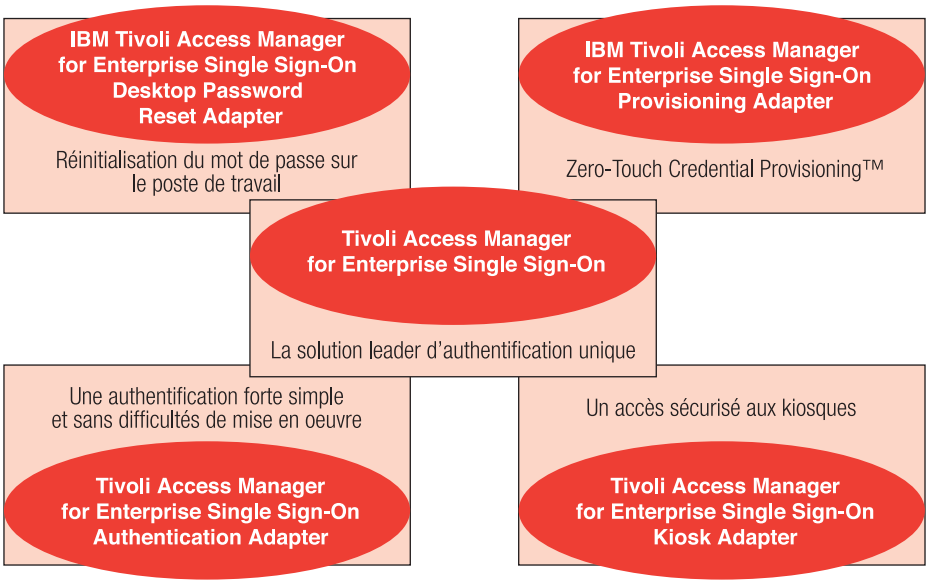
Exploitez les informations déjà stockées dans vos annuaires ou référentiels existants
IBM Tivoli Access Manager for Enterprise Single Sign-On peut stocker les informations d'authentification des utilisateurs ainsi que sa propre configuration système dans toute une gamme d'annuaires LDAP, dans des bases de données SQL telles qu'IBM DB2 Universal Database™, ou encore dans d'autres référentiels ou systèmes existants de stockage. L'utilisation d'un annuaire LDAP ou d'un autre référentiel propre à l'entreprise n'est pas une obligation lorsque l'on souhaite utiliser le produit IBM Tivoli Access Manager for Enterprise Single Sign-On. Cependant, les entreprises qui doivent administrer un grand nombre d'employés seront intéressées par les capacités d'intégration du produit avec les annuaires LDAP en place. Grâce à cette intégration, elles bénéficieront des capacités de création de rapports et de contrôle centralisés qu'un référentiel de type LDAP sait offrir.
Cette solution est capable par conséquent de s'appuyer et s'intégrer sur le référentiel en place. La configuration d'un référentiel ou d'un annuaire est en général très simple. IBM Tivoli Access Manager for

Enterprise Single Sign-On prend en charge les référentiels suivants (prise en charge totale, sauf indication contraire) :

- Les répertoires LDAP Version 2/Version 3 comme IBM Tivoli Directory Server, Sun Java System Directory Server, Novell eDirectory, Oracle Internet Directory
- Microsoft Active Directory® et Active Directory Application Mode (ADAM)
- Open LDAP (prise en charge de base)
- Critical Path (prise en charge de base)
- DB2® Universal Database
- Microsoft SQL Server
- Bases de données Oracle 9*i* et 10*g*
- Autres référentiels ou périphériques de stockage (en utilisant l'API de synchronisation)

IBM Tivoli Access Manager for Enterprise Single Sign-On est évolutif

IBM Tivoli Access Manager for Enterprise Single Sign-On est une solution d'entrée de gamme à laquelle peuvent s'ajouter plusieurs adaptateurs en option évolutifs (sans migration) et particulièrement intéressants pour certaines demandes spécifiques liées à la sécurité. Les options des adaptateurs de Tivoli Access Manager for Enterprise Single Sign-On assurent la prise en charge de scénarios additionnels qui vont de la réinitialisation des mots de passe à partir du poste de travail aux requêtes d'authentification multiple et à l'authentification forte. L'interface graphique de la console d'administration de ces adaptateurs simplifie les tâches de configuration, de déploiement, d'administration ainsi que le lancement d'audit et de génération de rapports évaluant la conformité.



Tivoli Access Manager for Enterprise Single Sign-On est un produit d'entrée de gamme disposant de quatre adaptateurs en option qui peuvent étendre dès que l'utilisateur le souhaite, sans migration et facilement, les fonctionnalités de base.

Les adaptateurs d'IBM Tivoli Access Manager for Enterprise Single Sign-On comprennent :

- *IIBM Tivoli Access Manager for Enterprise Single Sign-On Desktop Password Reset Adapter (adaptateur de réinitialisation du mot de passe)* permet aux utilisateurs finaux de réinitialiser leur mot de passe Windows depuis des postes de travail verrouillés et ainsi réduire les coûts de support technique.
- *IBM Tivoli Access Manager for Enterprise Single Sign-On Authentication Adapter (adaptateur d'authentification)* permet l'authentification forte à l'aide de jetons, de cartes à puce, de données biométriques et de jetons de proximité. Il dispose d'autres fonctionnalités comme le passage d'une authentification par mot de passe à une authentification forte afin d'accéder à des ressources sensibles.
- *IBM Tivoli Access Manager for Enterprise Single Sign-On Provisioning Adapter (adaptateur d'allocation des comptes)* permet l'automatisation du provisionnement des informations d'identification des utilisateurs. Les solutions de gestion des identités comme IBM Tivoli Identity Manager sont capables de créer les comptes et de recevoir les informations d'identification d'IBM Tivoli Access Manager for Enterprise Single Sign-On.
- *IBM Tivoli Access Manager for Enterprise Single Sign-On Kiosk Adapter (adaptateur de kiosque)* offre un environnement à base de kiosques et de postes de travail partagés (multi-utilisateurs). L'adaptateur de kiosque assure l'arrêt automatique des sessions inactives, l'arrêt des applications et le basculement d'un utilisateur à l'autre.

Réinitialisation en libre-service des mots de passe Windows afin de réduire les coûts de support technique

IBM Tivoli Access Manager for Enterprise Single Sign-On Desktop Password Reset Adapter

Les entreprises qui utilisent des systèmes de sécurité basés sur la multiplicité des mots de passe consacrent des efforts importants de support à leurs utilisateurs finaux. Ces appels au support technique peuvent coûter des millions de dollars aux entreprises et empêchent les équipes informatiques de se consacrer à des activités à valeur ajoutée.

IBM Tivoli Access Manager for Enterprise Single Sign-On permet aux utilisateurs de s'identifier une seule fois via leur mot de passe Windows et ainsi d'avoir accès à toutes les autres applications en ne retenant que cet unique mot de passe. Mais que se passe-t-il si un employé oublie son mot de passe Windows ? Afin de limiter les appels au support, l'adaptateur de réinitialisation permet aux employés de réinitialiser leur mot de passe à partir de leur poste de travail verrouillé à l'aide d'une procédure simple à base de questions-réponses.

Les administrateurs, via la console d'administration Web, saisissent, ajoutent ou modifient les questions en indiquant pour chaque réponse des niveaux de confiance en adéquation avec les politiques de sécurité. A sa prise de fonction, l'utilisateur doit répondre à un ensemble de questions qui seront ensuite posées aléatoirement lors du test de réinitialisation. Un référentiel central configurable permet de stocker les questions et les réponses cryptées de test.

Gestion simple des authentifications multiples

Tivoli Access Manager for Enterprise Single Sign-On Authentication Adapter

Aujourd'hui, les contraintes de sécurité sont de plus en plus fortes. Beaucoup d'entreprises veulent mettre en place des méthodes d'authentification qui vont au-delà des mots de passe. La biométrie, les cartes à puce, les jetons et les détecteurs de proximité en sont des exemples. Une entreprise peut, par exemple, déployer des jetons pour les utilisateurs nomades ou distants, des cartes à puce pour les employés fixes, ou des mots de passe pour les prestataires. L'objectif est que chacun, suivant son rôle, puisse accéder aux applications nécessaires à son travail.

Mais ces dispositifs posent des problèmes d'intégration et d'administration aux entreprises qui ne veulent pas être dépendantes d'un seul fournisseur ou d'une seule technologie. Il est important que l'adaptateur d'authentification supporte plusieurs méthodes d'authentification tout en assurant la gestion de la connexion.

En agissant comme médiateur entre les mécanismes d'authentification et IBM Tivoli Access Manager for Enterprise Single Sign-On, l'adaptateur permet aux administrateurs de contrôler de manière centralisée les demandes d'authentification des utilisateurs vers les applications.. Ce niveau renforcé de contrôle garantit que l'accès des utilisateurs aux applications est conforme à l'ensemble des règles de sécurité. Les entreprises bénéficient en final d'un niveau de protection des données beaucoup plus renforcé.

Mettez en place les accès d'une façon simple, rapide et sécurisée

Tivoli Access Manager for Enterprise Single Sign-On Provisioning Adapter

Sur demande des métiers ou des ressources humaines, les administrateurs créent les comptes et les informations d'authentification pour chaque application, plate-forme ou système, puis ils les communiquent par e-mail, voire sur papier, aux utilisateurs finaux. Cette approche est coûteuse et elle crée des failles de sécurité en laissant les utilisateurs manipuler eux-mêmes les données d'identification. L'adaptateur de provisionnement des comptes peut recevoir les instructions d'allocation transmises par un système de gestion des identités, comme par exemple IBM Tivoli Identity Manager. L'administrateur peut alors préremplir les propriétés d'identification des employés avec des informations générées aléatoirement. Grâce à la diffusion automatique et directe de ces informations, les employés n'ont pas besoin de gérer, ni même de connaître leur nom d'utilisateur

et leur mot de passe. Les administrateurs eux-mêmes peuvent ne pas connaître le mot de passe initial d'une application.

Renforcez la sécurité des kiosques et des postes de travail partagés

Tivoli Access Manager for Enterprise Single Sign-On Kiosk Adapter

Les entreprises où un grand nombre d'utilisateurs utilisent le même poste de travail, comme par exemple dans le secteur médical, s'orientent vers des approches de type kiosques et postes de travail partagés. Ces approches sont, en effet, particulièrement intéressantes dans le cas d'accès fréquents par plusieurs personnes sur le même poste de travail. Les kiosques permettent également aux employés de partager plusieurs ordinateurs en libre-service, sans avoir à revenir systématiquement à leur propre machine dédiée.

L'adaptateur de kiosque maintient les informations d'authentification en demandant à l'utilisateur de se connecter à un annuaire LDAP ou à toute autre source. Cette approche évite ainsi de redémarrer le système.

Après avoir vérifié l'identité au sein de l'annuaire LDAP, l'adaptateur de kiosque se sert des informations d'identification, des définitions d'applications et des paramètres de l'utilisateur pour toute activité liée au processus d'authentification.

Dans ce genre d'approche, il est très fréquent que les utilisateurs quittent leur poste de travail sans se déconnecter, ce qui expose les données sensibles à un risque réel.

Pour empêcher que des données sensibles ne soient exploitées par des personnes mal intentionnées, IBM Tivoli Access Manager for Enterprise Single Sign-On Kiosk Adapter assure l'interruption automatique des sessions inactives et l'arrêt des applications pour les utilisateurs de kiosques et de postes de travail partagés. Les administrateurs peuvent déterminer le temps d'inactivité autorisé pour une session donnée avant suspension ou arrêt de cette dernière.

Comme il ne dépend pas de la session Windows, l'adaptateur de kiosque permet aux utilisateurs de changer de compte rapidement et de façon très sécurisée.

Utilisés conjointement, les adaptateurs apportent une valeur ajoutée supplémentaire au produit. Ils peuvent être utilisés dans des environnements de type kiosque en offrant un service de détecteur de proximité.

Enrichir les installations existantes de Tivoli Access Manager for e-business et Tivoli Federated Identity Manager

Aujourd'hui, beaucoup d'utilisateurs prennent conscience des atouts que représentent l'authentification unique et la gestion des accès Web offertes par Tivoli Access Manager for e-business. Ce logiciel peut fonctionner de manière autonome et unitaire (dans le cadre d'un site) ou bien dans le cadre d'une architecture dite fédérée (au-delà des frontières de l'entreprise) intégrant Tivoli Access Manager for e-business et IBM Tivoli Federated Identity Manager.

IBM Tivoli Access Manager for Enterprise Single Sign-On est intégrable facilement dans ce type d'architecture fédérée.

Une prise en charge souple de votre sécurité et de votre environnement

La gamme complète des logiciels Tivoli Access Manager for Enterprise Single Sign-On vous aide à maîtriser les difficultés liées à la gestion des mots de passe, en particulier l'obligation de saisir ou de modifier en permanence les noms d'utilisateur ou les mots de passe associés. La version de base est déjà très puissante et enrichit l'offre IBM de gestion des identités en offrant l'authentification unique pour IBM Lotus Notes, pour des progiciels tels que SAP, pour les applications standard Windows, les applications Web, mainframe ou autres. Les adaptateurs en option étendent les fonctionnalités de base du logiciel en offrant la prise en charge de l'authentification multi-niveaux , la multi authentification, l'allocation automatisée des propriétés des comptes, la réinitialisation simplifiée du mot de passe sur le poste de travail, la gestion des kiosques et des postes de travail partagés. C'est un logiciel simple à configurer, à déployer et à administrer. Son architecture permet d'obtenir un bénéfice rapide tout en renforçant votre politique de sécurité.

Aperçu des caractéristiques techniques de Tivoli Access Manager for Enterprise Single Sign-On

Pré-requis pour l'agent installé sur le poste client

- Serveur Windows 2000, XP, 2003
- Processeur Intel® Pentium® à 100 Mhz et 64 Mo de RAM
- Espace disque : environ 2,5 Mo pour installer le programme et stocker les données. Une installation complète requiert 7 Mo ; il faut environ 25 Mo disponibles sur le disque dur pour l'installateur
- Microsoft Internet Explorer 5.5 SP2 ou plus avec chiffrement 128 bits

Pré-requis pour la console d'administration et le serveur

- Serveur Windows 2000, XP, 2003
- Processeur compatible Intel Pentium à 100 Mhz et 64 Mo de RAM
- Microsoft .NET Framework 1.0
- Windows Installer 2.0 ou plus
- Espace disque : environ 4 Mo pour MSI Installer. Environ 31 Mo pour EXE Installer ; environ 15 Mo au total pour le programme installé et les données
- Annuaires : IBM Tivoli Directory Server, Microsoft Active Directory, Sun Java System Directory 5.1 ou plus, Novell eDirectory 8.5 ou plus, ou autre répertoire LDAP compatible avec la Version 2/Version 3
- Base de données : DB2 Universal Database, Microsoft SQL Server, Oracle, entre autres

Pré-requis pour l'adaptateur de réinitialisation du mot de passe

- Microsoft Internet Information Server 5.0 ou 6.0
- Microsoft .NET 1.1
- Microsoft Active Directory et ADAM
- Microsoft SQL

Pré-requis pour l'adaptateur d'authentification

- Processeur Pentium à 120 Mhz
- Espace disque : environ 1 Mo
- Internet Explorer 6.0 ou plus avec chiffrement 128 bits
- Remarque : Certains systèmes d'authentification renforcée ont souvent leurs propres contraintes. Elles peuvent être différentes de celles mentionnées ici.
- Pré-requis pour la console d'administration et le serveur :
  - Processeur Pentium II à 400 Mhz et 96 Mo de RAM
  - Espace disque : environ 1 Mo

Pré-requis pour l'adaptateur d'allocation des comptes

- Espace disque pour l'agent du client : environ 1 Mo
- Pré-requis pour le serveur :
  - Microsoft Internet Information Server 5.x ou 6.x (6.x recommandé)
  - Répertoire : Microsoft Active Directory et ADAM, SunOne Directory ou IBM Tivoli Directory Server
  - Microsoft SQL Server 2000 ou Microsoft SQL Server 2000 Desktop Engine
  - Internet Explorer 6.0 ou plus avec chiffrement 128 bits
  - Espace disque : environ 3 Mo
  - Processeur Pentium III à 900 Mhz et 512 Mo de RAM

Pré-requis pour l'adaptateur de kiosque

- Microsoft .NET 1.1
- Processeur Pentium III à 733 Mhz et 128 Mo de RAM
- Espace disque : environ 3 Mo
- Internet Explorer 6.0 ou plus avec chiffrement 128 bits

Les logiciels Tivoli d'IBM

Avec les logiciels Tivoli d'IBM, les entreprises peuvent gérer de manière efficace et économique les ressources, les activités et les processus informatiques pour répondre aux exigences évolutives du métier et offrir la meilleure qualité de service en maîtrisant les coûts de production et d'exploitation. 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. Ces produits bénéficient de la qualité de support, de la recherche et des services IBM.

Pour plus d'informations

Pour savoir comment Tivoli Access Manager for Enterprise Single Sign-On peut simplifier la gestion des mots de passe de vos administrateurs et de vos utilisateurs finaux, 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

GC28-8426-FRA-00