

IBM Tivoli Security Compliance Manager

Points forts

- **Automatiser les contrôles de sécurité sur les serveurs et les ordinateurs de bureau, afin de limiter les coûts et les pertes de temps**
- **Fournir une solution rapide, simple, proactive et rentable pour protéger les infrastructures informatiques, en identifiant les vulnérabilités dans le système de sécurité avant que le mal ne soit fait**
- **Utiliser les règles et rapports fournis pour accélérer la prise en main et le retour sur investissement**
- **Offrir une manière efficace d'évaluer et de surveiller le respect des règles de sécurité à l'échelle de l'entreprise.**

Améliorer et contrôler le niveau de sécurité

Ces dernières années, les administrateurs chargés de l'informatique et de la sécurité ont vu le nombre d'attaques de virus et autres vers informatiques littéralement exploser. La plupart d'entre eux viennent de l'extérieur de l'entreprise. D'autres viennent de l'intérieur, le plus souvent à la suite d'une erreur humaine ou d'une négligence. Quelle que soit la cause, toute faille dans le système de sécurité d'une entreprise peut entraîner une perte de temps, la perte ou la corruption des données, une perte de crédibilité, de la gêne et même des problèmes contentieux.

Pourtant, 90 % des incidents de sécurité peuvent être évités en implémentant et en appliquant des stratégies de sécurité cohérentes à l'échelle de l'entreprise. IBM Tivoli Security Compliance Manager agit en amont, et aide les entreprises de toute taille à identifier les violations des règles de sécurité et les faiblesses potentielles des systèmes, avant qu'un incident de sécurité ne se produise. Ce produit offre aux entreprises une solution rapide, rentable et proactive pour collecter et gérer les informations liées à l'état de leur système de sécurité.

De plus en plus, les entreprises doivent se conformer aux règles définies face au nombre croissant de réglementations gouvernementales visant à garantir la protection et l'intégrité des données. Il est donc indispensable de disposer d'un système permettant de vérifier la conformité avec ces règles.

Simplifier un processus fastidieux grâce à l'automatisation

Le contrôle manuel du respect des règles de sécurité est un processus fastidieux et coûteux, qui peut prendre des journées entières et peut en outre être faussé par des erreurs humaines ou des incohérences. Tivoli Security Compliance Manager est basé sur l'automatisation à la demande, un concept au cœur même des stratégies largement reconnues et éprouvées d'IBM en matière de logiciels. Un contrôle automatisé et centralisé du respect des règles de sécurité est généralement l'affaire de quelques minutes. Cela peut décharger les administrateurs de fonctions de routine longues et fastidieuses, ce qui permet d'accroître l'efficacité, de réaliser des économies et de limiter les risques d'erreur humaine.

conformité et des audits de sécurité, décroît progressivement. En outre, des économies supplémentaires peuvent être réalisées dans la mesure où les éventuelles vulnérabilités dans vos systèmes (IBM AIX, Solaris, HP-UX, Microsoft® Windows®, Linux et Linux sur zSeries) sont identifiées avant qu'une brèche de sécurité ne se produise, induisant des coûts de réparation élevés.

Tivoli Security Compliance Manager comprend des fonctions autonomes, par exemple une fonction "heartbeat" qui envoie automatiquement et à intervalles réguliers des pulsations depuis les points terminaux gérés vers le serveur central, permettant au système de s'assurer que les différentes machines fonctionnent correctement et sont bien à jour. Ces fonctions autonomes permettent au logiciel de gérer lui-même les systèmes terminaux Java et de les mettre à jour. Partie intégrante de l'initiative à la demande d'IBM, cette approche automatisée de la conformité par rapport aux règles de sécurité offre au client davantage de robustesse et une certaine faculté à s'adapter aux différentes menaces.

Intégration avec les produits de gestion automatisée de la sécurité IBM Tivoli

Tivoli Security Compliance Manager transmet les informations liées au non respect ou à la violation des règles de sécurité aux outils Tivoli de gestion automatisée de la sécurité, afin de trouver une parade aux problèmes de sécurité et aux risques qui en découlent. En utilisant ce produit en collaboration avec d'autres logiciels Tivoli, comme IBM Tivoli Risk Manager, IBM Tivoli Enterprise Console ou IBM Tivoli Configuration Manager, les entreprises peuvent parvenir facilement à éviter tout dommage et à remédier aux violations des règles de sécurité. En effet, Tivoli Security Compliance Manager peut travailler en tandem avec ces solutions Tivoli pour arrêter les services inutiles, modifier les droits d'accès, mettre à niveau des logiciels ou encore déployer des correctifs.

Pour plus d'informations

Pour en savoir plus sur Tivoli Security Compliance Manager et les solutions intégrées d'IBM, contactez votre représentant IBM ou visitez notre site Web à l'adresse suivante : **ibm.com**/tivoli/products/security-compliance-mgr

Logiciels IBM Tivoli

Partie intégrante de la solution complète d'infrastructure à la demande d'IBM, les logiciels de gestion Tivoli aident les entreprises traditionnelles, les toutes nouvelles entreprises à la demande et les entreprises Internet du monde entier à tirer le maximum de profits de leurs investissements technologiques actuels et futurs. Soutenus par les services, le support et la recherche IBM, les logiciels Tivoli offrent une solution de gestion d'infrastructure intégrée et souple pour les entreprises à la demande, avec un système de sécurité robuste pour relier les employés, les partenaires commerciaux et les clients

Configuration matérielle

Configuration requise en termes de processeur et de mémoire pour un serveur Tivoli Security Compliance Manager

Type de déploiement Tivoli Security Compliance Manager	Processeur	Mémoire
Petit (1 à 500 clients)	1	512 Mo de RAM
Intermédiaire (501 à 2 500 clients)	2	512 Mo de RAM
Grand (2 501 à 10 000 clients)	2-4	2 à 4 Go de RAM

Il faut prévoir 5 Mo d'espace disque pour l'installation du package serveur.

Configuration requise en termes de disque et de mémoire pour les clients et les collecteurs

Configuration requise en termes de disque et de mémoire pour un client Tivoli Security Compliance Manager

Plate-forme client	Espace disque pour le répertoire d'installation	Espace disque pour le répertoire temporaire	Mémoire
AIX	64 Mo	45 Mo	75 Mo de RAM
HP-UX	64 Mo	6 Mo	75 Mo de RAM
Linux	64 Mo	46 Mo	75 Mo de RAM
Solaris	64 Mo	65 Mo	75 Mo de RAM
Windows	64 Mo	44 Mo	75 Mo de RAM

Remarque : Les valeurs concernant la plate-forme HP-UX sont bien inférieures à celles des autres plates-formes car Java Runtime Environment n'est pas fourni avec le client HP-UX.

Configuration requise en termes de disque et de mémoire pour les utilitaires d'administration

Configuration requise en termes de disque et de mémoire pour la console d'administration Tivoli Security Compliance Manager

Plate-forme console d'administration	Espace disque pour le répertoire d'installation	Espace disque pour le répertoire temporaire	Mémoire
Windows	64 Mo	42 Mo	128 Mo de RAM minimum, 256 Mo recommandé

Configuration logicielle

Tivoli Security Compliance Manager nécessite les logiciels suivants :

IBM DB2 Universal Database, Version 7.2 ou Version 8.1 (Tivoli Security Compliance Manager 5.1 inclut DB2 Universal Database, Version 8.1.)

Systèmes d'exploitation pris en charge

Les tableaux suivants répertorient les systèmes d'exploitation pris en charge pour le serveur, le client et la console d'administration Tivoli Security Compliance Manager.

Serveur Tivoli Security Compliance Manager

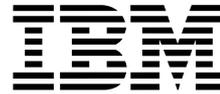
Système d'exploitation	Version	Correctif/maintenance
AIX	5.1, 5.2	Aucun correctif requis
Windows 2000	Server	Dernier correctif publié
Solaris	2.8, 2.9	Dernier correctif publié
SUSE Linux Enterprise Server	8	Dernier correctif publié

Client Tivoli Security Compliance Manager

Système d'exploitation	Version	Correctif/maintenance
AIX	5.1, 5.2	Derniers correctifs publiés
HP-UX	11.0, 11i	Derniers correctifs publiés
Red Hat Linux	6.2, 7.0, 7.1, 7.2, 7.3, 8.0, 9.0	Derniers correctifs publiés
Solaris	2.6, 2.7, 2.8, 2.9	Derniers correctifs publiés
Windows NT®	4.0 Server, 4.0 Workstation	Dernier service pack et package sécurité
Windows 2000	Server, Advanced Server, Professional	Dernier service pack et package sécurité
Windows XP	Professional	Dernier service pack et package sécurité
Windows 2003	Server Standard Edition, Enterprise Edition	Derniers correctifs publiés
Red Hat Enterprise Linux	2.1	Derniers correctifs publiés
Red Hat Enterprise Linux Advanced Server	3.0	Derniers correctifs publiés
Red Hat Enterprise Linux pour zSeries	3.0	Derniers correctifs publiés
Red Hat Enterprise Linux pour iSeries ou pSeries	3.0	Derniers correctifs publiés
Red Hat Enterprise Linux pour zSeries	7.2	Derniers correctifs publiés
Red Hat Enterprise Linux Advanced Server	2.1	Derniers correctifs publiés
SUSE Linux	7.0	Derniers correctifs publiés
SUSE Linux Enterprise Server	8	Derniers correctifs publiés
SUSE Linux Enterprise Server pour zSeries	8	Derniers correctifs publiés
SUSE Linux Enterprise Server pour iSeries ou pSeries	8	Derniers correctifs publiés

Console d'administration Tivoli Security Compliance Manager

Système d'exploitation	Version	Correctif/maintenance
Windows 2000	Professional	Dernier service pack et package sécurité
Windows XP	Professional	Dernier service pack et package sécurité



Compagnie IBM France

Tour Descartes - La Défense 5
2, avenue Gambetta
92066 - Paris-La Défense Cedex.

IBM Belgium

Avenue du Bourget/Bourgetlaan, 42
B - 1130 Brussels

La page d'accueil IBM est accessible sur ibm.com

IBM, le logo IBM, ibm.com, On Demand Business et le logo On Demand Business, AIX, Tivoli, Tivoli Enterprise Console, iSeries, pSeries et zSeries sont des marques ou des marques déposées d'International Business Machines Corporation aux États-Unis et/ou dans d'autres pays.

Java et toutes les marques basées sur Java sont des marques commerciales de Sun Microsystems, Inc. aux États-Unis et/ou dans d'autres pays.

Linux est une marque de Linus Torvalds aux États-Unis et/ou dans d'autres pays.

Microsoft, Windows et Windows NT sont des marques déposées de Microsoft Corporation aux États-Unis et/ou dans d'autres pays.

Les autres raisons sociales, noms de produit et noms de service peuvent être des marques ou des marques de service de leurs propriétaires respectifs.

Il incombe à chaque client IBM de veiller au respect des différentes lois et réglementations. Il est de la seule responsabilité du client de se renseigner auprès d'organismes de conseil juridique compétents quant à l'identification et l'interprétation des lois et réglementations applicables susceptibles d'affecter son entreprise, et aux actions à mettre en place pour respecter ces lois et réglementations. IBM ne fournit aucun conseil juridique et ne garantit en aucune manière que ses services et produits sont en mesure d'assurer la conformité avec une quelconque loi ou réglementation.

© Copyright IBM Corporation 2004
Tous droits réservés.

