IBM PowerSC

Conçu pour la sécurité et la conformité d'entreprise dans les environnement cloud et virtualisés

Points forts

- Simplifiez la gestion et l'évaluation pour la sécurité et la conformité
- Interface utilisateur centralisée qui permet d'identifier rapidement la mise en conformité de la sécurité d'un centre informatique complet
- Réduction du temps et des coûts d'administration de la mise en conformité aux réglementations
- Amélioration des capacités d'audit des systèmes virtualisés et réduction du temps et du niveau de compétences nécessaires à la préparation
- Amélioration de la détection et du reporting des risques de sécurité dans les environnements virtualisés.

Le contrôle de sécurité et la conformité figurent parmi les principaux composants nécessaires pour protéger le centre informatique virtualisé et l'infrastructure cloud des nouvelles menaces en renouvellement constant. Assurer la conformité des systèmes informatiques aux normes de sécurité communes de l'industrie et le maintien de la sécurité des systèmes peut s'avérer une activité complexe, onéreuse et gourmande en main d'œuvre, en particulier avec les infrastructures informatiques cloud ou virtualisées. IBM® PowerSC offre une solution de sécurité et de conformité optimale aux environnements cloud et virtualisés sur des serveurs Power Systems fonctionnant avec PowerVM.

PowerSC est une offre intégrée qui assure des niveaux élevés de sécurité et de conformité en tirant parti de l'ensemble des fonctions de la pile logicielle IBM Power Systems, de l'hyperviseur et du micrologiciel au système d'exploitation, en passant par la couche de virtualisation et le trafic réseau entre les couches.

La fonction PowerSC permet de réduire les coûts, de simplifier l'administration, d'accélérer la préparation des audits de conformité et de réduire le risque en augmentant la visibilité sur les menaces de sécurité.

Automatisation des paramètres système pour une sécurité et une conformité optimales

Nombreux sont les clients IBM Power System qui doivent se conformer aux normes strictes de leur secteur. La conformité réglementaire implique de définir la sécurité des systèmes de manière uniforme. La prise en compte de toutes les règles et l'application de certaines normes sont des obligations fastidieuses, chronophages et sources d'erreurs. Les normes de conformité sont généralement des documents longs et complexes,

comportant des centaines de règles difficiles à traduire dans les paramètres du système d'exploitation approprié. En outre, comme les normes englobent bien souvent plusieurs domaines différents du système d'exploitation et du logiciel de virtualisation, l'utilisation de plusieurs interfaces administratives différentes peut être nécessaire pour configurer correctement un système.

PowerSC Compliance Automation s'accompagne de profils pré-intégrés certifiés conformes aux normes de l'industrie telles que Payment Card Industry Data Security Standard (PCI) v3, HIPAA (Health Insurance Portability and Accountability Act Privacy and Security Rules) pour le secteur de la santé, NERC (North American Electric Reliability Corporation) pour les services publics tels que l'énergie, DoD STIG (US Department of Defence Security Technical Implementation Guide for UNIX) pour nos clients fédéraux ou d'un support de SOX-COBIT (meilleures pratiques Sarbanes- Oxley indiquées par les Control Objectives for Information and related Technology [objectifs de contrôle pour les technologies de l'information et technologies connexes]). PowerSC fournit également un profil d'automatisation de sécurité pour automatiser la configuration de sécurité optimale pour les serveurs de bases de données. En outre, il s'accompagne de niveaux de sécurité prêts à l'emploi : Faible, Moyen et Elevé.

PSCxpert (version optimisée d'AIXpert) constitue le mécanisme sous-jacent permettant d'appliquer les paramètres des politiques de sécurité et de vérifier la conformité. Ces outils ont toujours permis de gérer la conformité de manière remarquable. Cependant, pour gérer les profils, vous deviez vous connecter et exécuter des commandes sur chaque système individuellement. La nouvelle interface centralisée pour Compliance Automation, lancée pour la première fois avec PowerSC 1.1.5, facilite considérablement la gestions de la conformité de la sécurité (voir « Une nouvelle interface centralisée pour la sécurité et la conformité » ci-dessous)

Surveillance continue et alerte sur les modifications

Real Time Compliance permet la surveillance d'une liste de fichiers et envoie des notifications lorsque des atteintes à la conformité se produisent ou lorsqu'un fichier surveillé subit des modifications. En règle générale, les vérifications régulières de la conformité sont menées de manière planifiée. Ainsi, si votre système est victime d'une infraction, cela ne sera normalement pas remarqué avant la prochaine analyse. Real Time Compliance supprime ce délai en ajoutant des notifications en temps réel pour toutes les violations possibles de la politique sur votre serveur. Dès qu'une modification est contraire à la politique des profils de conformité, un message peut être envoyé aux administrateurs ou agents de sécurité par SMS ou courrier électronique. Il est également possible d'envoyer des messages Syslog ou SNMP (Simple Network Management Protocol) à votre serveur de surveillance, et d'intégrer la fonction à votre système de surveillance informatique. Certains produits tels qu'IBM QRadar peuvent accepter l'intégration de ces alertes à votre infrastructure existante.

PowerSC Real Time Compliance offre deux options de surveillance :

1. *La surveillance des contenus* permet de vérifier si le contenu des fichiers a été modifié

2. *La surveillance des attributs* permet de vérifier si les autorisations du fichier ont été modifiées

Nouvelle interface centralisée pour la sécurité et la conformité

La nouvelle interface centralisée pour la sécurité et la conformité (lancée pour la première fois avec PowerSC 1.1.5 et largement étendue avec PowerSC 1.1.6) facilite considérablement la gestion de la sécurité et de la conformité. Elle permet ainsi de réaliser des économies, de gagner du temps et de diminuer les risques d'erreur humaine.

- **Compliance Automation**
  Pour comprendre et gérer la conformité de la sécurité de tous les terminaux AIX gérés par PowerSC à travers votre environnement Power ; ceci avec un effort de découverte réduit au minimum et un emplacement centralisé. Cette fonction permet de vérifier et d'appliquer les profils PowerSC en utilisant aussi bien les modèles de série que les modèles personnalisés sur plusieurs terminaux à la fois. En outre, elle permet d'organiser et de regrouper les terminaux PowerSC afin de mettre en place un filtrage personnalisé
- **Intégration RTC / TE**
  Amélioration des fonctions de prévention/détection des intrusions de logiciels malveillants grâce à des capacités de configuration et de surveillance centralisées pour le contrôle de l'intégrité des fichiers (PowerSC RTC et AIX TE)
- **Intégration PowerVC**
  Permet de protéger vos clouds dès le départ. Nous avons semi-automatisé le processus de connexion des nouveaux terminaux déployés avec PowerVC en tant que nouveaux terminaux gérés avec la nouvelle interface PowerSC
- **Tableau de bord pour la sécurité et la conformité**
  Affichage consolidé de tous les composants de protection et de vérification de la sécurité AIX
- **Rapports supportant les audits**
  PowerSC 1.1.6 s'accompagne de cinq rapports OOTB pour supporter la préparation des audits et leur succès. Il permet de générer des fichiers html ou csv formatés qui peuvent même être programmés pour un envoi par courrier électronique à des moments définis
- **Optimisations de l'éditeur de profils**
  Alors que l'éditeur de profils de la version 1.1.5 se limitait à la création de profils personnalisés, celui de la version 1.1.6 permet aux clients de réunir les règles de plusieurs profils dans un profil personnalisé. En outre, il confère la possibilité de modifier les paramètres de certaines règles dans ces profils personnalisés
- **Intégration de Northbound (QRadar)**
  Dans la version 1.1.6, nous avons travaillé sur une intégration à des outils de sécurité de niveau supérieur par le biais des informations syslog pour qu'elles puissent être exploitées par QRadar et y être rendues disponibles
- **Améliorations apportées à UNDO**
  Le processus UNDO des profils est assez complexe. Dans PowerSC 1.1.6, le comportement de UNDO est améliorée pour le profil PCIv3. (Le comportement de UNDO des autres profils sera également amélioré dans les versions ultérieures)
- **Evolutivité de l'interface de conformité**
  PowerSC pouvait supporter 500 terminaux par serveur d'interface dans la version 1.1.5. PowerSC 1.1.6 multiplie ce nombre par deux pour supporter 1000 terminaux par serveur d'interface.

Remarque : Dans cette version, tous les autres composants PowerSC (TNC, Trusted Boot, Trusted Firewall, Trusted Logging) restent présents dans leur édition d'origine (ligne de commande) ;

La nouvelle interface centralisée pour la sécurité et la conformité supporte uniquement AIX dans la version actuelle

Mise en conformité aux règles de sécurité du site pour les machines virtuelles

Le maintien de machines virtuelles sur plusieurs systèmes présente différents défis administratifs pour le déploiement de systèmes physiques traditionnels. Par exemple, les machines virtuelles peuvent être suspendues ou éteintes ou encore déplacées vers d'autres serveurs au cours d'un processus d'application de correctif. Le déplacement d'une machine virtuelle, par exemple, peut ouvrir une fenêtre de vulnérabilité en présentant un niveau de correctif différent de celui requis sur un système physique cible.

Les fonctions Trusted Network Connect (TNC) et Patch Management de PowerSC permettent de détecter les machines virtuelles AIX qui ne respectent pas les règles de correctif de l'entreprise établies pour un centre informatique virtualisé. Des alertes sont déclenchées si une machine virtuelle non conforme est détectée. TNC et Patch Management analysent les données de l'assistant SUMA (Service Update Manager Assistant) et du gestionnaire NIM (Network Installation Manager) pour vérifier chaque machine virtuelle au cours de l'activation réseau.

TNC et Patch Management surveillent également le système IBM Electronic Customer Care et fournissent des alertes pour les nouveaux correctifs de sécurité ou mises à jour qui affectent les systèmes AIX. Les alertes peuvent également être configurées simplement pour envoyer des messages SMS aux périphériques mobiles.

Dans la dernière édition, TNC and Patch Management surveille également le logiciel Open Source fourni avec AIX de base pour les packages téléchargés depuis la boîte à outils AID ou d'autres sites Web pour les packages Open Source AIX.

Amélioration de la visibilité et renforcement de l'infrastructure virtuelle

PowerSC propose diverses fonctionnalités pour assurer une base de confiance aux machines virtuelles, notamment « Trusted Boot », une implémentation virtuelle du module TPM (Trusted Platform Module) de Trusted Computing Group. La fonction PowerSC Trusted Boot offre une fonctionnalité TPM virtuelle pour les machines virtuelles AIX exécutées avec l'hyperviseur PowerVM sur Power Systems.

La fonctionnalité TPM mesure le processus de démarrage du système dans chaque machine virtuelle et, en association avec la technologie AIX Trusted Execution, fournit la sécurité, la confiance et l'assurance de l'image de démarrage sur le disque, l'ensemble du système d'exploitation et les couches d'applications. Chaque machine virtuelle dispose de son propre module TPM virtuel distinct qui comporte ses données de mesure extraordinaires pour valider la base de confiance. Cette fonctionnalité est disponible sur tous les IBM Power Systems intégrant la technologie POWER8 ou sur les systèmes exécutant le microprogramme eFW7.4 ou version supérieure.

OpenPTS est un moniteur de confiance fourni avec PowerSC. Il permet aux administrateurs de surveiller et d'attester de la fiabilité de leurs machines virtuelles AIX.

Renforcement des enregistrements d'audit dans les environnements virtuels

Trusted Logging de PowerSC centralise les journaux système AIX de toutes les machines virtuelles sur un serveur, permettant ainsi aux journaux d'être conservés sur une seule instance du VIOS (PowerVM Virtual I/O Server). Cette machine virtuelle VIOS sécurisée protège toutes les données de journaux reçues de chaque machine virtuelle AIX. Aucun administrateur de machine virtuelle AIX ne peut supprimer ou modifier les journaux système sur le serveur VIOS sécurisé.

Avec l'introduction de la journalisation et de l'administration centralisées fournies par Trusted Logging, la sauvegarde, l'archivage et l'audit des journaux système sont considérablement simplifiés pour l'administrateur de sécurité.

Contrôler et renforcer la conformité des réseaux virtuels.

La fonction Trusted Firewall de PowerSC fournit un pare-feu virtuel qui permet le filtrage et le contrôle du réseau au sein de la virtualisation locale des serveurs. Le pare-feu virtuel améliore les performances et réduit la consommation de ressources réseau en offrant un accès direct et sécurisé au réseau à la machine virtuelle. Trusted Firewall permet de surveiller le trafic et de conseiller quel trafic il convient d'ajouter au pare-feu. Cet assistant peut générer les commandes appropriées pour ajouter des segments de réseau de machines virtuelles au pare-feu Trusted Firewall.

La fonction de sécurité et de conformité de PowerSC inclut les composants suivants

Automatisation de la mise en conformité incluant des profils pré-configurés pour les différentes normes de l'industrie	• L'automatisation de la mise en conformité de la sécurité fournit des profils pré-intégrés, certifiés conformes aux normes de l'industrie telles que PCIv3, HIPAA, NERC, DoD STIG et SOX-COBIT.
Mise en conformité en temps réel (RTC) incluant des fonctions de reporting	• Simplifie la gestion par l'automatisation de la surveillance et la visibilité immédiate conférée aux administrateurs. Envoie des alertes lorsqu'une modification apportée au système porte atteinte à une règle de la politique de configuration et entraîne la non-conformité des systèmes AIX.
Trusted Network Connect (TNC) et Patch Management	• Détecte automatiquement le système AIX en cours de démarrage, d'arrêt ou de déplacement grâce à une mobilité en temps réel dans l'environnement virtuel. S'assure que le niveau des installations et des correctifs est celui indiqué et envoie des alertes si un correctif de sécurité affecte les systèmes.
Trusted Boot	• Evalue l'image de démarrage, le système d'exploitation et les applications, atteste leur authenticité et confirme qu'ils n'ont pas été modifiés accidentellement ou de façon malintentionnée grâce à la technologie vTPM (virtual Trusted Platform Module).
Trusted Logging	• Les journaux d'AIX sont stockés de façon centralisée et en temps réel sur le serveur virtuel d'entrées/sorties (E/S). Cette fonction permet une journalisation inviolable et facilite la sauvegarde et la gestion des journaux. Elle supprime également le besoin de disposer d'agents de nettoyage des journaux. Ainsi, elle préserve la fiabilité des journaux système et des journaux d'audit.
Trusted Firewall	• Trusted Firewall s'assure que chaque machine virtuelle est isolée de manière adéquate dans le réseau. Cette fonction permet d'économiser du temps et des ressources en pratiquant le routage direct à travers les LAN virtuels indiqués (VLAN). Grâce aux services de pare-feu qu'elle procure au sein du serveur, aucun pare-feu externe n'est nécessaire pour le trafic de machine virtuelle à machine virtuelle sur le même CEC et les performances sont améliorées.

Pour plus d'informations

Pour en savoir plus sur IBM PowerSC, veuillez contacter votre représentant marketing IBM ou votre partenaire commercial IBM ; vous pouvez également consulter le site Web suivant : **ibm.com**/systems/power/software/security/index.html

Compagnie IBM France
17 avenue de l'Europe
92275 Bois-Colombes Cedex
France

IBM France est enregistré en France.

La page d'accueil d'IBM est accessible à l'adresse : **ibm.com**/fr

Veuillez recycler

PowerSC

POD03063-FRFR-09