IBM PowerSC

Standard Edition

Version 1.1.3

PowerSC Standard Edition

IBM PowerSC

Standard Edition

Version 1.1.3

PowerSC Standard Edition

Important
Avant d'utiliser le présent document et le produit associé, prenez connaissance des informations figurant à la section «Remarques», à la page 49.

LE PRESENT DOCUMENT EST LIVRE EN L'ETAT SANS AUCUNE GARANTIE EXPLICITE OU IMPLICITE. IBM DECLINE NOTAMMENT TOUTE RESPONSABILITE RELATIVE A CES INFORMATIONS EN CAS DE CONTREFACON AINSI QU'EN CAS DE DEFAUT D'APTITUDE A L'EXECUTION D'UN TRAVAIL DONNE.

Ce document est mis à jour périodiquement. Chaque nouvelle édition inclut les mises à jour. Les informations qui y sont fournies sont susceptibles d'être modifiées avant que les produits décrits ne deviennent eux-mêmes disponibles. En outre, il peut contenir des informations ou des références concernant certains produits, logiciels ou services non annoncés dans ce pays. Cela ne signifie cependant pas qu'ils y seront annoncés.

Pour plus de détails, pour toute demande d'ordre technique, ou pour obtenir des exemplaires de documents IBM, référez-vous aux documents d'annonce disponibles dans votre pays, ou adressez-vous à votre partenaire commercial.

Vous pouvez également consulter les serveurs Internet suivants :

- http://www.fr.ibm.com (serveur IBM en France)
- http://www.can.ibm.com (serveur IBM au Canada)
- http://www.ibm.com (serveur IBM aux Etats-Unis)

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

La présente édition s'applique à IBM PowerSC Version 1.1.3 et à toutes les éditions et modifications ultérieures, sauf indication contraire dans les nouvelles éditions.

© Copyright IBM Corporation 2012, 2013.

Table des matières

Avis aux lecteurs canadiens v

A propos de ce document vii

IBM PowerSC Standard Edition 1.1.3 . . 1

Nouveautés dans PowerSC Standard Edition 1.1.3 . . 1
Concepts PowerSC Standard Edition 1.1.3 2
Installation de PowerSC Standard Edition 1.1.3 . . . 3
Trusted Boot 4
Concepts Trusted Boot 4
Planification de Trusted Boot 5
Installation de Trusted Boot 6
Configuration de Trusted Boot 7
Gestion de Trusted Boot 8
Traitement des incidents liés à Trusted Boot . . . 9
Trusted Firewall 10
Concepts Trusted Firewall 10
Installation de Trusted Firewall 12
Configuration de Trusted Firewall 13
Trusted Logging 17
Journaux virtuels 18
Détection des unités de journal virtuel 18
Installation de Trusted Logging 19
Configuration de la journalisation sécurisée . . 19
Trusted Network Connect and Patch management 21
Concepts Trusted Network Connect 21
Installation de Trusted Network Connect . . . 23
Configuration de Trusted Network Connect and Patch management 24
Gestion de Trusted Network Connect and Patch management 28
Génération de rapports sur les serveurs TNC . . 31
Traitement des incidents liés à Trusted Network Connect and Patch management 31
Commandes de PowerSC Standard Edition 32
commande chvfilt 32
Commande genvfilt 34
Commande lsvfilt 35
Commande mkvfilt 36
Commande pmconf. 36
Commande psconf 40
Commande rmvfilt 45
Commande vlantfw 46

Remarques 49

Politique de protection des renseignements personnels 51
Marques 52

Index 53

© Copyright IBM Corp. 2012, 2013

Avis aux lecteurs canadiens

Le présent document a été traduit en France. Voici les principales différences et particularités dont vous devez tenir compte.

Illustrations

Les illustrations sont fournies à titre d'exemple. Certaines peuvent contenir des données propres à la France.

Terminologie

La terminologie des titres IBM peut différer d'un pays à l'autre. Reportez-vous au tableau ci-dessous, au besoin.

IBM France	IBM Canada
ingénieur commercial	représentant
agence commerciale	succursale
ingénieur technico-commercial	informaticien
inspecteur	technicien du matériel

Claviers

Les lettres sont disposées différemment : le clavier français est de type AZERTY, et le clavier français-canadien de type QWERTY.

OS/2 et Windows - Paramètres canadiens

Au Canada, on utilise :

- les pages de codes 850 (multilingue) et 863 (français-canadien),
- le code pays 002,
- le code clavier CF.

Nomenclature

Les touches présentées dans le tableau d'équivalence suivant sont libellées différemment selon qu'il s'agit du clavier de la France, du clavier du Canada ou du clavier des États-Unis. Reportez-vous à ce tableau pour faire correspondre les touches françaises figurant dans le présent document aux touches de votre clavier.

© Copyright IBM Corp. 2012, 2013

France	Canada	Etats-Unis
(Pos1)		Home
Fin	Fin	End
(PgAr)		PgUp
(PgAv)		PgDn
Inser	Inser	Ins
Suppr	Suppr	Del
Echap	Echap	Esc
Attn	Intrp	Break
Impr écran	ImpEc	PrtSc
Verr num	Num	Num Lock
Arrêt défil	Défil	Scroll Lock
(Verr maj)	FixMaj	Caps Lock
AltGr	AltCar	Alt (à droite)

Brevets

Il est possible qu'IBM détienne des brevets ou qu'elle ait déposé des demandes de brevets portant sur certains sujets abordés dans ce document. Le fait qu'IBM vous fournisse le présent document ne signifie pas qu'elle vous accorde un permis d'utilisation de ces brevets. Vous pouvez envoyer, par écrit, vos demandes de renseignements relatives aux permis d'utilisation au directeur général des relations commerciales d'IBM, 3600 Steeles Avenue East, Markham, Ontario, L3R 9Z7.

Assistance téléphonique

Si vous avez besoin d'assistance ou si vous voulez commander du matériel, des logiciels et des publications IBM, contactez IBM direct au 1 800 465-1234.

A propos de ce document

Ce document fournit aux administrateurs système des informations complètes sur la sécurité des fichiers, du système et du réseau.

Mise en évidence

Le présent document utilise les conventions typographiques suivantes :

Gras	Identifie les commandes, les sous-programmes, les mots clés, les fichiers, les structures, les répertoires, ainsi que d'autres éléments dont le nom est défini par le système. Permet également d'identifier les objets graphiques comme les boutons, libellés et icônes, sélectionnés par l'utilisateur.
Italique	Identifie les paramètres dont les noms ou les valeurs doivent être indiqués par l'utilisateur.
`Espacement fixe`	Identifie les exemples de valeurs de données, les exemples de textes similaires à ceux affichés, les exemples de parties de code similaires au code que vous serez susceptible de rédiger en tant que programmeur, les messages système ou les informations que vous devez saisir.

Distinction majuscules/minuscules dans AIX

La distinction majuscules/minuscules s'applique à toutes les données entrées dans le système d'exploitation AIX. Vous pouvez, par exemple, utiliser la commande **ls** pour afficher la liste des fichiers. Si vous entrez `LS`, le système affiche un message indiquant que la commande est `introuvable`. De la même manière, `FILEA`, `FiLea` et `filea` sont trois noms de fichiers distincts, même s'ils se trouvent dans le même répertoire. Pour éviter toute action indésirable, vérifiez systématiquement que vous utilisez la casse appropriée.

ISO 9000

Les systèmes de gestion de la qualité utilisés pour le développement et la fabrication de ce produit sont en conformité avec les normes ISO 9000.

© Copyright IBM Corp. 2012, 2013

IBM PowerSC Standard Edition 1.1.3

IBM® PowerSC Standard Edition intègre les fonctions Trusted Boot, Trusted Firewall, Trusted Logging, Trusted Network Connect and Patch management et Security and Compliance Automation.

Nouveautés dans PowerSC Standard Edition 1.1.3

Découvrez les nouveautés et modifications significatives apportées à l'ensemble de rubriques relatives à PowerSC Standard Edition version 1.1.3.

Ce fichier PDF peut comporter des barres de révision (|) dans la marge de gauche en regard des informations nouvelles ou modifiées.

Décembre 2013

- Mise à jour de la configuration système requise décrite dans «Concepts PowerSC Standard Edition 1.1.3», à la page 2.
- Identification d'un remplacement de fichier Trusted Boot obligatoire lors de la réinstallation du système d'exploitation AIX décrite dans «Configuration prérequise pour Trusted Boot», à la page 5.
- Ajout d'informations relatives à la fonction de contrôle de Trusted Firewall dans «Fonction de contrôle de Trusted Firewall», à la page 13.
- Ajout d'informations relatives à la fonction de journalisation de Trusted Firewall dans «Fonction de journalisation de Trusted Firewall», à la page 13.
- Ajout de la rubrique «Installation de Trusted Logging», à la page 19.
- Ajout d'informations relatives aux mises à jour de correctif temporaire pour Trusted Network Connect dans «Configuration du serveur de gestion de correctifs», à la page 25.
- Ajout d'informations relatives à la fonction de génération de rapports du serveur Trusted Network Connect dans «Génération de rapports sur les serveurs TNC», à la page 31.
- Ajout d'informations relatives à l'installation du vérificateur Trusted Network Connect dans «Installation du vérificateur», à la page 7.
- Ajout des commandes Trusted Firewall dans «Commandes de PowerSC Standard Edition», à la page 32.
- Remplacement de la commande **tscpmconsole** par **pmconf** et ajout des informations la concernant dans «Commande pmconf», à la page 36.
- Remplacement de la commande **tscconsole** par **psconf** et ajout des informations la concernant dans «Commande psconf», à la page 40.
- Mise à jour des informations relatives aux options de la commande **vlantfw** dans «Commande vlantfw», à la page 46.

Novembre 2012

Mise à jour des informations contenues dans la rubrique «Trusted Network Connect and Patch management», à la page 21.

Mai 2012

Ajout de la documentation relative à nouvelle fonction pour «Trusted Firewall», à la page 10.

© Copyright IBM Corp. 2012, 2013

Concepts PowerSC Standard Edition 1.1.3

Cette présentation de PowerSC Standard Edition décrit les fonctions et les composants, ainsi que le support matériel liés à la fonction PowerSC Standard Edition.

PowerSC Standard Edition assure la sécurité et le contrôle des systèmes qui fonctionnent dans un cloud ou dans des centres de données virtualisés, et offre aux entreprises des fonctions d'affichage et de gestion. PowerSC Standard Edition est une suite de fonctions qui intègre Security and Compliance Automation, Trusted Boot, Trusted Firewall, Trusted Logging et Trusted Network Connect and Patch management. La technologie de sécurité qui est placée dans la couche de virtualisation fournit de la sécurité supplémentaire pour les systèmes autonomes.

Le tableau suivant fournit des informations détaillées sur les éditions, les fonctions incluses dans les éditions, les composants, et le matériel à base de processeur sur lequel chaque composant matériel est disponible.

Tableau 1. Composants PowerSC Standard Edition, description, système d'exploitation et matériel pris en charge

Composants	Description	Système d'exploitation pris en charge	Matériel pris en charge
Security and Compliance Automation	Permet d'automatiser le paramétrage, la surveillance et l'audit de la configuration de la sécurité et de la conformité pour les normes suivantes : • Payment Card Industry Data Security Standard (PCI DSS) • Sarbanes-Oxley Act and COBIT compliance (SOX/COBIT) • U.S. Department of Defense (DoD) STIG • Health Insurance Portability and Accountability Act (HIPAA)	• AIX 5.3 • AIX 6.1 • AIX 7.1	• POWER5 • POWER6 • POWER7
Trusted Boot	Permet de mesurer l'image d'amorçage, le système d'exploitation et les applications, et d'attester qu'ils sont dignes de confiance à l'aide de la technologie TPM virtuelle.	• AIX 6 avec 6100-07 ou version ultérieure • AIX 7 avec 7100-01 ou version ultérieure	Microprogramme POWER7 eFW7.4, ou version suivante
Trusted Firewall	Permet d''économiser du temps et des ressources en activant le routage direct dans les réseaux locaux virtuels spécifiés qui sont contrôlés par le même serveur d'E-S virtuel.	• AIX 6.1 • AIX 7.1 • VIOS version 2.2.1.4 ou suivante	• POWER6 • POWER7 • serveur d'E-S virtuel version 6.1S ou suivante
Trusted Logging	Les journaux AIX sont centralisés sur le serveur virtuel d'E/S en temps réel. Cette fonction permet de protéger la consignation contre la falsification et offre une méthode pratique de gestion et de sauvegarde des journaux.	• AIX 5.3 • AIX 6.1 • AIX 7.1	• POWER5 • POWER6 • POWER7

Tableau 1. Composants PowerSC Standard Edition, description, système d'exploitation et matériel pris en charge (suite)

Composants	Description	Système d'exploitation pris en charge	Matériel pris en charge
Trusted Network Connect and patch management	Permet de vérifier que tous les systèmes AIX présents dans l'environnement virtuel sont conformes au niveau de module de correction et de logiciel indiqué, et fournit des outils de gestion permettant de s'assurer que tous les systèmes AIX correspondent au niveau de logiciel spécifié. Fournit des alertes pour signaler qu'un système virtuel de niveau inférieur est ajouté au réseau ou qu'un correctif de sécurité affectant les systèmes est émis.	• AIX 5.3 • AIX 6.1 • AIX 7.1 Le client Trusted Network Connect requiert l'un des composants suivants : • AIX 6.1 avec kit 6100-06 ou version ultérieure • Système de console SUMA (Service Update Management Assistant) AIX version 7.1 dans l'environnement SUMA pour la gestion de correctifs	• POWER5 • POWER6 • POWER7

Installation de PowerSC Standard Edition 1.1.3

Vous devez installer un ensemble de fichiers pour chaque fonction spécifique de PowerSC Standard Edition.

Les ensembles de fichiers suivants sont disponibles pour PowerSC Standard Edition :

- `powerscExp.ice` : Installé sur des systèmes AIX qui nécessitent la fonction Security and Compliance Automation de PowerSC Standard Edition.
- `powerscStd.vtpm` : Installé sur des systèmes AIX qui nécessitent la fonction Trusted Boot de PowerSC Standard Edition.
- `powerscStd.vlog` : Installé sur des systèmes AIX qui nécessitent la fonction Trusted Logging de PowerSC Standard Edition.
- `powerscStd.tnc_pm` : Installé sur AIX version 6.1 avec niveau de technologie 6100-06 ou version ultérieure ou sur le système de console SUMA (Service Update Management Assistant) AIX version 7.1 dans l'environnement SUMA pour la gestion de correctifs.
- `powerscStd.svm` : Installé sur les systèmes AIX qui peuvent bénéficier de la fonction de routage de PowerSC Standard Edition.

Installez PowerSC Standard Edition à l'aide de l'une des interfaces suivantes :

- la commande **installp**, exécutée à partir de l'interface de ligne de commande ;
- l'interface SMIT.

Pour installer PowerSC Standard Edition à l'aide de l'interface SMIT, procédez comme suit :

1. Exécutez la commande suivante :
   ```
   % smitty installp
   ```
2. Sélectionnez l'option **Install Software**.
3. Sélectionnez l'unité ou le répertoire d'entrée pour le logiciel afin de spécifier l'emplacement et le fichier d'installation de l'image d'installation d'IBM Compliance Expert. Par exemple, si l'image d'installation contient le chemin de répertoire et le nom de fichier `/usr/sys/inst.images/powerscStd.vtpm`, vous devez spécifier le chemin de répertoire dans la zone **INPUT**.
4. Affichez et acceptez le contrat de licence. Acceptez le contrat de licence en utilisant la flèche de défilement vers le bas pour sélectionner **ACCEPT new license agreements** et appuyez sur la touche de tabulation pour sélectionner la valeur **Yes**.

5. Appuyez sur **Entrée** pour démarrer l'installation.
6. Vérifiez que la commande est à l'état **OK** une fois l'installation terminée.

Affichage de la licence logicielle

La licence logicielle peut être affichée dans l'interface de ligne de commande à l'aide de la commande suivante :

```
% installp –lE –d path/filename
```

Où *path/filename* spécifie l'image d'installation de PowerSC Standard Edition.

Par exemple, vous pouvez entrer la commande suivante à l'aide de l'interface de ligne de commande pour spécifier les informations de licence relatives à PowerSC Standard Edition :

```
% installp -lE -d  /usr/sys/inst.images/powerscStd.vtpm
```

Concepts associés :

«Concepts PowerSC Standard Edition 1.1.3», à la page 2
Cette présentation de PowerSC Standard Edition décrit les fonctions et les composants, ainsi que le support matériel liés à la fonction PowerSC Standard Edition.

«Installation de Trusted Boot», à la page 6
Certaines configurations logicielles et matérielles sont requises pour installer Trusted Boot.

«Installation de Trusted Network Connect», à la page 23
Certaines étapes sont nécessaires pour l'installation des composants de Trusted Network Connect (TNC).

Tâches associées :

«Installation de Trusted Firewall», à la page 12
La procédure d'installation de PowerSC Trusted Firewall est semblable à la procédure d'installation d'autres fonctions PowerSC.

«Installation de Trusted Logging», à la page 19
Vous pouvez installer la fonction PowerSC Trusted Logging à l'aide de l'interface de ligne de commande ou de l'outil SMIT.

Trusted Boot

La fonction Trusted Boot utilise le module VTPM (Virtual Trusted Platform Module), instance virtuelle du TPM de Trusted Computing Group. Le module VTPM permet de stocker de manière sécurisée les mesures du système d'amorçage à des fins de vérification.

Concepts Trusted Boot

Il est important de comprendre l'intégrité du processus d'amorçage, ainsi que la procédure de classification de l'amorçage en tant qu'amorçage sécurisé ou non sécurisé.

Vous pouvez configurer un maximum de 60 partitions logiques activées par VTPM (LPAR) pour chaque système physique à l'aide de la Console HMC (Hardware Management Console) (HMC). Une fois cette configuration effectuée, le module VTPM est unique pour chaque LPAR. Lorsqu'il est utilisé avec la technologie AIX Trusted Execution, le module VTPM fournit des fonctions de sécurité et d'assurance aux partitions suivantes :

- L'image d'amorçage sur le disque
- La totalité du système d'exploitation
- Les couches application

Un administrateur peut afficher les systèmes sécurisés et non sécurisés à partir d'une console centrale qui est installée avec le vérificateur **openpts** fourni avec AIX Expansion Pack. La console **openpts** gère un ou

plusieurs serveurs Power Systems et contrôle ou atteste de l'état sécurisé des systèmes AIX partout dans le centre de données. Lors du processus d'attestation, le vérificateur détermine (ou atteste) si un collecteur a effectué un amorçage sécurisé.

Etat d'amorçage sécurisé

Une partition est considérée comme sécurisée si la procédure d'attestation de l'intégrité du collecteur effectuée par le vérificateur aboutit. Le vérificateur est la partition distante qui détermine si un collecteur a effectué un amorçage sécurisé. Le collecteur est la partition AIX à laquelle un module VTPM (Virtual Trusted Platform Module) est connecté et sur laquelle la pile TSS (Trusted Software Stack) est installée. Il indique que les mesures enregistrées dans le module VTPM correspondent aux informations de références détenues par le vérificateur. Un état d'amorçage sécurisé indique si la partition a été amorcée de manière sécurisée. Cette information concerne l'intégrité du processus d'amorçage du système et ne donne aucune indication sur le niveau en cours de la sécurité du système.

Etat d'amorçage non sécurisé

Une partition passe à l'état non sécurisé si le vérificateur ne parvient pas à attester de l'intégrité du processus d'amorçage. L'état non sécurisé indique que le processus d'amorçage présente des incohérences par rapport aux informations de référence détenues par le vérificateur. Les raisons de l'échec d'une attestation sont notamment les suivantes : amorçage à partir d'une unité d'amorçage différente, amorçage d'une image de noyau différente et modification de l'image d'amorçage existante.

Concepts associés :

«Traitement des incidents liés à Trusted Boot», à la page 9
Certains des scénarios et étapes de résolution couramment utilisés sont requis pour permettre d'identifier les raisons d'un échec d'attestation lors de l'utilisation de Trusted Boot.

Planification de Trusted Boot

Découvrez les configurations matérielles et logicielles requises pour installer Trusted Boot.

Configuration prérequise pour Trusted Boot

L'installation de Trusted Boot implique de configurer le collecteur et le vérificateur.

Lorsque vous vous préparez à réinstaller le système d'exploitation AIX sur un système sur lequel la fonction Trusted Boot existe déjà, vous devez copier le fichier `/var/tss/lib/tpm/system.data` et l'utiliser pour remplacer le fichier au même emplacement une fois que l'installation est terminée. Si vous ne copiez pas ce fichier, vous devez retirer le module VTPM à partir de la console de gestion et le réinstaller sur la partition.

Collecteur

Configuration requise pour installer un collecteur :

- Matériel POWER7 qui s'exécute sur une édition de microprogramme 740
- Installer IBM AIX 6 avec niveau de technologie 7 ou IBM AIX 7 avec niveau de technologie 1
- Installer la console HMC (HMC) version 7.4 ou ultérieure
- Configurer la partition avec le module VTPM et 1 Go de mémoire au minimum
- Installer Secure Shell (SSH), plus spécifiquement OpenSSH ou une option équivalente

Vérificateur

Le vérificateur **openpts** est accessible à partir de l'interface de ligne de commande et de l'interface graphique conçue pour s'exécuter sur toute une gamme de plateformes. La version AIX du vérificateur OpenPTS est disponible sur AIX Expansion Pack. Les versions du vérificateur OpenPTS pour Linux et d'autres plateformes sont disponibles via un téléchargement du Web. Configuration requise :

- Installer SSH, plus spécifiquement OpenSSH ou une option équivalente
- Etablir une connectivité réseau (via SSH) au collecteur
- Installer Java™ 1.6 ou une version suivante pour accéder à la console **openpts** à partir de l'interface graphique

Préparation aux actions de résolution

Les informations sur Trusted Boot décrites ici vous aident à identifier les situations qui peuvent nécessiter une action de résolution. Elles ne concernent pas le processus d'amorçage.

les circonstances relatives à l'échec d'une opération d'attestation sont nombreuses, et il est difficile de les anticiper. Vous devez décider de l'action appropriée à mener en fonction de ces circonstances. Toutefois, il est recommandé d'anticiper certains scénarios sévères et de prévoir une stratégie ou un flux de travaux destiné à faciliter le traitement des incidents de ce type. L'action de résolution est la mesure corrective qui doit être prise lorsque l'attestation signale que un ou plusieurs collecteurs ne sont pas sécurisés.

Par exemple, si l'échec d'une attestation est dû au fait que l'image d'amorçage est différente de l'image de référence du vérificateur, préparez-vous à répondre aux questions suivantes :

- Comment pouvez-vous vérifier que la menace est crédible ?
- Des opérations de maintenance planifiées, une mise à jour d'AIX ou une nouvelle installation matérielle récente ont-elles été exécutées ?
- Pouvez-vous contacter l'administrateur qui a accès à ces informations ?
- Quand le système a-t-il été amorcé à l'état sécurisé pour la dernière fois ?
- Si la menace de la sécurité paraît fondée, quelle action devez-vous entreprendre ? (Les actions suggérées incluent notamment de collecter des journaux de contrôle, déconnecter le système du réseau, mettre le système hors tension et prévenir les utilisateurs.)
- D'autres systèmes ont-ils été compromis et nécessitent d'être vérifiés ?

Concepts associés :

«Traitement des incidents liés à Trusted Boot», à la page 9
Certains des scénarios et étapes de résolution couramment utilisés sont requis pour permettre d'identifier les raisons d'un échec d'attestation lors de l'utilisation de Trusted Boot.

Considérations relatives à la migration

Certaines conditions prérequises doivent être prises en compte avant de migrer une partition activée pour le module VTPM (Virtual Trusted Platform Module).

Contrairement à un module TPM physique, un module VTPM permet le déplacement de la partition entre les systèmes tout en étant conservé. Pour migrer la partition logique de façon sécurisée, le microprogramme chiffre les données VTPM avant transmission. Afin de garantir une migration sécurisée, vous devez implémenter les mesures de sécurité suivantes avant la migration :

- Activez le protocole IPSEC pour le serveur d'E-S virtuel (VIOS) qui effectue la migration.
- Définissez la clé du système authentifié via la console de gestion du matériel (HMC) afin de contrôler les systèmes gérés qui peuvent déchiffrer les données VTPM après la migration. Le système cible de la migration doit posséder la même clé que le système source pour que la migration des données puisse aboutir.

Information associée :

Utilisation de la console HMC

Migration VIOS

Installation de Trusted Boot

Certaines configurations logicielles et matérielles sont requises pour installer Trusted Boot.

Information associée :

«Installation de PowerSC Standard Edition 1.1.3», à la page 3
Vous devez installer un ensemble de fichiers pour chaque fonction spécifique de PowerSC Standard Edition.

Installation du collecteur

Vous devez installer le collecteur à l'aide de l'ensemble de fichiers du CD de base AIX.

Pour installer le collecteur, installez les packages `powerscStd.vtpm` et `openpts.collector` qui se trouvent sur le CD de base, à l'aide de la commande **smit** ou **installp**.

Installation du vérificateur

Le vérificateur OpenPTS s'exécute sur le système d'exploitation AIX et sur d'autres plateformes.

La version AIX du vérificateur peut être installée à partir de l'ensemble de fichiers à l'aide de AIX Expansion Pack. Pour installer le vérificateur sur le système d'exploitation AIX, installez le package `openpts.verifier` à partir de AIX Expansion Pack en exécutant la commande **smit** ou **installp**. Cette commande permet d'installer les versions ligne de commande et interface graphique du vérificateur.

Le vérificateur OpenPTS pour les autres systèmes d'exploitation peut être téléchargé depuis `Télécharger le vérificateur Linux OpenPTS pour une utilisation avec AIX Trusted Boot`.

Information associée :

Télécharger le vérificateur Linux OpenPTS pour une utilisation avec AIX Trusted Boot

Configuration de Trusted Boot

Découvrez la procédure d'inscription et d'attestation d'un système pour Trusted Boot.

Inscription d'un système

Découvrez la procédure d'inscription d'un système auprès du vérificateur.

Inscrire un système consiste à fournir un ensemble initial de mesures au vérificateur, ce qui constitue la base des demandes d'attestation ultérieures. Pour inscrire un système à partir de la ligne de commande, utilisez la commande suivante depuis le vérificateur :

```
openpts -i <hostname>
```

Les informations sur la partition inscrite figurent dans le répertoire `$HOME/.openpts`. Un identificateur unique est affecté à chaque nouvelle partition au cours du processus d'inscription et les informations relatives aux partitions inscrites sont enregistrées dans le répertoire correspondant à l'ID unique.

Pour inscrire un système à partir de l'interface graphique, procédez comme suit :

1. Lancez l'interface graphique en utilisant la commande **/opt/ibm/openpts_gui/openpts_GUI.sh**.
2. Sélectionnez **Enroll** dans le menu de navigation.
3. Entrez le nom d'hôte et les données d'identification SSH du système.
4. Cliquez sur **Enroll**.

Concepts associés :

«Attestation d'un système»
Découvrez la procédure permettant d'attester un système à partir de la ligne de commande et à l'aide de l'interface graphique.

Attestation d'un système

Découvrez la procédure permettant d'attester un système à partir de la ligne de commande et à l'aide de l'interface graphique.

Pour interroger l'intégrité d'un amorçage de système, utilisez la commande suivante à partir du vérificateur :

```
openpts <hostname>
```

Pour attester un système à partir de l'interface graphique, procédez comme suit :

1. Sélectionnez une catégorie dans le menu de navigation.
2. Sélectionnez un ou plusieurs systèmes à attester.
3. Cliquez sur **Attest**.

Inscription et attestation d'un système sans mot de passe

La demande d'attestation est envoyée via Secure Shell (SSH). Installez le certificat du vérificateur sur le collecteur afin d'autoriser les connexions SSH sans mot de passe.

Pour configurer le certificat du vérificateur sur le système du collecteur, procédez comme suit :

- Sur le vérificateur, exécutez les commandes suivantes :

  ```
  ssh-keygen    # No passphrase
  scp ~/.ssh/id_rsa.pub <collector>:/tmp
  ```

- Sur le collecteur, exécutez la commande suivante :

  ```
  cat /tmp/id_rsa.pub >> ~/.ssh/authorized_keys
  ```

Gestion de Trusted Boot

Découvrez la procédure de gestion des résultats d'attestation de Trusted Boot.

Interprétation des résultats d'attestation

Découvrez la procédure permettant d'afficher et de comprendre les résultats d'attestation.

L'état d'une attestation peut être l'un des suivants :

1. Echec de la demande d'attestation : la demande d'attestation n'a pas abouti. Pour comprendre les causes possibles de cette défaillance, voir la sectionTraitement des incidents.
2. L'intégrité du système est valide : la demande d'attestation a abouti, et l'amorçage du système correspond aux informations de référence détenues par le vérificateur. Cela indique un amorçage sécurisé.
3. L'intégrité du système n'est pas valide : la demande d'attestation a abouti, mais une différence a été détectée entre les informations collectées au cours de l'amorçage du système et les informations de référence détenues par le vérificateur. Cela indique un amorçage non sécurisé.

L'attestation affiche également le message suivant lorsqu'une mise à jour a été appliquée au collecteur :

Mise à jour système disponible : ce message indique qu'une mise à jour a été appliquée au collecteur et qu'un ensemble d'informations de référence mises à jour est disponible pour le prochain amorçage. L'utilisateur est invité sur le vérificateur à accepter ou à rejeter les mises à jour. Par exemple, l'utilisateur peut choisir d'accepter ces mises à jour s'il sait qu'une opération de maintenance est en cours sur le collecteur.

Pour identifier et résoudre une erreur d'attestation à l'aide des interfaces graphiques, procédez comme suit :

1. Sélectionnez une catégorie dans le menu de navigation.
2. Sélectionnez un système à examiner.
3. Cliquez deux fois sur l'entrée correspondant au système. Une fenêtre de propriétés s'affiche. Cette fenêtre contient des informations de journal sur l'attestation ayant échoué.

Suppression de systèmes

Découvrez la procédure de suppression d'un système dans la base de données du vérificateur.

Pour supprimer un système de la base de données du vérificateur, exécutez la commande suivante :

```
openpts -r <hostname>
```

Traitement des incidents liés à Trusted Boot

Certains des scénarios et étapes de résolution couramment utilisés sont requis pour permettre d'identifier les raisons d'un échec d'attestation lors de l'utilisation de Trusted Boot.

La commande **openpts** déclare un système comme non valide si l'état d'amorçage en cours de ce dernier ne correspond pas aux informations de référence détenues par le vérificateur. La commande **openpts** identifie les raisons pour lesquelles l'intégrité n'est pas valide. Plusieurs variables sont prises en compte dans le cadre d'un amorçage AIX complet, et une analyse est nécessaire pour déterminer les causes de l'échec d'une attestation.

Le tableau suivant répertorie les scénarios et étapes de résolution couramment utilisés pour identifier les causes de l'échec d'une attestation :

Tableau 2. Traitement des incidents détectés lors de l'utilisation de certains scénarios courants

Motif de l'échec	Causes possibles	Résolution recommandée

L'attestation n'a pas abouti.	• Nom d'hôte incorrect.
	• Aucune route réseau entre la source et la cible.
	• Données d'identification de sécurité incorrectes.
		Vérifiez la connexion SSH (Secure Shell) à l'aide de la commande suivante :
		`ssh ptsc@hostname`
		
		Si la connexion SSH aboutit, vérifiez les raisons possibles de l'échec d'attestation répertoriées ci-dessous :
		• Le système qui fait l'objet d'une attestation n'exécute pas le démon **tcsd**.
		• Le système qui fait l'objet d'une attestation n'exécute pas la commande **ptsc**. Ce processus doit se produire automatiquement lors du démarrage du système, mais vous devez vérifier la présence d'un répertoire `/var/ptsc/` sur le collecteur. Si le répertoire `/var/ptsc/` n'existe pas, exécutez la commande suivante sur le collecteur :
		`ptsc -i`

Le microprogramme CEC a été modifié.	• Une mise à jour de microprogramme a été appliquée. • La partition logique a été migrée vers un système qui exécutait une autre version du microprogramme.	Vérifiez le niveau de microprogramme sur le système qui héberge la partition logique.
Les ressources attribuées à la partition logique ont été modifiées.	L'unité centrale ou la mémoire attribuée à la partition logique a été modifiée.	Vérifiez le profil de partition dans la console HMC.
Le microprogramme a été modifié pour les cartes qui sont disponibles dans la partition logique.	Une unité matérielle a été ajoutée ou retirée dans la partition logique.	Vérifiez le profil de partition dans la console HMC.
La liste des unités connectées à la partition logique a été modifiée.	Une unité matérielle a été ajoutée ou retirée dans la partition logique.	Vérifiez le profil de partition dans la console HMC.

Tableau 2. Traitement des incidents détectés lors de l'utilisation de certains scénarios courants (suite)

Motif de l'échec	Causes possibles	Résolution recommandée
L'image d'amorçage a été modifiée, ce qui inclut le noyau de système d'exploitation.	• Un mise à jour AIX a été appliquée et le vérificateur n'a pas eu connaissance de cette mise à jour. • La commande **bosboot** a été exécutée.	• Demandez à l'administrateur du collecteur si des opérations de maintenance ont été effectuées avant la dernière opération de réamorçage. • Vérifiez si une activité de maintenance a été enregistrée dans les journaux du collecteur.
La partition logique a été amorcée à partir d'une autre unité.	• L'inscription a été effectuée juste après l'installation réseau. • Le système a été amorcé à partir d'une unité de maintenance.	L'unité et les indicateurs d'amorçage peuvent être vérifiés à l'aide de la commande **bootinfo**. Si l'inscription a été exécutée juste après l'installation NIM et avant l'opération de réamorçage, les détails relatifs à l'inscription concernent l'installation réseau et non l'amorçage de disque suivant. Pour réparer cette inscription, supprimez-la, puis relancez l'inscription de la partition logique.
Le menu d'amorçage SMS (System Management Services) interactif a été appelé.		Pour qu'un système puisse être sécurisé, l'exécution du processus d'amorçage ne doit pas être interrompue par une interaction d'utilisateur. Si l'utilisateur accède au menu SMS, l'amorçage est non valide.
La base de données TE (Trusted Execution) a été modifiée.	• Des fichiers binaires ont été ajoutés ou retirés dans la base de données TE. • Des fichiers binaires ont été mis à jour dans la base de données.	Exécutez la commande **trustchk** pour vérifier la base de données.

Concepts associés :

«Préparation aux actions de résolution», à la page 6
Les informations sur Trusted Boot décrites ici vous aident à identifier les situations qui peuvent nécessiter une action de résolution. Elles ne concernent pas le processus d'amorçage.

«Concepts Trusted Boot», à la page 4
Il est important de comprendre l'intégrité du processus d'amorçage, ainsi que la procédure de classification de l'amorçage en tant qu'amorçage sécurisé ou non sécurisé.

Information associée :

Utilisation de la console HMC

Trusted Firewall

La fonction Trusted Firewall fournit une solution de sécurité fonctionnant avec une couche de virtualisation pour obtenir de meilleures performances et une plus grande efficacité des ressources lors de la communication entre différentes zones de sécurité de réseau local virtuel présentes sur le même serveur Power Systems. La fonction Trusted Firewall permet de réduire la charge sur le réseau externe en déplaçant vers la couche de virtualisation la fonction de filtrage des paquets de pare-feu répondant aux règles spécifiées. Cette fonction de filtrage est contrôlée par des règles de filtrage réseau faciles à définir qui autorisent un trafic réseau sécurisé entre des zones de sécurité de réseau local virtuel sans quitter l'environnement virtuel. La fonction Trusted Firewall protège et route le trafic réseau interne entre les systèmes d'exploitation AIX, IBM i et Linux.

Concepts Trusted Firewall

Vous devez comprendre certains concepts de base pour utiliser Trusted Firewall.

Le matériel Power Systems peut être configuré avec plusieurs zones de sécurité de réseau local virtuel. Une règle configurée par l'utilisateur, créée comme règle de filtrage Trusted Firewall, permet au trafic réseau sécurisé de traverser des zones de sécurité de réseau local virtuel tout en restant interne à la

couche de virtualisation. Cela revient à introduire un pare-feu physique connecté au réseau dans l'environnement virtualisé, ce qui permet d'implémenter de façon plus performante les fonctions de pare-feu pour les centres de données virtualisés.

La fonction Trusted Firewall vous permet de configurer des règles destinées à autoriser certains types de trafic afin de transférer des informations directement depuis un réseau local virtuel sur un serveur d'E-S virtuel (VIOS) vers un autre réseau local virtuel sur le même VIOS, tout en conservant un niveau de sécurité élevé dans la mesure où les autres types de trafic sont limités. Il s'agit d'un pare-feu configurable dans la couche de virtualisation des serveurs Power Systems.

En prenant l'exemple décrit dans figure 1, l'objectif est de pouvoir transférer des informations en toute sécurité et de manière efficace depuis LPAR1 sur VLAN 200 et depuis LPAR2 sur VLAN 100. Sans la fonction Trusted Firewall, les informations ciblées pour LPAR2 depuis LPAR1 sont envoyées du réseau interne vers le routeur, ce qui réachemine les informations vers LPAR2.

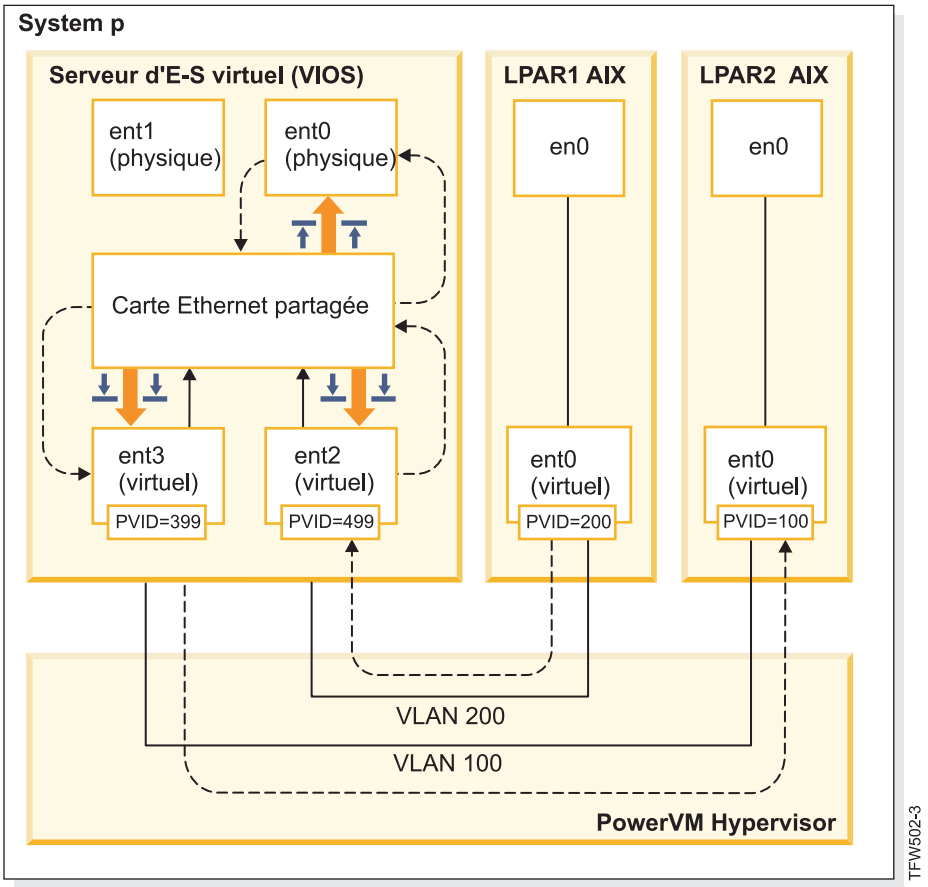

Figure 1. Exemple de transfert d'informations entre réseaux locaux virtuels sans la fonction Trusted Firewall

A l'aide de Trusted Firewall, vous pouvez configurer des règles pour autoriser le transfert d'informations entre LPAR1 et LPAR2 sans quitter le réseau interne. Ce chemin est illustré dans figure 2, à la page 12.

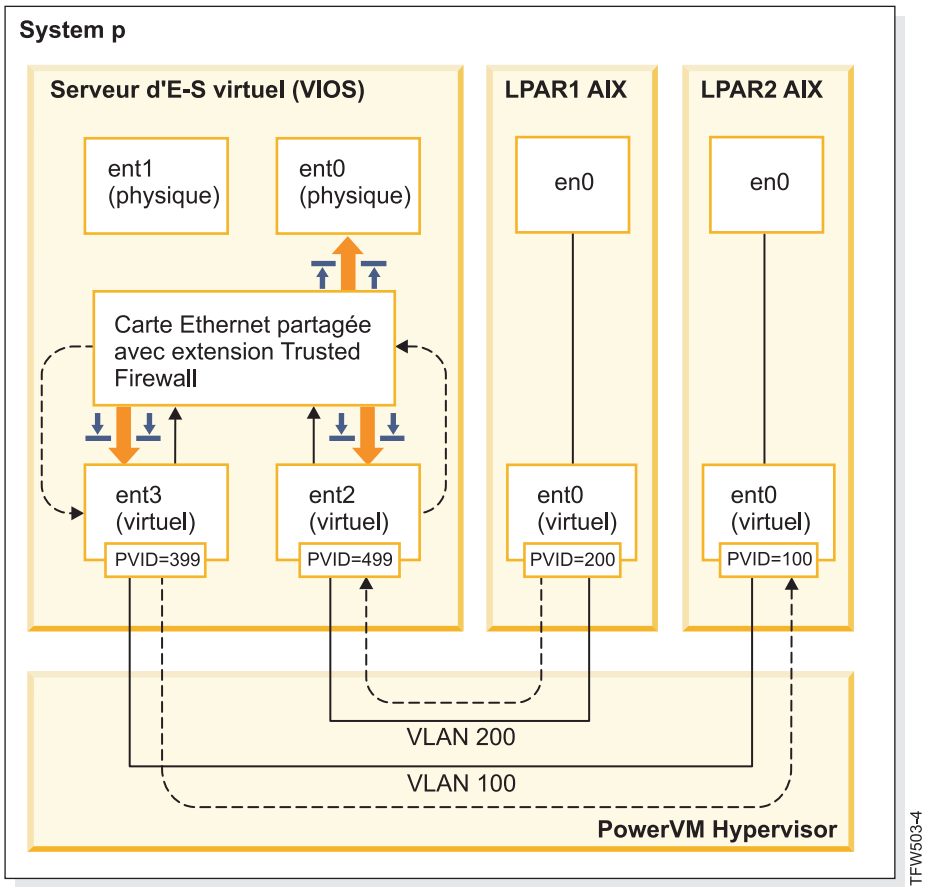

Figure 2. Exemple de transfert d'informations entre réseaux locaux virtuels avec la fonction Trusted Firewall

Les règles de configuration qui autorisent le transfert direct de certaines informations entre des réseaux locaux virtuels permettent d'acheminer ces informations plus rapidement. La fonction Trusted Firewall utilise la carte Ethernet partagée et l'extension du noyau SVM (Security Virtual Machine) pour activer la communication.

Carte Ethernet partagée
La carte Ethernet partagée est l'emplacement où débute et où se termine le routage. La carte Ethernet partagée reçoit les paquets et les transmet à la machine SVM lorsque cette dernière est enregistrée. Si la machine SVM détermine que le paquet est pour une partition logique présente sur le même serveur Power Systems, elle met à jour l'en-tête de la couche 2 du paquet. Le paquet est renvoyé à la carte Ethernet partagée pour être transmis à la destination finale au sein du système ou sur le réseau externe.

Machine SVM
La machine SVM est l'emplacement où sont appliquées les règles de filtrage. Les règles de filtrage sont nécessaires pour maintenir la sécurité sur le réseau interne. Après l'enregistrement de la machine SVM auprès de la carte Ethernet partagée, les paquets sont transmis à la machine SVM avant d'être envoyés au réseau externe. A partir des règles de filtrage actives, la machine SVM détermine si un paquet est conservé dans le réseau interne ou s'il est déplacé vers le réseau externe.

Installation de Trusted Firewall

La procédure d'installation de PowerSC Trusted Firewall est semblable à la procédure d'installation d'autres fonctions PowerSC.

Eléments prérequis :

- Les versions de PowerSC antérieures à la version 1.1.1.0 n'étaient pas dotées de l'ensemble de fichiers requis pour installer Trusted Firewall. Vérifiez que vous disposez du CD d'installation de PowerSC pour la version 1.1.1.0 ou ultérieure.
- Pour tirer parti de Trusted Firewall, vous devez avoir déjà utilisé la console HMC ou serveur d'E-S virtuel (VIOS) pour configurer vos réseaux locaux virtuels.

Trusted Firewall est fourni sous la forme d'un ensemble de fichiers supplémentaire sur le CD d'installation de PowerSC Standard Edition. Le nom de fichier est `powerscStd.svm.rte`. Vous pouvez ajouter Trusted Firewall à une instance existante de PowerSC version 1.1.0.0 ou ultérieure, ou vous pouvez l'ajouter lors d'une nouvelle installation de PowerSC version 1.1.1.0 ou ultérieure.

Pour ajouter la fonction Trusted Firewall à une instance PowerSC existante :

1. Vérifiez que vous exécutez VIOS version 2.2.1.4 ou ultérieure.
2. Insérez le CD d'installation de PowerSC pour la version 1.1.1.0 ou téléchargez l'image du CD d'installation.
3. Utilisez la commande **oem_setup_env** pour obtenir un accès root.
4. Utilisez la commande **installp** ou l'outil SMIT pour installer l'ensemble de fichiers `PowerscStd.svm.rte`.

Information associée :

«Installation de PowerSC Standard Edition 1.1.3», à la page 3
Vous devez installer un ensemble de fichiers pour chaque fonction spécifique de PowerSC Standard Edition.

Configuration de Trusted Firewall

Une fois installée, la fonction Trusted Firewall requiert des paramètres de configuration supplémentaires.

Fonction de contrôle de Trusted Firewall

La fonction de contrôle de Trusted Firewall analyse le trafic du système à partir de différentes partitions logiques afin de fournir des informations utiles permettant de déterminer si l'exécution de Trusted Firewall améliore les performances du système.

Si la fonction de contrôle de Trusted Firewall enregistre un niveau de trafic élevé à partir de différents réseaux locaux virtuels figurant sur le même processeur CEC, l'activation de Trusted Firewall devrait permettre d'améliorer les performances de votre système.

Pour activer la fonction de contrôle de Trusted Firewall, entrez la commande suivante :

```
vlantfw -m
```

Pour afficher les résultats de la fonction de contrôle de Trusted Firewall, entrez la commande suivante :

```
vlantfw -D
```

Pour désactiver la fonction de contrôle de Trusted Firewall, entrez la commande suivante :

```
vlantfw -M
```

Fonction de journalisation de Trusted Firewall

La fonction de journalisation de Trusted Firewall compile une liste des chemins du trafic réseau au sein du processeur CEC. Cette liste affiche les filtres utilisés par Trusted Firewall pour le routage du trafic.

Lorsque la fonction de contrôle de Trusted Firewall détermine que le routage du trafic permet d'améliorer les performances système, la fonction de journalisation de Trusted Firewall gère une liste de chemins dans le fichier `svm.log`. La taille du fichier `svm.log` est limitée à 16 Mo. Si la taille de ce fichier est supérieure à 16 Mo, les entrées les plus anciennes sont retirées.

| Pour démarrer la fonction de journalisation de Trusted Firewall, entrez la commande suivante :
| `vlantfw -l`

| Pour arrêter la fonction de journalisation de Trusted Firewall, entrez la commande suivante :
| `vlantfw -L`

| Vous pouvez visualiser le fichier journal à l'emplacement suivant : `/home/padmin/svm/svm.log`.

Plusieurs cartes Ethernet partagées

Vous pouvez configurer Trusted Firewall sur des systèmes qui utilisent plusieurs cartes Ethernet partagées.

Certaines configurations utilisent plusieurs cartes Ethernet partagées sur le même serveur d'E-S virtuel (VIOS). L'utilisation de plusieurs cartes Ethernet partagées peut permettre de bénéficier de la protection de reprise et du nivellement des ressources. Trusted Firewall prend en charge le routage de plusieurs cartes Ethernet partagées lorsque ces dernières figurent sur le même VIOS.

La figure 3 illustre un environnement dans lequel plusieurs cartes Ethernet partagées sont utilisées.

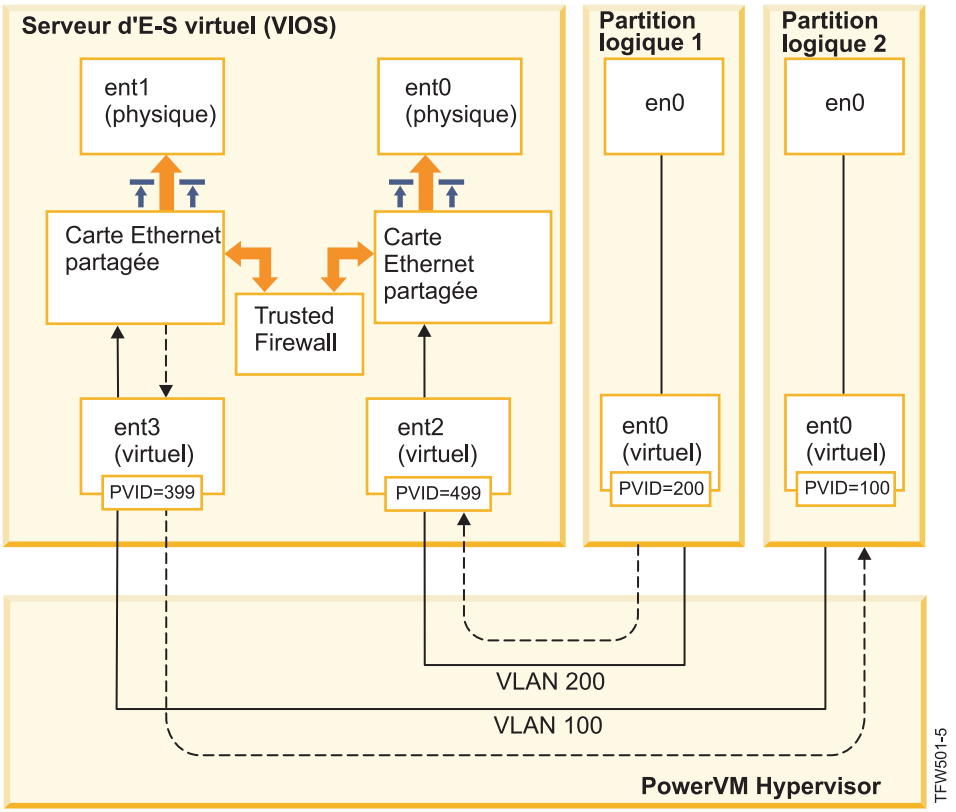

Figure 3. Configuration avec plusieurs cartes Ethernet partagées sur un VIOS

Exemples de configurations avec plusieurs cartes Ethernet partagées prises en charge par Trusted Firewall :

- Les cartes Ethernet partagées sont configurées avec des cartes de ligne réseau sur le même commutateur virtuel d'hyperviseur Power. Cette configuration est prise en charge car chaque carte Ethernet partagée reçoit du trafic réseau avec des ID de réseau local virtuel différents.
- Les cartes Ethernet partagées sont configurées avec des cartes de ligne réseau sur des commutateurs virtuels d'hyperviseur Power différents et chaque carte de ligne réseau se trouve sur un ID de réseau

local virtuel différent. Dans cette configuration, chaque carte Ethernet partagée continue de recevoir du trafic réseau en utilisant des ID de réseau local virtuel différents.

- Les cartes Ethernet partagées sont configurées avec des cartes de ligne réseau sur des commutateurs virtuels d'hyperviseur Power différents, et les mêmes ID de réseau local sont réutilisés sur les commutateurs virtuels. Dans ce cas, les mêmes ID de réseau local virtuel sont affectés au trafic pour les deux cartes Ethernet partagées.

  Voici un exemple de cette configuration : LPAR2 se trouve sur VLAN200 avec le commutateur virtuel 10 et LPAR3 figure sur VLAN200 avec le commutateur virtuel 20. Comme les deux partitions logiques et les cartes Ethernet partagées qui leur sont associées utilisent le même ID de réseau local virtuel (VLAN200), les deux cartes Ethernet partagées peuvent accéder aux paquets avec cet ID de réseau local.

Vous ne pouvez pas activer le pontage sur plusieurs VIOS. Par conséquent, les configurations avec plusieurs cartes Ethernet partagées qui sont décrites ci-dessous ne sont pas prises en charge par Trusted Firewall :

- Plusieurs VIOS et plusieurs pilotes de carte Ethernet partagée
- Partage de la charge de cartes Ethernet partagées redondantes : les cartes de ligne réseau configurées pour le routage entre les réseaux locaux virtuels ne peuvent pas être partagées entre des serveurs VIOS.

Retrait de cartes Ethernet partagées

Les étapes permettant de retirer des cartes Ethernet partagées du système doivent être exécutées dans un ordre précis.

Pour retirer une carte Ethernet partagée de votre système, procédez comme suit :

1. Retirez la machine virtuelle de sécurité qui est associée à la carte Ethernet partagée en entrant la commande suivante :

   ```
   rmdev -dev svm
   ```

2. Retirez la carte Ethernet partagée en entrant la commande suivante :

   ```
   rmdev -dev ID carte Ethernet partagée
   ```

Remarque : Le retrait de la carte Ethernet partagée avant le module SVM peut provoquer une défaillance du système.

Création de règles

Vous pouvez activer des règles pour autoriser le routage Trusted Firewall entre des réseaux locaux virtuels.

Pour activer les fonctions de routage de Trusted Firewall, vous devez créer des règles qui définissent les communications autorisées. Afin de renforcer la sécurité, il n'existe aucune règle unique autorisant la communication entre tous les réseaux locaux virtuels sur le système. Chaque connexion autorisée requiert sa propre règle, et chaque règle activée autorise la communication dans les deux sens pour les points d'extrémité spécifiés.

La création de règle étant exécutée dans l'interface serveur d'E-S virtuel (VIOS), des informations supplémentaires sur les commandes sont disponibles dans l'ensemble de rubriques VIOS du centre de documentation matériel Power Systems.

Pour créer une règle, procédez comme suit :

1. Ouvrez l'interface de ligne de commande du VIOS.
2. Initialisez le pilote SVM en entrant la commande suivante :

   ```
   mksvm
   ```

3. Démarrez Trusted Firewall en entrant la commande suivante :

   ```
   vlantfw -s
   ```

4. Pour afficher toutes les adresses MAC et IP LPAR connues, entrez la commande suivante :

   ```
   vlantfw -d
   ```

   Vous aurez besoin des adresses MAC et IP des partitions logiques pour lesquelles vous créez des règles.
5. Créer la règle de filtrage qui permet la communication entre les deux partitions logiques (LPAR1 et LPAR2) en entrant l'une des commandes suivantes
   - `genvfilt -v4 -a P -z [lpar1vlanid] -Z [lpar2vlanid] -s [lpar1ipaddress] -d [lpar2ipaddress]`
   - `genvfilt -v4 -a P -z [lpar1vlanid] -Z [lpar2vlanid] -s [lpar1ipaddress] -d [lpar2ipaddress]-o any -p 0 -O gt -P 23`

   Remarque : Une règle de filtrage autorise de communication dans les deux sens par défaut, en fonction du port et des entrées de protocole. Par exemple, vous pouvez activer Telnet entre LPAR1 et LPAR2 en exécutant la commande suivante :

   ```
   genvfilt -v4 -a-P -z [lpar1vlanid] -Z [lpar2vlanid] -s [lpar1ipaddress] -d [lpar2ipaddress] -o any -p 0 -O eq -P 23
   ```

6. Activez toutes les règles de filtrage dans le noyau en entrant la commande suivante :

   ```
   mkvfilt -u
   ```

Remarque : Cette procédure permet d'activer cette règle et les autres règles de filtrage présentes sur le système.

Autres exemples

Les exemples ci-après illustrent d'autres règles de filtrage que vous pouvez créer à l'aide de Trusted Firewall.

- Pour autoriser une communication Secure Shell entre la partition logique sur le réseau local virtuel 100 et la partition logique sur le réseau local virtuel 200, entrez la commande suivante :

  ```
  genvfilt -v4 -a P -z 100 -Z 200 -o any -p 0 -O eq -P 22 -c tcp
  ```

- Pour autoriser le trafic entre tous les ports compris entre 0 et 499, entrez la commande suivante :

  ```
  genvfilt -v4 -a P -z 100 -z 200 -o lt -p 500 -O lt -P 500 -c tcp
  ```

- Pour autoriser le trafic TCP entre les partitions logiques, entrez la commande suivante :

  ```
  genvfilt -v4 -a P -z 100 -Z 200 -c tcp
  ```

  Si vous ne spécifiez pas de port ni d'opération sur des ports, le trafic peut utiliser tous les ports.
- Pour autoriser la messagerie ICMP (protocole de message de gestion interréseau) entre les partitions logiques, entrez la commande suivante :

  ```
  genvfilt -v4 -a P -z 100 -Z 200 -c icmp
  ```

Concepts associés :

«Désactivation de règles»
Vous pouvez désactiver les règles qui autorisent le routage entre réseaux locaux virtuels dans la fonction Trusted Firewall.

Référence associée :

«Commande genvfilt», à la page 34

«Commande mkvfilt», à la page 36

«Commande vlantfw», à la page 46

Information associée :

Serveur d'E-S virtuel (Virtual I/O Server ou VIOS)

Désactivation de règles

Vous pouvez désactiver les règles qui autorisent le routage entre réseaux locaux virtuels dans la fonction Trusted Firewall.

La désactivation des règles étant exécutée dans l'interface serveur d'E-S virtuel (VIOS), des informations supplémentaires sur les commandes sont disponibles dans l'ensemble de rubriques VIOS du centre de documentation matériel Power Systems.

Pour désactiver une règle, procédez comme suit :

1. Ouvrez l'interface de ligne de commande du VIOS.
2. Pour afficher toutes les règles de filtrage actives, entrez la commande suivante :

   ```
   lsvfilt -a
   ```

   Vous pouvez omettre l'indicateur **-a** pour afficher toutes les règles de filtrage stockées dans Object Data Manager.
3. Notez le numéro d'identification de la règle de filtrage que vous désactivez. Dans le cadre de cet exemple, le numéro d'identification de la règle de filtrage est 23.
4. Désactivez la règle de filtrage 23 lorsqu'elle est active dans le noyau, en entrant la commande suivante :

   ```
   rmvfilt -n 23
   ```

   Pour désactiver toutes les règles de filtrage dans le noyau, entrez la commande suivante :

   ```
   rmvfilt -n all
   ```

Concepts associés :

«Création de règles», à la page 15
Vous pouvez activer des règles pour autoriser le routage Trusted Firewall entre des réseaux locaux virtuels.

Référence associée :

«Commande lsvfilt», à la page 35

«Commande rmvfilt», à la page 45

Trusted Logging

La fonction PowerVM Trusted Logging permet aux partitions logiques AIX d'écrire dans des fichiers journaux enregistrés sur un serveur d'E-S virtuel (VIOS) connecté. Les données sont transmises au VIOS directement via l'hyperviseur, et aucune connectivité réseau n'est requise entre la partition logique du client et le VIOS.

Journaux virtuels

L'administrateur serveur d'E-S virtuel (VIOS) crée et gère les fichiers journaux ; ceux-ci sont présents sur le système d'exploitation AIX en tant qu'unités de journal virtuel dans le répertoire `/dev`, de la même manière que les disques virtuels ou les supports optiques virtuels.

Le stockage de fichiers journaux en tant que journaux virtuels augmente le niveau de confiance relatif aux enregistrements car ils ne peuvent pas être modifiés par un utilisateur disposant des droits root sur la partition logique du client où ils sont générés. Plusieurs unités de journal virtuel peuvent être connectées à la même partition logique de client et chaque journal correspond à un fichier différent dans le répertoire `/dev`.

La fonction Trusted Logging permet de consolider des données de journal provenant de plusieurs partitions logiques de client en un seul système de fichiers, lequel est accessible à partir du VIOS. Ainsi, le VIOS fournit un emplacement unique sur le système pour l'analyse et l'archivage des journaux. L'administrateur de partitions logiques de client peut configurer des applications et le système d'exploitation AIX pour l'écriture de données sur les unités de journal virtuel, ce qui revient à écrire des données sur les fichiers locaux. Le sous-système de contrôle AIX peut être configuré pour diriger les enregistrements de contrôle vers des journaux virtuels, et d'autres services AIX, tels que syslog, peuvent être configurés pour fonctionner avec leur configuration existante afin de diriger des données vers des journaux virtuels.

Pour configurer le journal virtuel, l'administrateur VIOS doit lui affecter un nom, composé comme suit :

- Nom du client
- Nom du journal

L'administrateur VIOS peut affecter n'importe quel nom aux deux composants, mais le nom du client est généralement identique pour tous les journaux virtuels qui sont connectés à une partition logique donnée (par exemple, le nom d'hôte de partition logique). Le nom de journal permet d'identifier l'objectif de la journalisation (par exemple, contrôle ou syslog).

Sur une partition logique AIX, chaque unité de journal virtuel est présente sous la forme de fichiers équivalents du point de vue fonctionnel dans le système de fichiers `/dev`. Le premier fichier est nommé d'après l'unité, par exemple `/dev/vlog0`, et le second fichier est nommé en concaténant un préfixe `vl` avec le nom de journal et le numéro d'unité. Par exemple, si l'unité de journal virtuel `vlog0` a pour nom de journal `audit`, elle existe dans le système de fichiers `/dev` sous la forme des deux fichiers `vlog0` et `vlaudit0`.

Information associée :

Création de journaux virtuels

Détection des unités de journal virtuel

Une fois qu'un administrateur VIOS a créé et connecté des unités de journal virtuel à une partition logique de client, la configuration des unités de partition logique du client doit être actualisée de sorte que les unités soient affichées.

L'administrateur des partitions logiques du client actualise les paramètres en procédant de l'une des façons suivantes :

- Réamorçage de la partition logique du client
- Exécution de la commande **cfgmgr**

Exécutez la commande **lsdev** pour afficher les unités de journal virtuel. Par défaut, les unités sont précédées du préfixe `vlog`. Voici un exemple de sortie générée par la commande **lsdev** sur une partition logique AIX comportant deux unités de journal virtuel :

```
lsdev
vlog0  Virtual Log Device
vlog1  Virtual Log Device
```

Examinez les propriétés d'une unité de journal virtuel à l'aide de la commande `lsattr –El <device name>`, qui génère une sortie semblable à celle illustrée ci-dessous :

```
lsattr –El vlog0
PCM                         Path Control Module            False
client_name    dev-lpar-05 Client Name                     False
device_name    vlsyslog0   Device Name                     False
log_name       syslog      Log Name                        False
max_log_size   4194304     Maximum Size of Log Data File  False
max_state_size 2097152     Maximum Size of Log State File False
pvid           none        Physical Volume Identifier     False
```

Cette sortie affiche le nom du client, le nom de l'unité et la quantité de données de journal que le VIOS peut stocker.

Deux types de données de journal sont stockés par le journal virtuel :

- Données de journal : Données de journal brutes générées par des applications sur la partition logique AIX.
- Données d'état : Informations indiquant à quel moment les unités ont été configurées, ouvertes et fermées et concernant d'autres opérations. Ces informations sont utilisées pour analyser les activités de journalisation.

L'administrateur VIOS spécifie la quantité de **données de journal** et de **données d'état** qui peut être stocké pour chaque journal virtuel. Pour ce faire, il utilise les attributs `max_log_size` et `max_state_size`. Lorsque la quantité de données stockées dépasse la limite spécifiée, les données de journal les plus anciennes sont écrasées. L'administrateur VIOS doit s'assurer que les données de journal sont fréquemment collectées et archivées pour préserver les journaux.

Installation de Trusted Logging

Vous pouvez installer la fonction PowerSC Trusted Logging à l'aide de l'interface de ligne de commande ou de l'outil SMIT.

Les éléments prérequis pour l'installation de Trusted Logging sont les suivants : VIOS version 2.2.1.0 ou ultérieure et IBM AIX 6 avec niveau de technologie 7 or IBM AIX 7 avec niveau de technologie 1.

Le nom de fichier pour l'installation de la fonction Trusted Logging est `powerscStd.vlog` ; il figure sur le CD d'installation de PowerSC Standard Edition.

Pour installation la fonction Trusted Logging :

1. Prenez soin d'exécuter VIOS version 2.2.1.0 ou ultérieure.
2. Insérez le CD d'installation de PowerSC ou téléchargez l'image du CD d'installation.
3. Utilisez la commande **installp** ou l'outil SMIT pour installer l'ensemble de fichiers `powerscStd.vlog`.

Information associée :

«Installation de PowerSC Standard Edition 1.1.3», à la page 3
Vous devez installer un ensemble de fichiers pour chaque fonction spécifique de PowerSC Standard Edition.

Configuration de la journalisation sécurisée

Découvrez la procédure de configuration de la journalisation sécurisée sur le sous-système de contrôle AIX et syslog.

Configuration du sous-système de contrôle AIX

Le sous-système de contrôle AIX peut être configuré pour l'écriture de données binaires sur une unité de journal virtuel en plus de l'écriture de journaux sur le système de fichiers local.

Remarque : Avant de configurer le sous-système de contrôle AIX, vous devez exécuter la procédure décrite dans «Détection des unités de journal virtuel», à la page 18.

Pour configurer le sous-système de contrôle AIX, procédez comme suit :

1. Configurez le sous-système de contrôle AIX pour qu'il écrive des données au format binaire (`auditbin`).
2. Activez la journalisation sécurisée pour le contrôle AIX en éditant le fichier de configuration `/etc/security/audit/config`.
3. Ajoutez un paramètre `virtual_log = /dev/vlog0` à la strophe `bin:`.

   Remarque : L'instruction est valide si l'administrateur LPAR souhaite que les données `auditbin` soient écrites dans `/dev/vlog0`.
4. Redémarrez le sous-système de contrôle AIX en respectant l'ordre suivant :

   ```
   audit shutdown
   audit start
   ```

Les enregistrements de contrôle sont écrits sur serveur d'E-S virtuel (VIOS) via l'unité de journal virtuel spécifiée en plus des journaux écrits sur le système de fichiers local. Le stockage des journaux est régi par les paramètres `bin1` et `bin2` existant dans la strophe `bin:` du fichier de configuration `/etc/security/audit/config`.

Information associée :

Sous-système de contrôle

Configuration de syslog

Syslog peut être configuré pour écrire des messages dans des journaux virtuels en ajoutant des règles au fichier `/etc/syslog.conf`.

Remarque : Avant de configurer le fichier `/etc/syslog.conf`, vous devez exécuter la procédure décrite dans «Détection des unités de journal virtuel», à la page 18.

Vous pouvez éditer le fichier `/etc/syslog.conf` pour qu'il corresponde aux messages de journal, lesquels sont basés sur les critères suivants :

- Fonction
- Niveau de priorité

Pour utiliser les journaux virtuels pour les messages syslog, vous devez configurer le fichier `/etc/syslog.conf` avec des règles qui prévoient que les messages souhaités doivent être écrits dans le journal virtuel approprié dans le répertoire `/dev`.

Par exemple, pour envoyer des messages de niveau débogage générés par une fonction quelconque dans le journal virtuel `vlog0`, ajoutez la ligne suivante dans le fichier `/etc/syslog.conf` :

```
*.debug /dev/vlog0
```

Remarque : N'utilisez pas les fonctions de rotation de journal qui sont disponibles dans le démon `syslogd` pour une commande qui écrit des données dans des journaux virtuels. Les fichiers présents dans le système de fichiers `/dev` ne sont pas des fichiers standard et ne peuvent pas être renommés ni déplacés. L'administrateur VIOS doit configurer la rotation de journal virtuel dans le VIOS.

Le démon `syslogd` doit être redémarré après la configuration à l'aide de la commande suivante :

```
refresh -s syslogd
```

Information associée :

Démon syslogd

Ecriture de données sur des unités de journal virtuel

L'écriture de données arbitraires sur une unité de journal virtuel s'effectue en ouvrant le fichier approprié dans le répertoire `/dev` et en écrivant les données dans le fichier. Un journal virtuel peut être ouvert par un seul processus à la fois.

Par exemple :

La commande **echo** permettant d'écrire des messages sur les unités de journal virtuel est la suivante :

```
echo "Log Message" > /dev/vlog0
```

La commande **cat** permettant de stocker des fichiers sur les unités de journal virtuel est la suivante :

```
cat /etc/passwd > /dev/vlog0
```

La taille d'écriture maximale individuelle est limitée à 32 ko, et les programmes qui tentent d'écrire une quantité de données plus élevée en une seule fois reçoivent un message d'erreur d'E-S. Les utilitaires de l'interface de ligne de commande, tels que la commande **cat**, scindent automatiquement les transferts en opérations d'écriture de 32 ko.

Trusted Network Connect and Patch management

Trusted Network Connect (TNC) fait partie du groupe TCG (Trusted Computing Group) qui fournit des spécifications permettant de vérifier l'intégrité des points d'extrémité. TNC est doté d'une architecture de solution ouverte qui aide les administrateurs à appliquer des règles destinées à renforcer le contrôle des accès à l'infrastructure réseau.

Concepts Trusted Network Connect

Découvrez les composants, la configuration de la communication sécurisée et le système de gestion de correctifs de la fonction Trusted Network Connect (TNC).

Composants Trusted Network Connect

Découvrez les composants de l'infrastructure préfabriquée Trusted Network Connect (TNC).

Le modèle TNC comprend les composants suivants :

Serveur Trusted Network Connect :

Le serveur Trusted Network Connect (TNC) identifie les clients qui sont ajoutés au réseau, puis il les vérifie.

Le client TNC fournit au serveur les informations de niveau ensemble de fichiers requis pour vérification. Le serveur détermine si le niveau d'installation du client correspond à celui qui a été configuré par l'administrateur. Si tel n'est pas le cas, le serveur TNC informe l'administrateur qu'une action de résolution est nécessaire.

Le serveur TNC lance des vérifications sur les clients qui tentent d'accéder au réseau. Le serveur TNC charge un ensemble de vérificateurs de mesure d'intégrité (IMV) qui peuvent demander des mesures d'intégrité aux clients et il vérifie ces derniers. Un module IMV est installé par défaut sous AIX ; il vérifie l'ensemble de fichiers et le niveau de correctif de sécurité des systèmes. Le serveur TNC est une infrastructure préfabriquée qui charge et gère plusieurs modules IMV. Il s'appuie sur les modules IMV pour demander des informations aux clients et il vérifie ces derniers.

Gestion de correctifs :

Le serveur Trusted Network Connect (TNC) s'intègre au module SUMA pour fournir une solution de gestion de correctifs.

Le module SUMA d'AIX télécharge les derniers Service Packs et correctifs de sécurité disponibles sur les sites IBM ECC et Fix Central. Le démon TNC and patch management insère sur le serveur TNC les dernières informations mises à jour, lesquelles constituent un ensemble de fichiers de référence pour la vérification des clients.

Le démon **tncpmd** doit être configuré pour gérer les téléchargements du module SUMA (Service Update Management Assistant) et pour insérer les informations d'ensemble de fichiers sur le serveur TNC. Ce démon doit être hébergé sur un système qui est connecté à Internet pour pouvoir télécharger les mises à jour automatiquement. Pour utiliser le serveur de gestion de correctifs TNC sans le connecter à Internet, vous pouvez enregistrer un référentiel de correctifs défini par l'utilisateur auprès du serveur de gestion de correctifs TNC.

Remarque : Le serveur TNC et le démon **tncpmd** peuvent être hébergés sur le même système.

Client Trusted Network Connect :

Le client Trusted Network Connect (TNC) fournit les informations requises par le serveur TNC à des fins de vérification.

Le serveur détermine si le niveau d'installation du client correspond à celui qui a été configuré par l'administrateur. Si tel n'est pas le cas, le serveur TNC informe l'administrateur que des mises à jour sont nécessaires.

Le client TNC charge les modules IMC lors du démarrage et il les utilise pour collecter les informations requises.

Référenceur IP Trusted Network Connect :

Le serveur Trusted Network Connect (TNC) peut lancer automatiquement la vérification sur les clients qui font partie du réseau. Le référenceur IP qui s'exécute sur la partition serveur d'E-S virtuel (VIOS) détecte les nouveaux clients qui sont gérés par le VIOS et envoie leurs adresses IP au serveur TNC. Le serveur TNC vérifie le client par rapport à la règle qui est définie.

Communication Trusted Network Connect sécurisée

Les démons TNC communiquent via les canaux chiffrés qui sont activés par le protocole TLS (Transport Layer Security) ou la couche SSL (Secure Sockets Layer).

La communication sécurisée permet de garantir l'authentification et la sécurisation des données et des commandes qui transitent sur le réseau. Chaque système doit posséder sa propre clé et son propre certificat, lesquels sont générés lors de l'exécution de la commande d'initialisation des composants. Ce processus est complètement transparent pour l'administrateur et nécessite moins d'intervention de sa part.

Pour vérifier un nouveau client, son certificat doit être importé dans la base de données du serveur. Au départ, le certificat est marqué comme non sécurisé, et l'administrateur entre la commande **psconf** suivante pour afficher et marquer le certificat comme étant sécurisé :

```
psconf certadd –i<ip> -t<TRUSTED|UNTRUSTED>
```

Si vous souhaitez utiliser une autre clé et un autre certificat, la commande **psconf** fournit l'option permettant d'importer le certificat.

| Pour importer le certificat à partir du serveur, entrez la commande suivante :

```
psconf import  -S -k<key filename> -f<key filename>
```

| Pour importer le certificat à partir du client, entrez la commande suivante :

```
psconf import -C -k<key filename> -f<key filename>
```

Protocole Trusted Network Connect

Le protocole Trusted Network Connect (TNC) est utilisé avec l'infrastructure préfabriquée TNC pour assurer l'intégrité du réseau.

TNC fournit des spécifications pour vérifier l'intégrité des points d'extrémité. Les points d'intégrité qui demandent un accès sont évalués en fonction des mesures d'intégrité des composants critiques susceptibles d'affecter leur environnement fonctionnel. L'infrastructure préfabriquée TNC permet aux administrateurs de contrôler l'intégrité des systèmes du réseau. La fonction TNC est intégrée à l'infrastructure de distribution des correctifs d'AIX pour générer une solution de gestion de correctifs complète.

Les spécifications TNC doivent satisfaire aux exigences de l'architecture système AIX et Gamme POWER. Les composants de TNC ont été conçus pour fournir une solution de gestion de correctifs complète sur le système d'exploitation AIX. Cette configuration permet aux administrateurs de gérer efficacement la configuration logicielle sur les déploiements AIX. Elle fournit les outils permettant de vérifier les niveaux de correctif des systèmes et de générer un rapport sur les clients qui ne sont pas conformes. En outre, la gestion de correctifs permet de simplifier le téléchargement et l'installation des correctifs.

Modules IMC et IMV

Le serveur ou le client TNC (Trusted Network Connect) utilise en interne les modules IMC (collecteur de mesure d'intégrité) et IMV (vérificateur de mesure d'intégrité) pour effectuer la vérification du serveur.

Cette infrastructure préfabriquée permet le chargement de plusieurs modules IMC et IMV dans le serveur et les clients. Le module chargé de vérifier le niveau de système d'exploitation et d'ensemble de fichiers est livré par défaut avec le système d'exploitation AIX. Pour accéder aux modules qui sont livrés avec le système d'exploitation AIX, utilisez l'un des chemins suivants :

- `/usr/lib/security/tnc/libfileset_imc.a` : Collecte le niveau du système d'exploitation et les informations sur l'ensemble de fichiers qui est installé à partir du système client et les envoie au module IMV (serveur TNC) pour vérification.
| - `/usr/lib/security/tnc/libfileset_imv.a` : Demande au client le niveau du système d'exploitation et
| les informations sur l'ensemble de fichiers afin de les comparer avec les informations de référence. Il
| procède également à la mise à jour de l'état du client dans la base de données du serveur TNC. Pour
| afficher l'état, entrez la commande suivante :

```
psconf list -s<COMPLIANT|IGNORE|FAILED|ALL>-i<ip|ALL> [-c] [-q]
```

Référence associée :

«Commande psconf», à la page 40

Installation de Trusted Network Connect

Certaines étapes sont nécessaires pour l'installation des composants de Trusted Network Connect (TNC).

Pour définir la configuration permettant d'utiliser les composants de TNC, procédez comme suit :

1. Identifiez les adresses IP des systèmes pour configurer le serveur TNC, le serveur TNCPM (Trusted Network Connect and Patch Management) et le référenceur IP TNC pour le serveur d'E-S virtuel (VIOS).

   Remarque : Le serveur TNC ne peut pas être configuré en tant que client TNC.
2. Configurez le serveur NIM. Le système qui est configuré en tant que serveur est le maître NIM, et les ensembles de fichiers `sets:bos.sysmgt.nim.master` doivent être installés sur le système client.

3. Configurez le serveur TNCPM. Cette configuration peut être définie sur le système NIM. Le serveur TNCPM utilise le système de console SUMA pour télécharger les correctifs à partir des sites Web IBM Fix Central et ECC. Pour que les mises à jour puissent être téléchargées, le système doit être connecté à Internet : Entrez la commande suivante pour configurer le serveur TNCPM :

   ```
   pmconf mktncpm [pmport=<port>]tncserver=<host:port>
   ```

   Par exemple :

   ```
   pmconf mktncpm pmport=20000 tncserver=1.1.1.1:10000
   ```

4. Configurez les règles sur le serveur TNC. Pour créer les règles de vérification des clients, voir «Création de règles pour le client Trusted Network Connect», à la page 28.
5. Configurez le référenceur IP TNC sur VIOS. Cette configuration sur VIOS permet de déclencher la vérification des clients qui se connectent au réseau. Entrez la commande suivante pour configurer le référenceur :

   ```
   psconf mkipref tncport=<port> tncserver=<ip:port>
   ```

   Par exemple :

   ```
   psconf mkipref tncport=10000 tncserver=1.1.1.1:10000
   ```

   Remarque : La valeur du port de serveur et celle du port TNC (port de client) doivent être identiques.
6. Configurez les clients à l'aide de la commande suivante :

   ```
   psconf mkclient tncport=<port> tncserver=<serverip>:<port>
   ```

   Par exemple :

   ```
   psconf mkclient tncport=10000 tncserver=10.1.1.1:10000
   ```

Référence associée :

«Commande psconf», à la page 40

Information associée :

«Installation de PowerSC Standard Edition 1.1.3», à la page 3
Vous devez installer un ensemble de fichiers pour chaque fonction spécifique de PowerSC Standard Edition.

Installation à l'aide de NIM

IBM Fix Central

Centre d'aide en ligne pour Passport Advantage

Configuration de Trusted Network Connect and Patch management

Vous devez configurer Trusted Network Connect (TNC) comme un démon de gestion de correctifs. Le serveur TNC s'intègre au module SUMA pour fournir une solution de gestion de correctifs complète.

Configuration du serveur Trusted Network Connect

Découvrez la procédure de configuration du serveur TNC.

Pour que le serveur TNC puisse être configuré, une valeur semblable à la suivante doit être spécifiée dans le fichier `/etc/tnccs.conf` :

```
component = SERVER
```

Pour configurer un système en tant que serveur, entrez la commande suivante :

```
psconf mkserver tncport=<port> pmserver=<ip|hostname[,ip2|hostname2..]:port>
[recheck_interval=<time in mins>]
```

Par exemple :

```
psconf mkserver tncport=10000 pmserver=2.2.2.2:20000 recheck_interval=20
```

Remarque : Le port `tncport` et le port `pmserver` doivent être définis avec des valeurs différentes, et si la valeur du paramètre `recheck_interval` n'est pas indiquée, une valeur par défaut de 1440 minutes est utilisée.

La valeur utilisée par défaut pour le port `tncport` est 42830 minutes et la valeur par défaut du port `pmserver` est 38240 minutes.

Référence associée :

«Commande psconf», à la page 40

Configuration du client Trusted Network Connect

Découvrez la procédure de configuration du client Trusted Network Connect (TNC) et les paramètres de configuration requis.

Pour que le client puisse être configuré, une valeur semblable à la suivante doit être spécifiée dans le fichier `/etc/tnccs.conf` :

```
component = CLIENT
```

Pour configurer un système en tant que client, entrez la commande suivante :

```
psconf mkclient tncport=<port> tncserver=<ip:port>
```

Par exemple :

```
psconf mkclient tncport=10000 tncserver=1.1.1.1:10000
```

Remarque : La valeur du port de serveur et la valeur `tncport` (port de client) doivent être identiques.

Référence associée :

«Commande psconf», à la page 40

Configuration du serveur de gestion de correctifs

Découvrez la procédure de configuration d'un système en tant que serveur de gestion de correctifs.

Le serveur de gestion de correctifs Trusted Network Connect (TNC) doit être configuré sur le serveur NIM (Network Installation Management) de manière à permettre la mise à jour des clients TNC.

Pour initialiser les répertoires de correctifs pour la gestion de correctifs TNC, entrez la commande suivante :

```
pmconf init -i <download interval> -l <TL list> [-A] [-P <download path>][-x <ifix interval>]
[-K <ifix key>]
```

Voici un exemple de la commande **pmconf** :

```
pmconf init -i 1440 -l 6100-07,7100-01
```

La commande **init** télécharge le dernier Service Pack pour chaque niveau de technologie et le met à la disposition du serveur TNC. Les Service Packs mis à jour permettent au serveur TNC d'exécuter une vérification de client TNC de référence, et permettent au serveur de gestion de correctifs TNC d'installer les mises à jour de client TNC. Spécifiez l'indicateur **-A** pour accepter tous les contrats de licence lorsque vous exécutez les mises à jour de client. Par défaut, les répertoires de correctifs qui sont téléchargés par le serveur de gestion de correctifs TNC se trouvent dans le fichier `/var/tnc/tncpm/fix_repository`. Utilisez l'indicateur **-P** pour spécifier un autre répertoire.

Pour activer le téléchargement automatique des recommandations de sécurité IBM et des correctifs temporaires correspondants, vous pouvez spécifier un intervalle pour ces deniers. Cette fonction permet

d'envoyer automatiquement des notifications lorsque des correctifs temporaires de sécurité et les identificateurs CVE qui leur sont associés sont publiés. Toutes les recommandations de sécurité et tous les correctifs temporaires correspondants sont vérifiés avant d'être enregistrés auprès de TNC. La clé publique de vulnérabilité IBM AIX, requise pour activer le téléchargement automatique des correctifs temporaires, est disponible sur le site Web de sécurité IBM AIX. Les téléchargements automatiques de Service Packs et de correctifs temporaires sont désactivés en affectant la valeur 0 à l'intervalle de téléchargement et à l'intervalle de correctif temporaire.

Vous pouvez également mettre à jour manuellement l'enregistrement de Service Pack et de correctif temporaire. Pour enregistrer manuellement une recommandation de sécurité IBM avec les correctifs temporaires qui lui sont associés, entrez la commande suivante :

```
pmconf add -y <advisory file> -v <signature file>  -e <ifix tar file>
```

Pour enregistrer manuellement un correctif temporaire autonome, entrez la commande suivante :

```
pmconf add -p <SP> -e <ifix file>
```

Pour enregistrer un nouveau niveau technologique et télécharger le dernier Service Pack qui lui est associé, entrez la commande suivante :

```
pmconf add -l <TL list>
```

Pour télécharger un Service Pack qui n'est pas le plus récent ou pour télécharger le niveau technologique à utiliser pour la vérification et les mise à jour de client, entrez la commande suivante :

```
pmconf add -l <TL list> -d
pmconf add -s <SP List>
```

Pour enregistrer un Service Pack ou un référentiel de correctifs de niveau technologique existant sur le système, entrez la commande suivante :

```
pmconf add -s <SP> -p <user_defined_fix_repository>
pmconf add -l <TL> -p <user_defined_fix_repository>
```

Pour configurer un système en tant que serveur de gestion de correctifs, entrez la commande suivante :

```
pmconf mktncpm [pmport=<port>] tncserver=ip_list[:port]
```

Voici un exemple de cette commande :

```
pmconf mktncpm pmport=20000 tncserver=1.1.1.1:100000
```

Le serveur de gestion de correctifs TNC prend toujours en charge la gestion des APAR. Entrez la commande suivante pour configurer la gestion de correctifs TNC afin de gérer d'autres types d'APAR :

```
pmconf add -t <APAR_type_list>
```

Dans l'exemple précédent, <APAR_type_list> est une liste séparée par des virgules qui répertorie les types d'APAR suivants :

- HIPER
- PE
- Enhancement

Le serveur de gestion de correctifs TNC prend en charge **syslog** pour télécharger le Service Pack, le niveau technologique et les mises à jour de client. La fonction est `user` et le niveau de priorité est `info`. Par exemple, `user.info`.

Le serveur de gestion de correctifs TNC gère également un journal contenant toutes les mises à jour de client dans le répertoire `/var/tnc/tncpm/log/update/<ip>/<timestamp>`.

Référence associée :

«Commande psconf», à la page 40

Information associée :

Sécurité IBM AIX

Configuration de la notification par courrier électronique pour le serveur Trusted Network Connect

Découvrez la procédure permettant de configurer la notification par courrier électronique pour le serveur Trusted Network Connect (TNC).

Le serveur TNC vérifie le niveau de module de correction du client et si ce dernier n'est pas conforme, le serveur TNC envoie un courrier électronique à l'administrateur avec le résultat et l'action de résolution requise.

Pour configurer l'adresse électronique de l'administrateur, entrez la commande suivante :

```
psconf add –e <email_id>[ipgroup=[±]G1, G2 ..]
```

Par exemple :

```
psconf add –e abc@ibm.com ipgroup=vayugrp1,vayugrp2
```

Dans l'exemple précédent, le courrier électronique pour le groupe IP *vayugrp1* et *vayugrp2* est envoyé à l'adresse abc@ibm.com.

Pour envoyer un courrier électronique à une adresse de courrier électronique globale pour le groupe IP auquel aucune adresse de courrier électronique n'est affectée, entrez la commande suivante :

```
psconf add –e <mailaddress>
```

Par exemple :

```
psconf add –e abc@ibm.com
```

Dans l'exemple précédent, si aucune adresse de courrier électronique n'est affectée à un groupe IP, le courrier électronique est envoyé à l'adresse de courrier électronique abc@ibm.com. Elle agit comme une adresse de courrier électronique globale.

Référence associée :

«Commande psconf», à la page 40

Configuration du référenceur IP sur VIOS

Découvrez la procédure de configuration du référenceur IP sur serveur d'E-S virtuel (VIOS) pour lancer automatiquement le processus de vérification.

Remarque : Vous devez configurer l'extension du noyau SVM sur le serveur virtuel d'entrée-sortie avant de configurer le référenceur IP.

Pour que le référenceur IP TNC puisse être configuré, un paramètre semblable au suivant doit être spécifié dans le fichier de configuration `/etc/tnccs.conf` : `component = IPREF`.

Vous pouvez configurer un système en tant que client en entrant la commande suivante :

```
psconf mkipref tncport=<port> tncserver=<ip:port>
```

Par exemple :

```
psconf mkipref tncport=10000 tncserver=1.1.1.1:10000
```

La valeur du port de `tncserver` et la valeur `tncport` (port de client) doivent être identiques.

Référence associée :

«Commande psconf», à la page 40

Gestion de Trusted Network Connect and Patch management

Découvrez la procédure de gestion de Trusted Network Connect (TNC) pour implémenter des tâches, telles que l'ajout des clients, règles, journaux et résultats de vérification, et la mise à jour des clients et des certificats liés à TNC.

Affichage des journaux du serveur Trusted Network Connect

Découvrez la procédure permettant d'afficher les journaux du serveur Trusted Network Connect (TNC).

Le serveur TNC enregistre dans un journal les résultats relatifs à la vérification de tous les clients. Pour afficher le journal, exécutez la commande **psconf** :

```
psconf list –H –i <ip |ALL>
```

Référence associée :

«Commande psconf», à la page 40

Création de règles pour le client Trusted Network Connect

Découvrez la procédure de configuration de règles relatives au client Trusted Network Connect (TNC).

La console `psconf` fournit l'interface requise pour gérer les règles TNC. Chaque client ou un groupe de clients peut être associé à une règle.

Les règles suivantes peuvent être créées :

- Un groupe IP (Internet Protocol) contient plusieurs adresses IP client.
- Chaque IP client peut appartenir à un seul groupe.
- Le groupe IP est associé à un groupe de règles.
- Un groupe de règles contient différents types de règles. Par exemple, la règle d'ensemble de fichiers qui spécifie le niveau du système d'exploitation du client (c'est-à-dire l'édition, le niveau technologique et le Service Pack). Un groupe de règles peut contenir plusieurs règles d'ensemble de fichiers et le niveau du client qui fait référence à cette règle doit correspondre au niveau spécifié par l'une des règles d'ensemble de fichiers.

Les commandes suivantes permettent de créer un groupe IP, un groupe de règles et des règles d'ensemble de fichiers.

Pour créer un groupe IP, entrez la commande suivante :

```
psconf add –G <ipgrpname> ip=[±]<ip1,ip2,ip3 ...>
```

Par exemple :

```
psconf add –G myipgrp ip=1.1.1.1,2.2.2.2
```

Remarque : Pour un groupe, au moins un IP doit être fourni. Plusieurs IP doivent être séparés par une virgule.

Pour créer une règle d'ensemble de fichiers, entrez la commande suivante :

```
psconf add –F <fspolicyname> <rel00-TL-SP>
```

Par exemple :

```
psconf add –F myfspol  6100-02-03 aparlist=IY0001,IY0002
```

Remarque : Les informations de génération doivent être spécifiées au format `<rel00-TL-sp>`.

| Pour créer une règle et affecter un groupe IP, entrez la commande suivante :

```
| psconf add –P <policyname> ipgroup=[±] <ipgrp1, ipgrp2 ...]
```

| Par exemple :

```
| psconf add –P mypol ipgroup=myipgrp,myipgrp1
```

Pour affecter une règle d'ensemble de fichiers à une règle, entrez la commande suivante :

```
psconf add –P <policyname> fspolicy=[±]<fspol1, fspol2 ...>
```

Par exemple :

```
psconf add –P mypol fspolicy=myfspol,myfspol1
```

Remarque : Si plusieurs règles d'ensemble de fichiers sont fournies, celle qui correspond le mieux au client est appliquée par le système. Par exemple, si le client figure sur `6100-02-01` et que vous indiquez `7100-03-04` et `6100-02-03` comme règle d'ensemble de fichiers, le système applique `6100-02-03` au client.

Référence associée :

«Commande psconf», à la page 40

Démarrage de la vérification du client Trusted Network Connect

Découvrez la procédure de vérification du client TNC (Trusted Network Connect).

Pour procéder à la vérification du client, utilisez l'une des méthodes suivantes :

- Le démon du référenceur IP sur le serveur d'E-S virtuel (VIOS) transmet l'IP client au serveur TNC : Le client LPAR acquiert l'IP et tente d'accéder au réseau. Le démon du référenceur IP sur VIOS détecte la nouvelle adresse IP et la transmet au serveur TNC : Le serveur TNC lance la vérification dès qu'il reçoit la nouvelle adresse IP.
- Le serveur TNC vérifie le client régulièrement : L'administrateur peut ajouter les IP client qui doivent être vérifiées dans la base de données de règles TNC. Le serveur TNC vérifie les clients qui se trouvent dans la base de données. La nouvelle vérification se produit automatiquement à intervalles réguliers en fonction de la valeur d'attribut `recheck_interval` spécifiée dans le fichier de configuration `/etc/tnccs.conf`.
- L'administrateur lance la vérification du client manuellement : L'administrateur peut vérifier manuellement si un client est ajouté au réseau en exécutant la commande suivante :

  ```
  tncconsole verify -i <ip>
  ```

Remarque : Pour les ressources qui ne sont pas connectées à un VIOS, les clients peuvent être vérifiés et mis à jour lorsqu'ils sont ajoutés manuellement au serveur TNC.

Référence associée :

«Commande psconf», à la page 40

Affichage des résultats de la vérification du client Trusted Network Connect

Découvrez la procédure permettant d'afficher les résultats de la vérification du client Trusted Network Connect (TNC).

| Pour afficher les résultats de la vérification des clients du réseau, entrez la commande suivante :

```
| psconf list -s ALL -i ALL
```

| Cette commande permet d'afficher tous les clients qui sont à l'état **IGNORED**, **COMPLIANT** ou **FAILED**.

| • **IGNORED** : L'IP du client est ignoré dans la liste des IP (le client peut être exempté de vérification).
| • **COMPLIANT** : Le processus de vérification du client a abouti (le client est conforme à la règle).
| • **FAILED** : Le processus de vérification du client a échoué (le client n'est pas conforme à la règle et une | action d'administration est requise).

Pour connaître la raison de l'échec de la vérification, exécutez la commande **psconf** en indiquant l'IP du client ayant échoué :

```
psconf list -s ALL -i <ip>
```

Référence associée :

«Commande psconf», à la page 40

Mise à jour du client Trusted Network Connect

Le serveur Trusted Network Connect (TNC) vérifie un client et met la base de données à jour avec l'état de ce dernier et les résultats de la vérification. L'administrateur peut afficher ces résultats et procéder à la mise à jour du client.

Pour mettre à jour un client installé avec un niveau antérieur, entrez la commande suivante :

```
psconf update -i <ip> -r <buildinfo> [-a apar1,apar2...]
```

Par exemple :

```
psconf update –i 4.4.4.4 –r 6100-02-03 –a IY0004
```

La commande **psconf** met le client à jour avec la version et les installations de partition logique, le cas échéant.

Référence associée :

«Commande psconf», à la page 40

Gestion des règles de gestion de correctifs

La commande **pmconf** permet de configurer les règles de gestion de correctifs.

Les règles de gestion de correctifs fournissent des informations, telles que l'adresse IP du serveur TNC et l'intervalle de temps pour lancer la mise à jour SUMA.

Pour gérer la règle de gestion de correctifs, entrez la commande suivante :

```
pmconf mktncpm [pmport=<port>] tncserver=<host:port>
```

Par exemple :

```
pmconf mktncpm pmport=2000 tncserver=10.1.1.1:1000
```

Remarque : Les valeurs de `pmport` et de `tncserver` doivent être différentes.

Référence associée :

«Commande pmconf», à la page 36

Importation de certificats Trusted Network Connect

Découvrez la procédure permettant d'importer un certificat et de transmettre des données en toute sécurité au sein du réseau.

Les démons TNC communiquent via les canaux chiffrés qui sont activés à l'aide du protocole TLS (Transport Layer Security) ou SSL (Secure Sockets Layer). Ces démons garantissent que les données et les commandes qui transitent dans le réseau sont authentifiées et sécurisées. Chaque système possède sa propre clé et son propre certificat, lesquels sont générés lors de l'exécution de la commande d'initialisation des composants. Ce processus est transparent pour l'administrateur et nécessite moins d'intervention de sa part. Lorsqu'un client est vérifié pour la première fois, son certificat est importé dans la base de données du serveur. Au départ, le certificat est marqué comme non sécurisé, et l'administrateur entre la commande **psconf** suivante pour afficher et marquer le certificat comme étant sécurisé :

```
psconf certadd –i <ip> -t <TRUSTED|UNTRUSTED>
```

Si l'administrateur souhaite utiliser une autre clé et un autre certificat, la commande **psconf** fournit la fonction permettant de les importer.

Pour importer le certificat à partir d'un serveur, entrez la commande suivante :

```
psconf import  -S -k <key filename> -f <filename>
```

Pour importer le certificat à partir d'un client, entrez la commande suivante :

```
psconf import -C -k <key filename> -f <filename>
```

Référence associée :

«Commande psconf», à la page 40

Génération de rapports sur les serveurs TNC

Le serveur Trusted Network Connect (TNC) prend en charge le format CSV et la format de sortie texte pour afficher le rapport CVE (Common Vulnerabilities and Exposures), le rapport IBM Security Advisory, le rapport sur les règles du serveur TNC, le rapport sur les correctifs de sécurité du client TNC et le rapport sur les Service Packs enregistrés et les correctifs temporaires qui leur sont associés.

Le rapport CVE affiche toutes les vulnérabilités et menaces courantes relatives aux Service Packs enregistrés. Pour afficher les résultats de ce rapport, entrez la commande suivante :

```
psconf report -v {CVEid|ALL} -o {TEXT|CSV}
```

Le rapport IBM Security Advisory affiche les vulnérabilités de sécurité connues relatives aux logiciels IBM installés. Pour afficher les résultats de ce rapport, entrez la commande suivante :

```
psconf report -A <advisoryname>
```

Le rapport sur les règles de sécurité du serveur TNC affiche les règles de sécurité appliquées sur le serveur TNC. Pour afficher les résultats de ce rapport, entrez la commande suivante :

```
psconf report -P {policyname|ALL} -o {TEXT|CSV}
```

Le rapport sur les correctifs de client TNC affiche les correctifs temporaires manquants et installés pour le client TNC. Pour afficher les résultats de ce rapport, entrez la commande suivante :

```
psconf report -i {ip|ALL} -o {TEXT|CSV}
```

Vous pouvez également exécuter un rapport qui génère la liste des Service Packs enregistrés avec les APAR et les correctifs temporaires qui leur sont associés. Pour afficher les résultats de ce rapport, entrez la commande suivante :

```
psconf report -B {buildinfo|ALL} -o {TEXT|CSV}
```

Référence associée :

«Commande psconf», à la page 40

Traitement des incidents liés à Trusted Network Connect and Patch management

Découvrez les causes possibles de défaillance, ainsi que les étapes permettant de traiter les incidents liés à TNC and Patch management.

Pour traiter les incidents liés à TNC and Patch management, vérifiez les paramètres de configuration répertoriés dans le tableau ci-après.

Tableau 3. Traitement des incidents liés aux paramètres de configuration pour les systèmes TNC and Patch management

Problème	Solution
Le serveur TNC ne démarre pas ou ne répond pas	Procédez comme suit : 1. Entrez la commande suivante pour déterminer si le démon de serveur TNC est en cours d'exécution : `ps –eaf | grep tnccsd` 2. S'il n'est pas en cours d'exécution, supprimez le fichier `/var/tnc/.tncsock`. 3. Redémarrez le serveur. Si le problème persiste, vérifiez l'entrée `component = SERVER` dans le fichier de configuration `/etc/tnccs.conf` sur le serveur TNC.
Le serveur de gestion de correctifs TNC ne démarre pas ou ne répond pas	• Entrez la commande suivante pour déterminer si le démon de serveur de gestion de correctifs TNC est en cours d'exécution : `ps –eaf | grep tncpmd` • Vérifiez l'entrée `component = TNCPM` dans le fichier de configuration `/etc/tnccs.conf` sur le serveur de gestion de correctifs TNC.
Le client TNC ne démarre pas ou ne répond pas	• Entrez la commande suivante pour déterminer si le démon de client TNC est en cours d'exécution : `ps –eaf | grep tnccsd` • Vérifiez l'entrée `component = CLIENT` dans le fichier de configuration `/etc/tnccs.conf` sur le client TNC.
Le référenceur IP TNC n'est pas en cours d'exécution sur serveur d'E-S virtuel (VIOS)	• Entrez la commande suivante pour déterminer si le démon de référenceur IP TNC est en cours d'exécution : `ps –eaf | grep tnccsd` • Vérifiez l'entrée `component = IPREF` dans le fichier de configuration `/etc/tnccs.conf` sur VIOS.
Impossible de configurer un système comme serveur et client TNC	Le serveur et le client TNC ne peuvent pas s'exécuter simultanément sur le même système.
Les démons sont en cours d'exécution, mais la vérification ne s'exécute pas	Activez la journalisation des messages pour les démons. Définissez le niveau de journalisation `level=info` dans le fichier `/etc/tnccs.conf`. Vous pouvez analyser les messages de journal.

Commandes de PowerSC Standard Edition

PowerSC Standard Edition fournit les commandes qui pemettent d'activer la communication avec le composant Trusted Firewall et le composant Trusted Network Connect à partir de la ligne de commande.

commande chvfilt

Objectif

Modifie les valeurs de la règle de filtrage inter réseau local virtuel existante.

Syntaxe

chvfilt [-v <4|6>] -n fid [-a <D|P>] [-z <svlan>] [-Z <dvlan>] [-s <s_addr>] [-d <d_addr>] [-o <src_port_op>] [-p <src_port>] [-O <dst_port_op>] [-P <dst_port>] [-c <protocol>]

Description

La commande **chvfilt** permet de modifier la définition d'une règle de filtrage inter-réseau local virtuel dans la table des règles de filtrage.

Indicateurs

-a Indique l'action. Les valeurs admises sont les suivantes :
- D (Deny) : Bloque le trafic
- P (Permit) : Autorise le trafic

-c Indique les différents protocoles auxquels s'applique la règle de filtrage. Les valeurs admises sont les suivantes :
- udp
- icmp
- icmpv6
- tcp
- any

-d Indique l'adresse de destination au format IPv4 ou IPv6.

-m Indique le masque d'adresse source.

-M Indique le masque d'adresse de destination.

-n Indique l'ID de filtre de la règle de filtrage qui doit être modifiée.

-o Indique le port source ou une opération de type ICMP (protocole de message de gestion interréseau). Les valeurs admises sont les suivantes :
- lt
- gt
- eq
- any

-O Indique le port de destination ou l'opération de code ICMP. Les valeurs admises sont les suivantes :
- lt
- gt
- eq
- any

-p Indique le port source ou le type ICMP.

-P Indique le port de destination ou le code ICMP.

-s Indique l'adresse source au format v4 ou v6.

-v Indique la version IP de la table de règles de filtrage. Les valeurs admises sont 4 et 6.

-z Indique l'ID de réseau local virtuel de la partition logique source.

-Z Indique l'ID de réseau local virtuel de la partition logique de destination.

Etat de sortie

Cette commande renvoie les valeurs de sortie suivantes :

0 L'opération a abouti.

>0 Une erreur s'est produite.

Exemples

1. Pour modifier une règle de filtrage valide qui existe dans le noyau, entrez la commande comme suit :
   ```
   chvfilt -n 1 -v4 -a P -z 100 -Z 300 -o eq -p 23 -O lt -P 345 -c tcp
   ```
2. Si une règle de filtrage (n=2) ne figure pas dans le noyau, la sortie se présente comme suit :
   ```
   chvfilt -n 2 -v4 -a P -z 100 -Z 300 -o eq -p 23 -O lt -P 345 -c tcp
   ```

   Le système affiche la sortie comme suit :
   ```
   ioctl(QUERY_FILTER) failed no filter rule err=2
   Cannot Change the filter rule.
   ```

Commande genvfilt

Objectif

Permet d'ajouter une règle de filtrage pour le croisement VLAN entre les partitions logiques sur le même serveur IBM Power Systems.

Syntaxe

genvfilt -v <**4**|**6**> **-a** <**D**|**P**> **-z** <**svlan**> **-Z** <**dvlan**> [**-s** <**s_addr**>] [**-d** <**d_addr**>] [**-o** <**src_port_op**>] [**-p** <**src_port**>] [**-O** <**dst_port_op**>] [**-P** <**dst_port**>] [**-c** <**protocol**>]

Description

La commande **genvfilt** permet d'ajouter une règle de filtrage pour le croisement VLAN entre les partitions logiques sur le même serveur IBM Power Systems.

Indicateurs

-a Indique l'action. Les valeurs admises sont les suivantes :
- D (Deny) : Bloque le trafic
- P (Permit) : Autorise le trafic

-c Indique les différents protocoles auxquels s'applique la règle de filtrage. Les valeurs admises sont les suivantes :
- udp
- icmp
- icmpv6
- tcp
- any

-d Indique l'adresse de destination au format v4 ou v6.

-m Indique le masque d'adresse source.

-M Indique le masque d'adresse de destination.

-o Indique le port source ou une opération de type ICMP (protocole de message de gestion interréseau). Les valeurs admises sont les suivantes :
- lt
- gt
- eq
- any

-0 Indique le port de destination ou l'opération de code ICMP. Les valeurs admises sont les suivantes :
- lt

- gt
- eq
- any

-p Indique le port source ou le type ICMP.

-P Indique le port de destination ou le code ICMP.

-s Indique l'adresse source au format IPv4 ou IPv6.

-v Indique la version IP de la table de règles de filtrage. Les valeurs admises sont 4 et 6.

-z Indique l'ID de réseau local virtuel de la partition logique source. L'ID de réseau local virtuel doit être compris entre 1 et 4096.

-Z Indique l'ID de réseau local virtuel de la partition logique de destination. L'ID de réseau local virtuel doit être compris entre 1 et 4096.

Etat de sortie

Cette commande renvoie les valeurs de sortie suivantes :

0 L'opération a abouti.

>0 Une erreur s'est produite.

Exemples

1. Pour ajouter une règle de filtrage qui autorise les données TCP d'un ID VLAN source 100 vers un ID VLAN de destination 200 sur des ports spécifiques, entrez la commande qui suit :

```
genvfilt -v4 -a P -z 100 -Z 200  -o lt -p 345 -O lt -P 345 -c tcp
```

Référence associée :

«Commande mkvfilt», à la page 36

«Commande vlantfw», à la page 46

Commande lsvfilt

Objectif

Permet d'afficher la liste des règles de filtrage inter-réseaux locaux virtuels à partir de la table de filtres.

Syntaxe

lsvfilt [**-a**]

Description

La commande **lsvfilt** d'afficher la liste des règles de filtrage inter-réseaux locaux virtuels à partir de la table de filtres ainsi que leur état.

Indicateurs

-a Affiche uniquement la liste des règles de filtrage actives.

Etat de sortie

Cette commande renvoie les valeurs de sortie suivantes :

0 L'opération a abouti.

>0 Une erreur s'est produite.

Exemples

1. Pour afficher la liste de toutes les règles de filtrage actives du noyau, entrez la commande comme suit :

```
lsvfilt -a
```

Concepts associés :

«Désactivation de règles», à la page 17
Vous pouvez désactiver les règles qui autorisent le routage entre réseaux locaux virtuels dans la fonction Trusted Firewall.

Commande mkvfilt

Objectif

Permet d'activer les règles de filtrage inter-réseaux locaux virtuels définies par la commande **genvfilt**.

Syntaxe

mkvfilt -u

Description

La commande **mkvfilt** permet d'activer les règles de filtrage inter-réseaux locaux virtuels définies par la commande **genvfilt**.

Indicateurs

-u Active les règles de filtrage dans la table des règles de filtrage.

Etat de sortie

Cette commande renvoie les valeurs de sortie suivantes :

0 L'opération a abouti.

>0 Une erreur s'est produite.

Exemples

1. Pour activer les règles de filtrage du noyau, entrez la commande comme suit :

```
mkvfilt -u
```

Référence associée :

«Commande genvfilt», à la page 34

Commande pmconf

Objectif

Permet d'effectuer des opérations de génération de rapports et de gestion pour le serveur Trusted Network Connect Patch Management (TNCPM) en enregistrant les niveaux technologiques et les serveurs TNC afin de recevoir les derniers correctifs et en générant des rapports sur l'état de TNCPM.

Remarque : Le serveur TNCPM doit être exécuté uniquement sous AIX version 7.1 avec le niveau technologique 7100-02 pour autoriser le téléchargement des métadonnées de Service Pack.

Syntaxe

pmconf mktncpm [**pmport=**<*port*>] **tncserver=***ip* | hostname **:** *port*

pmconf rmtncpm

pmconf start

pmconf stop

| **pmconf init -i** <*download interval*> **-l** <*TL List*> **-A** [**-P** <*download path*>] [**-x** <*ifix interval*>] [**-K** <*ifix*
| *key*>]

pmconf add -l *TL_list*

pmconf add -p <*SP List*> [**-U** <*user-defined SP path*>]

| **pmconf add -p** <*SP*> **-e** <*ifix file*>

| **pmconf add -y** <*advisory file*> **-v** <*signature file*> **-e** <*ifix tar file*>

pmconf delete -l *TL_list*

pmconf delete -p <*SP List*>

| **pmconf delete -p** <*SP*>**-e** *ifix file*

pmconf list -s [**-c**] [**-q**]

pmconf list -l *SP*

pmconf list -C

pmconf list -a *SP*

pmconf hist -u

pmconf hist -d

pmconf import -f *cert_filename* **-k** *key_filename*

pmconf export -f *filename*

pmconf modify -i < *download interval*>

pmconf modify -P <*download path*>

pmconf modify -g <*yes or no to accept all licenses*>

pmconf modify -t <*APAR type list*>

| **pmconf modify -x** <*ifix interval*>

| **pmconf modify -K** <*ifix key*>

pmconf delete -l <*TL list*>

pmconf restart

pmconf status

pmconf log loglevel = info | error | none

pmconf chtncpm attribute = *value*

Description

Les fonctions de la commande **pmconf** sont les suivantes :

Gestion de référentiel de correctifs
Permet d'enregistrer ou de désenregistrer les niveaux technologiques, et de désenregistrer les serveurs TNC. TNCPM crée un référentiel de correctifs pour chaque niveau technologique qui contient les derniers correctifs, les informations **lslpp** (par exemple, les informations sur les ensembles de fichiers installés ou les mises à jour d'ensemble de fichiers) et les informations de correctif de sécurité pour ce niveau technologique.

Génération de rapports
Permet de générer des rapport sur l'état de TNCPM.

La commande **pmconf** permet d'exécuter les opérations suivantes :

Elément	Description
add	Permet d'enregistrer un nouveau niveau technologique à l'aide de TNCPM.
chtncpm	Permet de modifier les attributs contenus dans le fichier tnccs.conf. Une commande **start** explicite est nécessaire pour que les modifications soient effectives dans le serveur TNCPM.
delete	Permet de désenregistrer un niveau technologique à l'aide de TNCPM.
history	Permet d'afficher l'historique de mise à jour et de téléchargement.
list	Permet d'afficher les informations sur TNCPM.
log	Permet de définir le niveau de journalisation pour les composants TNC.
mktncpm	Permet de créer le serveur TNCPM.
modify	Permet de modifier les attributs de tncpm.conf.
rmtncpm	Permet de supprimer le serveur TNCPM.
start	Permet de démarrer le serveur TNCPM.
stop	Permet d'arrêter le serveur TNCPM.

Options

Elément	Description
-A	Permet d'accepter tous les contrats de licence lors des opérations de mises à jour client.
-a <advisory file>	Permet de spécifier un fichier de recommandation correspondant au paramètre **ifix**. Si le fichier de recommandation n'est pas fourni, le paramètre **ifix** n'est pas considéré comme une adresse CVE du correctif temporaire.
-e <ifix file>	Permet de spécifier les correctifs temporaires qui sont ajoutés au serveur TNCPM.
-i *download_interval*	Permet de spécifier la fréquence à laquelle TNCPM vérifie la présence d'un nouveau Service Pack pour les niveaux technologiques enregistrés. Cet intervalle est un nombre entier qui représente des minutes ou exprimé au format suivant **d** (nb de jours): **h** (heures): **m** (minutes).
-K <ifix key>	Permet de spécifier la clé publique de l'outil IBM AIX Product Security Incident Response Tool (PSIRT) qui est utilisé pour authentifier les recommandations et les correctifs temporaires téléchargés. Cette clé publique peut être téléchargée à partir d'un serveur de clés publiques PGP à l'aide de l'ID **0x28BFAA12**.
-p *SP_list*	Permet de spécifier la liste des Service Packs à télécharger. Il s'agit d'une liste séparée par des virgules utilisant le format REL00-TL-SP (par exemple, `6100-01-04` représente le Service Pack 04 pour le niveau technologique 01 et la version 6.1). Lorsque vous utilisez l'option -U, spécifiez un seul Service Pack.
-t *APAR_type_list*	Permet de spécifier les types d'APAR pris en charge par TNCPM pour les listes de mise à jour client et de serveur TNC. Les APAR de sécurité sont toujours pris en charge. APAR_type_list est une liste séparée par des virgules contenant les types suivants : HIPER, FileNet Process Engine, Enhancement.
-P *fix_repository_path*	Permet de spécifier le répertoire téléchargé pour les référentiels de correctifs qui seront téléchargés par TNCPM. Le répertoire par défaut est **/var/tnc/tncpm/fix_repository**.

Elément	Description
-U *user_defined_fix_repository*	Permet de spécifier le chemin d'accès au répertoire de référentiels défini par l'utilisateur. Spécifiez l'édition, le niveau technologique et le Service Pack qui sont associés au référentiel de correctifs utilisé pour la vérification et les mises à jour des clients.
-s	Permet de générer un rapport sur les Service Packs enregistrés.
-l *SP*	Permet de générer un rapport sur les informations **lslpp** relatives au Service Pack. *SP* est au format REL00-TL-SP (par exemple, `6100-01-04` représente le Service Pack 04 pour le niveau technologique 01 et la version 6.1).
-u	Permet de générer un rapport sur l'historique de mise à jour client.
-d	Permet de générer un rapport sur l'historique de téléchargement de Service Pack.
-C	Permet de générer un rapport sur le certificat de serveur.
-a *SP*	Permet de générer un rapport officiel d'analyse de programme pour le Service Pack. *SP* est au format REL00-TL-SP (par exemple, `6100-01-04` représente le Service Pack 04 pour le niveau technologique 01 et la version 6.1).
-f *filename*	Permet de spécifier le nom du fichier certificat.
-k *key_filename*	Permet de spécifier le fichier à partir duquel la clé de certificat doit être lue dans le cas d'une importation.

-c	Permet d'afficher les attributs utilisateur dans des enregistrements séparés par un deux-points, comme suit :
	`# name: attribute1 : attribute2 : ...`
	`policy: value1 : value2 : ...`

-v *<signature file>*	Permet de spécifier le fichier de signature relatif à la recommandation de vulnérabilité IBM AIX.
-y *<advisory file>*	Permet de spécifier le fichier de recommandation de vulnérabilité IBM AIX.
-q	Permet de supprimer les informations d'en-tête.
-x *<ifix interval>*	Permet de spécifier le nombre de minutes observé entre chaque processus de recherche et téléchargement de nouveaux correctifs temporaires. Si cette valeur est égale à 0, le processus de notification et téléchargement automatique de correctif temporaire est désactivé. L'intervalle par défaut est de 24 heures.

Etat de sortie

Cette commande renvoie les valeurs de sortie suivantes :

Elément	Description
0	L'exécution de la commande a abouti, et toutes les modifications demandées ont été effectuées.
>0	Une erreur s'est produite Le message d'erreur imprimé contient des informations détaillées sur le type de la défaillance.

Exemples

1. Pour initialiser TNCPM, entrez la commande suivante :
   ```
   pmconf init -f 10080 -l 5300-11,6100-00
   ```
2. Pour créer le démon TNCPM, entrez la commande suivante :
   ```
   mktncpm pmport=55777 tncserver=11.11.11.11:77555
   ```
3. Pour démarrer le serveur, entrez la commande suivante :
   ```
   pmconf start
   ```
4. Pour arrêter le serveur, entrez la commande suivante :
   ```
   pmconf stop
   ```
5. Pour enregistrer un nouveau niveau technologique à l'aide de TNCPM, entrez la commande suivante :
   ```
   pmconf add -l 6100-01
   ```
6. Pour désenregistrer un niveau technologique de TNCPM, entrez la commande suivante :
   ```
   pmconf delete -l 6100-01
   ```
7. Pour désenregistrer de TNCPM un serveur TNC dont l'adresse IP est 11.11.11.11, entrez la commande suivante :
   ```
   pmconf delete -t 11.11.11.11
   ```
8. Pour enregistrer une version plus récente d'un Service Pack antérieur sur TNCPM, entrez la commande suivante :
   ```
   pmconf add -s 6100-01-04
   ```

9. Pour désenregistrer un Service Pack antérieur de TNCPM, entrez la commande suivante :
   ```
   pmconf delete -s 6100-01-04
   ```
10. Pour générer un rapport sur les référentiels de correctifs pour chaque niveau technologique enregistré, entrez la commande suivante :
    ```
    pmconf list -s
    ```
11. Pour générer un rapport sur les informations **lslpp** d'un niveau technologique enregistré, entrez la commande suivante :
    ```
    pmconf list -l 6100-01-02
    ```
12. Pour générer un rapport sur l'historique de mise à jour, entrez la commande suivante :
    ```
    pmconf hist -u
    ```
13. Pour générer un rapport sur l'historique de téléchargement, entrez la commande suivante :
    ```
    pmconf hist -d
    ```
14. Pour générer un rapport sur le certificat du serveur, entrez la commande suivante :
    ```
    pmconf list -C
    ```
15. Pour générer un rapport sur les informations APAR de sécurité d'un Service Pack, entrez la commande suivante :
    ```
    pmconf list -a 6100-01-02
    ```
16. Pour importer un certificat de serveur, entrez la commande suivante :
    ```
    pmconf import -f /tmp/server.txt -k /tmp/server-cert-key.txt
    ```
17. Pour exporter un certificat de serveur, entrez la commande suivante :
    ```
    pmconf export -f /tmp/server.txt
    ```

Commande psconf

Objectif

Permet d'effectuer des opérations de génération de rapports et de gestion pour le serveur Trusted Network Connect (TNC), le client TNC, le référenceur IP TNC (IPRef) et le module SUMA (Service Update Management Assistant). Elle permet de gérer des règles de gestion d'ensemble de fichiers et de correctifs par rapport à l'intégrité du point d'extrémité (serveur et client) pendant ou après la connexion la connexion réseau afin de protéger le réseau contre des menaces et des attaques.

Syntaxe

Opérations serveur TNC :

psconf mkserver [**tncport=**<*port*>] **pmserver=**<*host*:*port*> [tsserver=<host>] [**recheck_interval=**<*time_in_minutes*> | **d** (days) : **h** (hours) : **m** (minutes)] [**dbpath** = <*user-defined directory*>]

psconf { **rmserver** | **status** }

psconf { **start** | **stop** | **restart** } **server**

psconf chserver attribute = *value*

psconf add -F <*FSPolicyname*> -r <*buildinfo*> [**apargrp= [±]**<*apargrp1, apargrp2.. >*] [*ifixgrp*=[+|-]<*ifixgrp1,ifixgrp2...>*]

psconf add { **-G** <*ipgroupname*> **ip=[±]**<*host1, host2...*> | {**-A**<*apargrp*> [**aparlist**=**[±]***apar1, apar2...* | {**-V** <*ifixgrp*> [*ifixlist*=[+|-]*ifix1,ifix2...*]}

psconf add -P <*policyname*> { **fspolicy=[±]**<*f1,f2...*> | **ipgroup=[±]**<*g1,g2...*> }

| **psconf add -e** *emailid* [-E FAIL | COMPLIANT | ALL] **[ipgroup=** [**±**]<*g1,g2...*>]

| **psconf add -I ip=** [**±**]<*host1, host2...*>

| **psconf delete** { **-F** <*FSPolicyname*> | **-G** <*ipgroupname*> | **-P** <*policyname*> | **-A** <*apargrp*> | **-V** <*ifixgrp*>}

| **psconf delete -H -i** <*host* | **ALL**> **-D** <*yyyy-mm-dd*>

| **psconf certadd -i** <*host*> **-t** <**TRUSTED** | **UNTRUSTED**>

| **psconf certdel -i** <*host*>

| **psconf verify -i** <*host*> | **-G** <*ipgroup*>

| **psconf update [-p] {-i**< *host* >| **-G** <*ipgroup*> **[-r** <*buildinfo*> | **-a** <*apar1, apar2...*> | **[-u] -v** <*ifix1, ifix2,...*>}

| **psconf log loglevel=<info** | **error** | **none**>

| **psconf import -C -i** <*host*> **-f** <*filename*> | **–d** <*import database filename*>

| **psconf** { **import -k** <*key_filename*> | **export**} **-S -f** <*filename*>

| **psconf list** { **-S** | **-G** < *ipgroupname* | **ALL** > | **-F** < *FSPolicyname* | **ALL** > | **-P** < *policyname* | **ALL** > | **-r**
| < *buildinfo* | **ALL** > | **-I -i** < *ip* | **ALL** > | **-A** < *apargrp* | **ALL** > | **-V** <*ifixgrp*>} **[-c] [-q]**

| **psconf list** { **-H** | **-s** <**COMPLIANT** | **IGNORE** | **FAILED** | **ALL**> } **-i** <*host* | **ALL**> **[-c] [-q]**

| **psconf export -d** <*path to export directory*>

| **psconf report -v <CVEid|ALL> -o <TEXT|CSV>**

| **psconf report -A <advisoryname>**

| **psconf report -P <policyname|ALL> -o <TEXT|CSV>**

| **psconf report -i <ip|ALL> -o <TEXT|CSV>**

| **psconf report -B <buildinfo|ALL> -o <TEXT|CSV>**

| Opérations client TNC :

| **psconf mkclient** [**tncport=**<*port*>] **tncserver=**<*host:port*>

| **psconf mkclient tncport=**<*port*> -T

| **psconf** { **rmclient** | **status** }

| **psconf** {**start** | **stop** | **restart** } **client**

| **psconf chclient** attribute = *value*

| **psconf list** { **-C** | **-S** }

| **psconf export** { **-C** | **-S** } **-f** <*filename*>

| **psconf import** { **-S** | **-C -k** <*key_filename*> } **-f** <*filename*>

| Opérations IPRef TNC :

| **psconf mkipref [tncport=**<*port*> **] tncserver=**<host:port>

| **psconf** { **rmipref** | **status**}

| **psconf** { **start** | **stop** | **restart**} ipref

| **psconf chipref** attribute = *value*

| **psconf** { **import -k** <*key_filename*> | **export** } **-R -f** <*filename*>

| **psconf list -R**

Description

La technologie TNC est une architecture basée sur des normes ouvertes utilisée pour l'authentification des points d'extrémité, la mesure d'intégrité des plateformes et l'intégration des systèmes de sécurité. L'architecture TNC vérifie que les points d'extrémité (clients et serveurs du réseau) sont conformes à des règles de sécurité avant de les autoriser à pénétrer sur le réseau protégé. Le référenceur IPRef TNC informe le serveur TNC lorsque de nouvelles adresses IP sont détectées sur le serveur virtuel d'E-S.

Le module SUMA permet aux administrateurs système de ne plus avoir à extraire extraire manuellement les mises à jour de maintenance à partir du Web. Grâce aux options extrêmement souples de ce module, les administrateurs système peuvent configurer une interface automatisée pour télécharger les correctifs d'un site Web de distribution de correctifs sur leurs systèmes.

La commande **psconf** permet de gérer le serveur et les clients du réseau en ajoutant ou en supprimant des règles de sécurité, en validant des clients comme sécurisés ou non sécurisés, en générant des rapports et en mettant à jour le serveur et le client.

La commande **psconf** permet d'exécuter les opérations suivantes :

Elément	Description
add	Permet d'ajouter une règle, un client ou les informations de courrier électronique sur le serveur TNC.
apargrp	Permet de spécifier les noms de groupe d'APAR inclus dans la règle d'ensemble de fichiers qui sont utilisés pour la vérification des clients TNC.
aparlist	Permet de spécifier la liste des APAR qui font partie du groupe d'APAR.
certadd	Permet de marquer le certificat comme sécurisé ou non sécurisé.
certdel	Permet de supprimer les informations client.
chclient	Permet de modifier les attributs contenus dans le fichier `tnccs.conf`. Une commande **start** explicite est nécessaire pour que les modifications soient effectives dans le client TNC. La syntaxe de attribute=value est la même que pour **mkclient**.
chipref	Permet de modifier les attributs contenus dans le fichier `tnccs.conf`. Une commande **start** explicite est nécessaire pour que les modifications soient effectives dans le référenceur IPRef. La syntaxe de attribute=value est la même que pour **mkipref**.
chserver	Permet de modifier les attributs contenus dans le fichier `tnccs.conf`. Une commande **start** explicite est nécessaire pour que les modifications soient effectives dans le serveur TNC. La syntaxe de attribute=value est la même que pour **mkserver**. **Remarque :** L'attribut **dbpath** ne peut pas être modifié à l'aide de la commande **chserver**. Il ne peut être défini que lors de l'exécution de **mkserver**.
dbpath	Permet de spécifier l'emplacement de la base de données TNC. La valeur par défaut est `/var/tnc`.
delete	Permet de supprimer une règle ou les informations client.
export	Permet d'exporter le certificat serveur ou client ou la base de données sur le serveur TNC.
fspolicy	Permet de spécifier les règles d'ensemble de fichiers d'édition, de niveau technologique et de Service Pack utilisées pour la vérification des clients TNC.
import	Permet d'importer le certificat serveur ou client ou la base de données sur le serveur TNC.
ipgroup	Permet de spécifier un groupe IP (Internet Protocol) contenant plusieurs adresses IP client ou noms d'hôte.

Elément	Description
list	Permet d'afficher des informations sur le serveur TNC, le client TNC ou le module SUMA.
log	Permet de définir le niveau de journalisation pour les composants TNC.
mkclient	Permet de configurer le client TNC.
mkipref	Permet de configurer le référenceur IPRef TNC.
mkserver	Permet de configurer le serveur TNC.
pmport	Permet de spécifier le numéro de port sur lequel **pmserver** est en mode écoute. La valeur par défaut est 38240.
pmserver	Permet de spécifier le nom d'hôte ou l'adresse IP de la commande **suma** qui télécharge les derniers Service Packs et les derniers correctifs de sécurité disponibles sur le site Web IBM ECC et le site Web IBM Fix Central.
recheck_interval	Permet de spécifier la fréquence en nombre de minutes ou au format d (jours) : h (heures) : m (minutes) à laquelle le serveur TNC vérifie les clients TNC. **Important :** La valeur **recheck_interval=0** signifie que le planificateur ne lance pas d'opération de vérification des clients à intervalles réguliers et que les clients enregistrés sont automatiquement vérifiés au démarrage. Dans ce cas, le client peut être vérifié manuellement.
report	Permet de générer un rapport ayant .txt ou .csv pour extension de fichier.
restart	Permet de redémarrer le client TNC, le serveur TNC ou le référenceur IPRef TNC.
rmclient	Permet de déconfigurer le client TNC.
rmipref	Permet de déconfigurer le référenceur IPRef TNC.
rmserver	Permet de déconfigurer le serveur TNC.
start	Permet de démarrer le client TNC, le serveur TNC ou le référenceur IPRef TNC.
status	Permet d'afficher l'état de la configuration TNC.
stop	Permet d'arrêter le client TNC, le serveur TNC ou le référenceur IPRef TNC.
tncport	Permet de spécifier le numéro de port sur lequel le serveur TNC est en mode écoute. La valeur par défaut est 42830.
tncserver	Permet de spécifier le serveur TNC qui vérifie ou met à jour les clients TNC.
tssserver	Permet de spécifier l'adresse IP ou le nom d'hôte du serveur Trusted Surveyor.
update	Permet d'installer les correctifs sur le client.
verify	Permet de lancer une opération de vérification manuelle des clients.

Options

Elément	Description
-A <advisoryName>	Permet de spécifier le nom de recommandation pour le rapport.
-B <buildinfo>	Permet de spécifier les informations de version pour préparer un rapport de correctifs.

-c	Permet d'afficher les attributs utilisateur dans des enregistrements séparés par un deux-points, comme suit :
	`# name: attribute1 : attribute2 : ...`
	`policy: value1 : value2 : ...`

-C	Permet de spécifier que l'opération concerne un composant client.
-d *database file location/dir path of database*	Permet de spécifier l'emplacement du chemin d'accès au fichier pour l'importation de la base de données/de spécifier l'emplacement du chemin de répertoire pour l'exportation de la base de données.
-D *yyyy-mm-dd*	Permet de spécifier la date d'une entrée client donnée dans l'historique de journalisation, où *yyyy* indique l'année, *mm* le mois et *dd* le jour.
-e *emailid* **ipgroup=[±]***g1, g2...*	Permet de spécifier l'ID de messagerie électronique suivi d'une liste de noms de groupe IP séparés par des virgules.
-E | **FAIL** | **COMPLIANT** | **ALL** |	Permet de spécifier l'événement pour lequel les courriers électroniques doivent être envoyés à l'ID de messagerie électronique configuré. FAIL - Des courriers électroniques sont envoyés lorsque l'état de la vérification du client est à l'état FAILED. COMPLIANT - Des courriers électroniques sont envoyés lorsque l'état de la vérification du client est à l'état COMPLIANT. ALL - Des courriers électroniques sont envoyés dans tous les cas, quel que soit l'état de la vérification du client.
-f *filename*	Permet de spécifier le fichier à partir duquel le certificat doit être lu dans le cadre d'une opération d'importation ou d'indiquer l'emplacement où le certificat doit être écrit dans le cadre d'une opération d'exportation.

Elément	Description
-F *fspolicy buildinfo*	Permet de spécifier le nom des règles du système de fichiers, suivi des informations de version. Les informations de version peuvent être indiquées au format suivant : `6100-04-01`, où `6100` représente la version 6.1, `04` le niveau de maintenance et `01` le Service Pack.
-G *ipgroupname* **ip=[±]***ip1, ip2...*	Permet de spécifier le nom de groupe IP suivi d'une liste d'adresses IP séparées par des virgules.
-H	Permet d'afficher le journal historique.
-i *host*	Permet de spécifier l'adresse IP ou le nom d'hôte.
-I ip=[±]*ip1, ip2...* | [±] host1,host2...	Permet de spécifier l'adresse IP/le nom d'hôte qui doit être ignoré lors d'une opération de vérification.
-k *filename*	Permet de spécifier le fichier à partir duquel la clé de certificat doit être lue dans le cas d'une importation.
-p	Permet de prévisualiser la mise à jour client TNC.
-P <policyName>	Permet de spécifier le nom de règle pour préparer un rapport sur la règle de client.
-q	Permet de supprimer les informations d'en-tête.
-r *buildinfo*	Permet de générer le rapport basé sur les informations de version. Les informations de version peuvent être indiquées au format suivant : `6100-04-01`, où `6100` représente la version 6.1, `04` le niveau de maintenance et `01` le Service Pack.
-R	Permet de spécifier que l'opération concerne un composant référenceur IPRef.
-s COMPLIANT | IGNORE | FAILED | ALL	Permet d'afficher les clients en fonction de leur état, comme suit : **COMPLIANT** Affiche les clients actifs. **IGNORE** Affiche les clients qui sont exclus d'une opération de vérification. **FAILED** Affiche les clients dont la vérification a échoué par rapport à la règle configurée. **ALL** Affiche tous les clients, quel que soit leur état.
-S <host>	Permet de spécifier le nom d'hôte pour préparer un rapport sur les correctifs de sécurité d'un client.
-t TRUSTED | UNTRUSTED	Permet de marquer le client spécifié comme sécurisé ou non sécurisé. **Remarque :** Seuls les administrateurs système peuvent vérifier que le serveur ou le client est sécurisé ou non.
-T	Permet de spécifier que le client peut accepter une demande d'un serveur TS doté d'un certificat valide.
-u	Permet de désinstaller un correctif temporaire qui est installé sur un client TNC.
-v	Permet de spécifier une liste de correctifs temporaires séparés par des virgules.
-V	Permet de spécifier le nom du groupe de correctifs temporaires.

Etat de sortie

Cette commande renvoie les valeurs de sortie suivantes :

Elément	Description
0	L'exécution de la commande a abouti, et toutes les modifications demandées ont été effectuées.
>0	Une erreur s'est produite Le message d'erreur imprimé contient des informations détaillées sur le type de la défaillance.

Exemples

1. Pour démarrer le serveur TNC, entrez la commande suivante :
   ```
   psconf start server
   ```
2. Pour ajouter une règle de système de fichiers nommée `71D_latest` pour la version `7100-04-02`, entrez la commande suivante :
   ```
   psconf add -F 71D_latest 7100-04-02
   ```
3. Pour supprimer une règle de système de fichiers nommée `71D_old`, entrez la commande suivante :
   ```
   psconf delete -F 71D_old
   ```
4. Pour indiquer que le client doté de l'adresse IP `11.11.11.11` est **sécurisé**, entrez la commande suivante :

```
psconf certadd -i 11.11.11.11 -t TRUSTED
```

5. Pour supprimer le client doté de l'adresse IP 11.11.11.11 sur le serveur, entrez la commande suivante :
   ```
   psconf certdel -i 11.11.11.11
   ```
6. Pour vérifier les informations sur le client doté de l'adresse IP 11.11.11.11, entrez la commande suivante :
   ```
   psconf verify -i 11.11.11.11
   ```
7. Pour afficher les informations sur le client doté de l'adresse IP 11.11.11.11, entrez la commande suivante :
   ```
   psconf list -i 11.11.11.11
   ```
8. Pour générer le rapport sur les clients à l'état **COMPLIANT**, entrez la commande suivante :
   ```
   psconf list -s CPMPLIANT -i ALL
   ```
9. Pour générer le rapport sur la version 7100-04-02, entrez la commande suivante :
   ```
   psconf list -r 7100-04-02
   ```
10. Pour afficher l'historique de connexion d'un client doté de l'adresse IP 11.11.11.11, entrez la commande suivante :
    ```
    psconf list -H -i 11.11.11.11
    ```
11. Pour supprimer l'entrée d'un client doté de l'adresse IP 11.11.11.11 qui est datée du 1er février ou qui est antérieure à cette date dans l'historique système, entrez la commande suivante :
    ```
    psconf delete -H -i 11.11.11.11 -D 2009-02-01
    ```
12. Pour importer le certificat client d'un client doté de l'adresse IP 11.11.11.11 à partir du serveur, entrez la commande suivante :
    ```
    psconf import -C -i 11.11.11.11 -f /tmp/client.txt
    ```
13. Pour exporter le certificat serveur à partir d'un client, entrez la commande suivante :
    ```
    psconf export -S -f /tmp/server.txt
    ```
14. Pour mettre à jour le client doté de l'adresse IP 11.11.11.11 vers un niveau approprié à partir du serveur, entrez la commande suivante :
    ```
    psconf update -i 11.11.11.11
    ```
15. Pour afficher l'état des clients, entrez la commande suivantes :
    ```
    psconf status
    ```
16. Pour afficher le certificat client, entrez la commande suivante :
    ```
    psconf list -C
    ```
17. Pour démarrer le client, entrez la commande suivante :
    ```
    psconf start client
    ```

Sécurité

Avertissement destiné aux utilisateurs de RBAC et de Trusted AIX :

Cette commande peut effectuer des opérations privilégiées. Seuls les utilisateurs privilégiés peuvent exécuter des opérations privilégiées. Pour plus d'informations sur les autorisations et les privilèges, voir la base de données des commandes privilégiées disponible dans Sécurité. Pour obtenir la liste des privilèges et autorisations associés à cette commande, voir la commande **lssecattr** ou la sous-commande **getcmdattr**.

Commande rmvfilt

Objectif

Permet de supprimer des règles de filtrage inter-réseaux locaux virtuels à partir de la table de filtres.

Syntaxe

rmvfilt -n [fid | all>]

Description

La commande **rmvfilt** permet de supprimer des règles de filtrage inter-réseaux locaux virtuels de la table de filtres.

Indicateurs

-n Indique l'ID de filtre de la règle de filtrage qui doit être supprimée. L'option **all** permet de supprimer toutes les règles de filtrage.

Etat de sortie

Cette commande renvoie les valeurs de sortie suivantes :

0 L'opération a abouti.

>0 Une erreur s'est produite.

Exemples

1. Pour supprimer toutes les règles de filtrage ou pour désactiver toutes les règles de filtrage du noyau; entre la commande comme suit :

```
rmvfilt -n all
```

Concepts associés :

«Désactivation de règles», à la page 17
Vous pouvez désactiver les règles qui autorisent le routage entre réseaux locaux virtuels dans la fonction Trusted Firewall.

Commande vlantfw

Objectif

Permet d'afficher ou d'effacer les informations de mappage MAC (Media Access Control) et IP et de contrôler la fonction de journalisation.

Syntaxe

vlantfw -h | -s | -t | -d | -f | -G | -q | -D | -E | -F | -i | -l | -L | -m | -M | -N *integer*

Description

La commande **vlantfw** permet d'afficher ou d'effacer les entrées de mappage MAC et IP. Elle permet également de démarrer ou d'arrêter la fonction de journalisation de Trusted Firewall.

Indicateurs

-d Affiche toutes les informations de mappage IP.

-D Affiche les données de connexion collectées.

-E Affiche les données de connexion entre des partitions logiques situées sur des processeurs CPC différents.

-f Supprime toutes les informations de mappage IP.

-F Efface le cache de données de connexion.

-G Affiche les règles de filtrage qui peuvent être configurées pour router le trafic en interne à l'aide de Trusted Firewall.

-I Affiche les données de connexion entre des partitions logiques qui sont associées à des ID de réseau local virtuel différents mais qui partagent le même processeur CPC.

-l Démarre la fonction de journalisation de Trusted Firewall.

-L Arrête la fonction de journalisation de Trusted Firewall et redirige le contenu du fichier de trace vers le fichier `/home/padmin/svm/svm.log`.

-m Active le la fonction de contrôle de Trusted Firewall.

-M Désactive la fonction de contrôle de Trusted Firewall.

-q Interroge l'état de la machine virtuelle sécurisée.

-s Démarre Trusted Firewall.

-t Arrête Trusted Firewall.

Paramètres

-N *integer*
Affiche la règle de filtrage qui correspond au nombre entier spécifié.

Etat de sortie

Cette commande renvoie les valeurs de sortie suivantes :

0 L'opération a abouti.

>0 Une erreur s'est produite.

Exemples

1. Pour afficher tous les mappages IP, entrez la commande comme suit :
   ```
   vlantfw -d
   ```
2. Pour supprimer tous les mappages IP, entrez la commande comme suit :
   ```
   vlantfw -f
   ```
3. Pour démarrer la fonction de journalisation de Trusted Firewall, entrez la commande comme suit :
   ```
   vlantfw -l
   ```
4. Pour vérifier l'état d'une machine virtuelle sécurisée, entrez la commande comme suit :
   ```
   vlantfw -q
   ```
5. Pour démarrer le pare-feu sécurisé, tapez la commande comme suit :
   ```
   vlantfw -s
   ```
6. Pour arrêter le pare-feu sécurisé, tapez la commande comme suit :
   ```
   vlantfw -t
   ```
7. Pour afficher les règles correspondantes permettant de générer des filtres pour le routage du trafic au sein du processeur CPC, entrez la commande comme suit :
   ```
   vlantfw -G
   ```

Référence associée :

«Commande genvfilt», à la page 34

Remarques

Ces informations ont été développées pour les produits et services proposés aux Etats-Unis.

IBM ne peuvent pas proposer les produits, services ou fonctions présentés dans ce document dans d'autres pays. Consultez votre interlocuteur commercial IBM local pour plus d'informations sur les produits et services disponibles dans votre pays. Toute référence à un produit, logiciel ou service IBM n'implique pas que seul ce produit, logiciel ou service puisse être utilisé. Tout autre élément fonctionnellement équivalent peut être utilisé, s'il n'enfreint aucun droit d'IBM. Il est de la responsabilité de l'utilisateur d'évaluer et de vérifier lui-même les installations et applications réalisées avec des produits, logiciels ou services non expressément référencés par IBM.

IBM peut posséder des brevets ou des applications de brevet en attente traitant du sujet décrit dans ce document. La remise de ce document ne vous donne aucun droit de licence sur ces brevets ou demandes de brevet. Si vous désirez recevoir des informations concernant l'acquisition de licences, veuillez en faire la demande par écrit à l'adresse suivante :

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
U.S.A.

Pour le Canada, veuillez adresser votre courrier à :

IBM Director of Commercial Relations
IBM Canada Ltd.
3600 Steeles Avenue East
Markham, Ontario
L3R 9Z7
Canada

Les informations sur les licences concernant les produits utilisant un jeu de caractères double octet (DBCS) peuvent être obtenues auprès du Département de la propriété intellectuelle IBM de votre pays ou par demande écrite envoyée à l'adresse suivante :

Intellectual Property Licensing
Legal and Intellectual Property Law
IBM Japan, Ltd.
19-21, Nihonbashi-Hakozakicho, Chuo-ku
Tokyo 103-8510, Japon

Le paragraphe suivant ne s'applique ni au Royaume-Uni, ni dans aucun pays dans lequel il serait contraire aux lois locales : LE PRESENT DOCUMENT EST LIVRE EN L'ETAT. IBM DECLINE TOUTE RESPONSABILITE, EXPLICITE OU IMPLICITE, RELATIVE AUX INFORMATIONS QUI Y SONT CONTENUES, Y COMPRIS EN CE QUI CONCERNE LES GARANTIES DE VALEUR MARCHANDE OU D'ADAPTATION A VOS BESOINS. Certaines juridictions n'autorisent pas l'exclusion des garanties implicites, auquel cas l'exclusion ci-dessus ne vous sera pas applicable.

Le présent document peut contenir des inexactitudes ou des coquilles. Ce document est mis à jour périodiquement. Chaque nouvelle édition inclut les mises à jour. IBM peut, à tout moment et sans préavis, apporter des améliorations et/ou des modifications aux produits et/ou programmes décrits dans ce document.

© Copyright IBM Corp. 2012, 2013

Les références à des sites Web non IBM sont fournies à titre d'information uniquement et n'impliquent en aucun cas une adhésion aux données qu'ils contiennent. Les éléments figurant sur ces sites Web ne font pas partie des éléments du présent produit IBM et l'utilisation de ces sites relève de votre seule responsabilité.

IBM peut utiliser ou publier les informations que vous fournissez si elle le juge approprié sans aucune obligation pour vous.

Les licenciés souhaitant obtenir des informations permettant : (i) l'échange des données entre des logiciels créés de façon indépendante et d'autres logiciels (dont celui-ci), et (ii) l'utilisation mutuelle des données ainsi échangées, doivent adresser leur demande à :

IBM Corporation
Dept. LRAS/Bldg. 903
11501 Burnet Road
Austin, TX 78758-3400
U.S.A.

Ces informations peuvent être soumises à des conditions particulières, prévoyant notamment le paiement d'une redevance.

Le logiciel sous licence décrit dans ce document et tous les éléments sous licence disponibles s'y rapportant sont fournis par IBM conformément aux dispositions du Livret contractuel IBM, des Conditions Internationales d'Utilisation de Logiciels IBM ou de tout autre accord équivalent.

Les données de performance indiquées dans ce document ont été déterminées dans un environnement contrôlé. Par conséquent, les résultats peuvent varier de manière significative selon l'environnement d'exploitation utilisé. Certaines mesures évaluées sur des systèmes en cours de développement ne sont pas garanties sur tous les systèmes disponibles. En outre, elles peuvent résulter d'extrapolations. Les résultats peuvent donc varier. Il incombe aux utilisateurs de ce document de vérifier si ces données sont applicables à leur environnement d'exploitation.

Les informations concernant des produits non IBM ont été obtenues auprès des fournisseurs de ces produits, par l'intermédiaire d'annonces publiques ou via d'autres sources disponibles. IBM n'a pas testé ces produits et ne peut confirmer l'exactitude de leurs performances ni leur compatibilité. Elle ne peut recevoir aucune réclamation concernant des produits non IBM. Toute question concernant les performances de produits non IBM doit être adressée aux fournisseurs de ces produits.

Toute instruction relative aux intentions d'IBM pour ses opérations à venir est susceptible d'être modifiée ou annulée sans préavis, et doit être considérée uniquement comme un objectif.

Tous les prix IBM affichés sont les prix de vente suggérés d'IBM et sont des prix actuels pouvant être changés sans avis. Les tarifs appliqués peuvent varier selon les revendeurs.

Ces informations sont fournies uniquement à titre de planification. Elles sont susceptibles d'être modifiées avant la mise à disposition des produits décrits.

Le présent document peut contenir des exemples de données et de rapports utilisés couramment dans l'environnement professionnel. Ces exemples mentionnent des noms fictifs de personnes, de sociétés, de marques ou de produits à des fins illustratives ou explicatives uniquement. Toute ressemblance avec des noms de personnes, de sociétés ou des données réelles serait purement fortuite.

LICENCE DE COPYRIGHT :

Le présent logiciel contient des programmes exemples d'application en langage source destinés à illustrer les techniques de programmation sur différentes plates-formes d'exploitation. Vous avez le droit de copier, de modifier et de distribuer ces programmes exemples sous quelque forme que ce soit et sans paiement d'aucune redevance à IBM à des fins de développement, d'utilisation, de vente ou de distribution de programmes d'application conformes à l'interface de programme d'application de la plateforme pour lesquels ils ont été écrits. Ces programmes exemples n'ont pas été rigoureusement testés dans toutes les conditions. Par conséquent, IBM ne peut garantir expressément ou implicitement la fiabilité, la maintenabilité ou le fonctionnement de ces programmes. Les programmes exemples sont livrés "EN L'ETAT", sans garantie d'aucune sorte. IBM ne sera en aucun cas responsable des dommages liés à l'utilisation des programmes exemples.

Toute copie totale ou partielle de ces programmes exemples et des oeuvres qui en sont dérivées doit comprendre une notice de copyright, libellée comme suit :

© (le nom de votre société) (année). Des segments de code sont dérivés des Programmes exemples d'IBM Corp. © Copyright IBM Corp. _entrez l'année ou les années_.

Si vous visualisez ces informations en ligne, il se peut que les photographies et illustrations en couleur n'apparaissent pas à l'écran.

Politique de protection des renseignements personnels

Les logiciels IBM, y compris les Logiciels sous forme de services (("Offres Logiciels"), peuvent utiliser des cookies ou d'autres technologies pour collecter des informations sur l'utilisation des produits, améliorer l'acquis utilisateur, personnaliser les interactions avec celui-ci, ou dans d'autres buts. Bien souvent, aucune information personnelle identifiable n'est collectée par les Offres Logiciels. Certaines Offres Logiciels vous permettent cependant de le faire. Si la présente Offre Logiciels utilise des cookies pour collecter des informations personnelles identifiables, des informations spécifiques sur cette utilisation sont fournies ci-dessous.

La présente Offre Logiciels n'utilise pas de cookies, ni d'autres technologies, pour collecter des informations personnelles identifiables.

Si les configurations déployées de cette Offre Logiciels vous permettent, en tant que client, de collecter des informations permettant d'identifier les utilisateurs par l'intermédiaire de cookies ou par d'autres techniques, vous devez solliciter un avis juridique sur la réglementation applicable à ce type de collecte, notamment en termes d'information et de consentement.

Pour plus d'informations sur l'utilisation à ces fins des différentes technologies, y compris celle des cookies, consultez les Points principaux de la Déclaration IBM de confidentialité sur Internet à l'adresse http://www.ibm.com/privacy, la section "Cookies, pixels espions et autres technologies" de la Déclaration IBM de confidentialité sur Internet à l'adresse http://www.ibm.com/privacy/details, ainsi que la page "IBM Software Products and Software-as-a-Service Privacy Statement" à l'adresse http://www.ibm.com/software/info/product-privacy.

Marques

IBM, le logo IBM et ibm.com sont des marques d'International Business Machines Corp. dans de nombreux pays. Les autres noms de produits ou de services peuvent être des marques d'IBM ou d'autres sociétés. La liste actualisée de toutes les marques d'IBM est disponible sur la page Web Copyright and trademark information à www.ibm.com/legal/copytrade.shtml.

Linux est une marque de Linus Torvalds aux Etats-Unis et/ou dans certains autres pays.

Java ainsi que tous les logos et toutes les marques incluant Java sont des marques d'Oracle et/ou de ses sociétés affiliées.

Index

A

affichage des journaux 28
affichage des résultats de la vérification 29
affichage des unités de journal virtuel 18
attestation d'un système 8

C

client TNC 22
commande chvfilt 32
commande genvfilt 34
commande lsvfilt 35
commande mkvfilt 36
commande pmconf 36
commande psconf 40
commande rmvfilt 45
commande vlantfw 46
commandes
  chvfilt 32
  genvfilt 34
  lsvfilt 35
  mkvfilt 36
  rmvfilt 45
  vlantfw 46
communication sécurisée 22
composants 21
concepts 21
concepts Trusted Boot 4
concepts Trusted Firewall 10
configuration 24
configuration d'un serveur de gestion de correctifs 25
configuration de la journalisation sécurisée 20
configuration de serveur 24
configuration de Trusted Boot 7
configuration du client 25
configuration matérielle et logicielle 2
configuration prérequise 5
considérations relatives à la migration 6

E

écriture de données sur des unités de journal virtuel 21

F

fichier syslog AIX 20

G

gestion de correctifs 22
gestion de TNC and Patch management 28
gestion de Trusted Boot 8
gestion des règles 30

I

importation de certificats 22, 30
inscription d'un système 7
installation 3, 23
installation de PowerSC Standard Edition 3
installation de Trusted Boot 7
installation du collecteur 7
installation du vérificateur 7
interprétation des résultats d'attestation 8

J

journaux virtuels 18

M

mise à jour du client TNC 30
modules IMC et IMV 23

N

notification par courrier électronique 27

O

outil de génération de rapports et de gestion pour TNC, SUMA
  utilisation de la commande psconf 40
outil de génération de rapports et de gestion pour TNCPM
  utilisation de la commande pmconf 36

P

planification 5
PowerSC
  Trusted Firewall
    configuration 13
    configuration avec plusieurs cartes Ethernet partagées 14
    création de règles 15
    désactivation de règles 17
    installation 13
    retrait de cartes Ethernet partagées 15
  Trusted Logging
    installation 19
PowerSC Standard Edition 1, 2, 3
préparation aux actions de résolution 6
présentation 2, 21
protocole 23

R

référenceur IP 22
référenceur IP sur VIOS 27
règles client 28

S

serveur 21
serveur Trusted Network Connect 27, 28
sous-système de contrôle AIX 20

© Copyright IBM Corp. 2012, 2013

SUMA 22
suppression de systèmes 9

T

TNC 31
traitement des incidents 9
traitement des incidents liés à TNC and Patch management 31
Trusted Boot 4, 5, 6, 7, 8, 9
Trusted Firewall 10
  configuration 13
    plusieurs cartes Ethernet partagées 14
  création de règles 15
  désactivation de règles 17
  installation 13
  retrait
    cartes Ethernet partagées 15
Trusted Logging 18, 21
  installation 19
Trusted Logging, présentation 18
Trusted Network Connect 21, 22, 23, 24, 25, 27, 28, 29, 30
Trusted Network Connect and Patch management 21

V

vérification du client 29