IBM PowerSC

Standard Edition

Version 1.1.4

PowerSC Standard Edition

IBM PowerSC

Standard Edition

Version 1.1.4

PowerSC Standard Edition

Important
Avant d'utiliser le présent document et le produit associé, prenez connaissance des informations générales figurant à la section «Remarques», à la page 175.

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.ibm.com/ca/fr (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 Standard Edition version 1.1.4 et à toutes les éditions et modifications ultérieures, sauf indication contraire dans les nouvelles éditions.

Table des matières

Avis aux lecteurs canadiens v

A propos de ce document vii

Nouveautés dans PowerSC Standard Edition 1.1.4 1

PowerSC Standard Edition - Notes sur l'édition de la version 1.1.4 3

Concepts de PowerSC Standard Edition 1.1.4 5

Installation de PowerSC Standard Edition 1.1.4 7

Automatisation de la sécurité et de la conformité 9

Concepts de l'automatisation de la sécurité et de la conformité 9
- Conformité au guide STIG du département de la défense des Etats-Unis (Department of Defense Security Technical Implementation Guide) . .. 10
- Conformité au standard PCI-DSS (Payment Card Industry Data Security Standard) 84
- Loi Sarbanes-Oxley et conformité COBIT . .. 100
- La loi Health Insurance Portability and Accountability Act (HIPAA) 101
- Conformité à la norme North American Electric Reliability Corporation (NERC) 106

Gestion de l'automatisation de la sécurité et de la conformité 111
- Examen d'une règle ayant échoué 112
- Mise à jour de la règle ayant échoué. 112
- Création d'un profil de configuration de sécurité personnalisé 112
- Test des applications avec AIX Profile Manager 113
- Surveillance des systèmes pour une conformité continue avec AIX Profile Manager 113

Configuration de l'automatisation de la sécurité et de la conformité de PowerSC 114
- Configuration des paramètres des options de conformité PowerSC 114
- Configuration de la conformité PowerSC depuis la ligne de commande 114
- Configuration de la conformité à PowerSC avec AIX Profile Manager 115

PowerSC Real Time Compliance . .. 117

installation de PowerSC Real Time Compliance .. 117

Configuration de PowerSC Real Time Compliance 117
- Identification des fichiers surveillés par la fonction PowerSC Real Time Compliance . .. 118
- Définition d'alertes pour PowerSC Real Time Compliance 118

Trusted Boot. 119

Concepts Trusted Boot 119

Planification de Trusted Boot 119
- Configuration prérequise pour Trusted Boot .. 120
- Préparation aux actions de résolution 120
- Considérations relatives à la migration 121

Installation de Trusted Boot 121
- Installation du collecteur 121
- Installation du vérificateur 121

Configuration de Trusted Boot. 121
- Inscription d'un système. 122
- Attestation d'un système 122

Gestion de Trusted Boot 122
- Interprétation des résultats d'attestation . .. 123
- Suppression de systèmes 123

Traitement des incidents liés à Trusted Boot . .. 123

Trusted Firewall 127

Concepts Trusted Firewall 127

Installation de Trusted Firewall 130

Configuration de Trusted Firewall 130
- Fonction de contrôle de Trusted Firewall . .. 130
- Fonction de journalisation de Trusted Firewall 131
- Plusieurs cartes Ethernet partagées 131
- Retrait de cartes Ethernet partagées 133
- Création de règles 133
- Désactivation de règles 134

Trusted Logging 137

Journaux virtuels 137

Détection des unités de journal virtuel 138

Installation de Trusted Logging 138

Configuration de la journalisation sécurisée . .. 139
- Configuration du sous-système de contrôle AIX 139
- Configuration de syslog 139
- Ecriture de données sur des unités de journal virtuel. 140

Trusted Network Connect and Patch management. 141

Concepts Trusted Network Connect 141
- Composants Trusted Network Connect 141
- Communication Trusted Network Connect sécurisée 142
- Protocole Trusted Network Connect 142
- Modules IMC et IMV. 143

Installation de Trusted Network Connect 143

Configuration de Trusted Network Connect and Patch management 144
- Configuration du serveur Trusted Network Connect 144

Configuration du client Trusted Network Connect 144
Configuration du serveur de gestion de correctifs 145
Configuration de la notification par courrier électronique pour le serveur Trusted Network Connect 146
Configuration du référenceur IP sur VIOS . . 147
Gestion de Trusted Network Connect and Patch management 147
Affichage des journaux du serveur Trusted Network Connect 147
Création de règles pour le client Trusted Network Connect 148
Démarrage de la vérification du client Trusted Network Connect 149
Affichage des résultats de la vérification du client Trusted Network Connect 149
Mise à jour du client Trusted Network Connect 149
Gestion des règles de gestion de correctifs. . 150
Importation de certificats Trusted Network Connect 150
Génération de rapports sur les serveurs TNC. . 151
Traitement des incidents liés à Trusted Network Connect and Patch management 151

Commandes de PowerSC Standard Edition 153
commande chvfilt 153
Commande genvfilt 154
Commande lsvfilt 156
Commande mkvfilt 156
Commande pmconf 157
Commande psconf 161
Commande pscxpert 167
Commande rmvfilt 171
Commande vlantfw 172

Remarques 175
Politique de protection des renseignements personnels 177
Marques 177

Index 179

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.

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.

Nouveautés dans PowerSC Standard Edition 1.1.4

Découvrez les nouveautés et les modifications significatives apportées à l'ensemble de rubriques relatives à PowerSC Standard Edition version 1.1.4.

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

Décembre 2015

- Ajout d'informations sur les profils de conformité dans les rubriques suivantes :
  - «Conformité à la norme North American Electric Reliability Corporation (NERC)», à la page 106
  - «Conformité au standard PCI-DSS (Payment Card Industry Data Security Standard)», à la page 84
  - «Conformité au guide STIG du département de la défense des Etats-Unis (Department of Defense Security Technical Implementation Guide)», à la page 10
  - «Loi Sarbanes-Oxley et conformité COBIT», à la page 100
  - «La loi Health Insurance Portability and Accountability Act (HIPAA)», à la page 101
- Ajout d'informations sur la fonction Real Time Compliance dans la rubrique «PowerSC Real Time Compliance», à la page 117.
- Ajout des opérations **clientData** et **default_policy** ainsi que des indicateurs **-l** et **-g** dans la commande **psconf**.
- Mise à jour des indicateurs **-a**, **-c**, **-l** et **-n** dans la commande **pscxpert**.
- Mise à jour des indicateurs **-i** et **-x** dans la commande **pmconf**.

PowerSC Standard Edition - Notes sur l'édition de la version 1.1.4

Les notes sur l'édition contiennent des informations sur les modifications apportées à PowerSC Standard Edition version 1.1.4 et qui ont été identifiées après la publication de la documentation.

Modifications apportées aux ensembles de fichiers PowerSC Standard Edition

PowerSC Express Edition n'est plus proposé à l'achat par IBM®. PowerSC Standard Edition 1.1.4 ou version ultérieure inclut la fonctionnalité et les fonctions suivantes, qui étaient auparavant disponibles dans PowerSC Express Edition :

- Conformité au guide STIG du département de la défense des Etats-Unis (Department of Defense Security Technical Implementation Guide)
- Conformité à la loi Sarbanes-Oxley et à COBIT
- Conformité à la loi Health Insurance Portability and Accountability Act (HIPAA)
- Real Time Compliance

Le tableau ci-dessous répertorie le nom des ensembles de fichiers PowerSC Express Edition qui ont été fusionnés dans les ensembles de fichiers PowerSC Standard Edition version 1.1.4 ou ultérieure.

Tableau 1. Ensembles de fichiers PowerSC Standard Edition 1.1.4 ou version ultérieure

Ensemble de fichiers PowerSC Express Edition	Ensemble de fichiers PowerSC Standard Edition
powerscExp.rtc	powerscStd.rtc
powerscExp.msg.<LANGUE>	powerscStd.msg.<LANGUE>
powerscExp.license	powerscStd.license
powerscExp.ice	powerscStd.ice

Lisez ces informations avant d'installer PowerSC Standard Edition

Pour afficher la version la plus récente des notes sur l'édition, voir les notes sur l'édition en ligne dans l'IBM Knowledge Center (http://www.ibm.com/support/knowledgecenter/SSTQK9_1.1.4/com.ibm.powersc114.se/powersc_se_rn.htm).

PowerSC Standard Edition est un programme sous licence qui n'est pas inclus avec le système d'exploitation AIX.

Remarque : Il se peut que le logiciel contienne des erreurs pouvant avoir un impact critique sur l'activité. Installez les derniers correctifs disponibles avant de l'utiliser.

Informations sur l'installation, la migration, la mise à niveau et la configuration

Pour des informations sur l'installation de PowerSC Standard Edition, voir Installation de PowerSC Standard Edition version 1.1.4.

Pour des informations sur le matériel et les versions du système d'exploitation AIX pris en charge pour PowerSC Standard Edition, voir Concepts PowerSC Standard Edition 1.1.4.

Ensemble de fichiers supplémentaire requis pour l'exécution de Trusted Network Connect

Pour exécuter Trusted Network Connect, vous devez installer l'ensemble de fichiers `powerscStd.tnc_commands` qui est disponible sur votre DVD IBM PowerSC Standard Edition. Installez l'ensemble de fichiers sur votre système AIX avec la commande **installp**. Cet ensemble de fichiers fournit la fonction des commandes **psconf** et **pmconf**.

Remarque : Si vous utilisez la fonction IP Referrer de Trusted Network Connect, vous devez aussi installer l'ensemble de fichiers `powerscStd.tnc_commands` sur votre système VIOS.

Modifications apportées aux commandes

Les commandes suivantes ont changé :

- Dans IBM AIX 6 avec niveau de technologie 8 ou version ultérieure, vous pouvez utiliser la commande **tncconsole** pour générer des rapports et gérer le serveur Trusted Network Connect (TNC), le client TNC, la fonction TNC IP Referrer (IPRef) et l'assistant Service Update Management Assistant (SUMA). Toutefois, la commande **tncconsole** présente des fonctions limitées. Pour utiliser la fonction complète de la commande **tncconsole**, vous devez installer PowerSC Standard Edition. Dans PowerSC Standard Edition, le nom de la commande **tncconsole** est désormais **psconf**.
- L'indicateur **-o** a été supprimé de la commande **pscxpert**.

Concepts de PowerSC Standard Edition 1.1.4

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 l'automatisation de la sécurité et de la conformité, 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 2. 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
Automatisation de la sécurité et de la conformité	Permet d'automatiser le paramétrage, la surveillance et l'audit de la configuration de la sécurité et de la conformité pour les normes suivantes : • Le standard PCI-DSS (Payment Card Industry Data Security Standard) • La loi Sarbanes-Oxley et la conformité COBIT (SOX/COBIT) • Le guide STIG du département de la défense des Etats-Unis (Department of Defense Security Technical Implementation Guide) • La loi Health Insurance Portability and Accountability Act (HIPAA)	• AIX 5.3 • AIX 6.1 • AIX 7.1	• POWER5 • POWER6 • POWER7 • POWER8
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 • POWER8 • serveur d'E-S virtuel version 6.1S ou suivante

Tableau 2. 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 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 • POWER8
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 • POWER8

Installation de PowerSC Standard Edition 1.1.4

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 :

- `powerscStd.ice` : installé sur les systèmes AIX qui nécessitent la fonction d'automatisation de la sécurité et de la conformité de PowerSC Standard Edition.
- `powerscStd.vtpm` : installé sur les systèmes AIX qui nécessitent la fonction Trusted Boot de PowerSC Standard Edition.
- `powerscStd.vlog` : installé sur les systèmes AIX qui nécessitent la fonction Trusted Logging de PowerSC Standard Edition.
- `powerscStd.tnc_pm` : installé sur le système de console SUMA (Service Update Management Assistant) AIX version 6.1 avec niveau de technologie 6100-06 ou ultérieure ou AIX version 7.1 ou ultérieure, dans l'environnement SUMA pour la gestion des correctifs.
- `powerscStd.svm` : installé sur les systèmes AIX qui peuvent bénéficier de la fonction de routage de PowerSC Standard Edition.
- `powerscStd.rtc` : installé sur les systèmes AIX qui nécessitent la fonction Real Time Compliance de PowerSC Standard Edition.

Vous pouvez installer PowerSC Standard Edition en utilisant 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 de PowerSC Standard Edition 1.1.4», à la page 5
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 121
Certaines configurations logicielles et matérielles sont requises pour installer Trusted Boot.

«Installation de Trusted Network Connect», à la page 143
Certaines étapes sont nécessaires pour l'installation des composants de Trusted Network Connect (TNC).

Tâches associées:

«Installation de Trusted Firewall», à la page 130
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 138
Vous pouvez installer la fonction PowerSC Trusted Logging à l'aide de l'interface de ligne de commande ou de l'outil SMIT.

Automatisation de la sécurité et de la conformité

AIX Profile Manager gère des profils prédéfinis pour la sécurité et la conformité. PowerSC Real Time Compliance surveille en permanence les systèmes AIX activés pour s'assurer qu'ils sont configurés de façon cohérente et sécurisée.

Les profils XML automatisent la configuration système AIX recommandée d'IBM pour qu'elle soit cohérente avec le standard PCI-DSS (Payment Card Industry Data Security Standard), la loi Sarbanes-Oxley ou le guide STIG du département de la défense des Etats-Unis (Department of Defense Security Technical Implementation Guide) pour UNIX et la loi Health Insurance Portability and Accountability Act (HIPAA). Les organisations qui respectent les normes de sécurité doivent utiliser les paramètres de sécurité du système prédéfinis.

AIX Profile Manager agit en tant que plug-in IBM Systems Director qui simplifie l'application des paramètres de sécurité, leur surveillance et leur audit pour le système d'exploitation AIX et les systèmes de serveur d'E-S virtuel (VIOS). Pour que vous puissiez utiliser la fonction de sécurité et de conformité, l'application PowerSC doit être installée sur les systèmes gérés AIX qui respectent les normes de conformité. La fonction d'automatisation de la sécurité et de la conformité est incluse dans PowerSC Standard Edition.

Le module d'installation de PowerSC Standard Edition, 5765-PSE, doit être installé sur les systèmes gérés AIX. Il installe l'ensemble de fichiers `powerscStd.ice` qui peut être implémenté sur le système avec AIX Profile Manager ou la commande **pscxpert**. PowerSC avec IBM Compliance Expert Express (ICEE) est activé pour gérer et améliorer les profils XML. Les profils XML sont gérés par AIX Profile Manager.

Remarque : Installez toutes les applications sur le système avant d'appliquer un profil de sécurité.

Concepts de l'automatisation de la sécurité et de la conformité

La fonction d'automatisation de la sécurité et de la conformité de PowerSC est une méthode automatisée permettant de configurer et d'effectuer un audit des systèmes AIX conformément au guide STIG du département de la défense des Etats-Unis (Department of Defense Security Technical Implementation Guide), au standard PCI-DSS (Payment Card Industry Data Security Standard), à la loi Sarbanes-Oxley et à la conformité COBIT (SOX/COBIT), ainsi qu'à la loi Health Insurance Portability and Accountability Act (HIPAA).

PowerSC permet d'automatiser la configuration et la surveillance des systèmes qui doivent être conformes au standard PCI-DSS (Payment Card Industry Data Security Standard) version 1.2, 2.0 ou 3.0. Par conséquent, la fonction d'automatisation de la sécurité et de la conformité de PowerSC est une méthode complète et précise d'automatisation de la configuration de la sécurité qui est utilisée pour satisfaire les exigences de conformité informatique du guide STIG du département de la défense des Etats-Unis (Department of Defense Security Technical Implementation Guide) pour UNIX, du standard PCI-DSS, de la loi Sarbanes-Oxley, de la conformité COBIT (SOX/COBIT) et de la loi Health Insurance Portability and Accountability Act (HIPAA).

Remarque : La fonction d'automatisation de la sécurité et de la conformité PowerSC met à jour les profils xml existants qui sont utilisés par l'édition IBM Compliance Expert Express (ICEE). Vous pouvez utiliser les profils XML PowerSC Standard Edition avec la commande **pscxpert**, comme pour ICEE.

Les profils de conformité préconfigurés qui sont distribués avec PowerSC Standard Edition réduisent la charge de travail administratif consistant à interpréter la documentation relative à la conformité et à implémenter les normes sous forme de paramètres de configuration du système spécifiques. Cette technologie réduit le coût de la configuration de la conformité et de l'audit en automatisant les processus.

IBMPowerSC Standard Edition a été conçu pour vous aider à gérer efficacement la configuration requise par le système associée à la conformité aux normes externes pouvant potentiellement réduire les coûts et améliorer la conformité.

Conformité au guide STIG du département de la défense des Etats-Unis (Department of Defense Security Technical Implementation Guide)

Le département de la défense des Etats-Unis exige des systèmes informatiques extrêmement sécurisés. Le niveau de sécurité et de qualité défini par le département de la défense des Etats-Unis est en corrélation avec la qualité et la base clients du serveur AIX on Power Systems.

Un système d'exploitation sécurisé tel qu'AIX doit être configuré précisément pour atteindre les buts de sécurité spécifiés. Le département de la défense des Etats-Unis reconnaît la nécessité de configurations de sécurité sur tous les systèmes d'exploitation dans la directive 8500.1. Cette directive établit la stratégie et attribue à l'agence américaine DISA (Defense Information Security Agency) la responsabilité de fournir des conseils pour la configuration de la sécurité.

L'agence DISA a développé les principes et les instructions dans le guide STIG du département de la défense des Etats-Unis (Department of Defense Security Technical Implementation Guide) pour UNIX, qui fournit un environnement répondant aux exigences de sécurité des systèmes du département de la défense des Etats-Unis qui fonctionnent au niveau MAC (Mission Assurance Category) de sensibilité II, qui contient des informations sensibles, ou dépassant ces exigences. Le département de la défense des Etats-Unis impose des exigences de sécurité informatique strictes et a énuméré les détails des paramètres de configuration requis permettant au système de fonctionner de façon sécurisée. Vous pouvez optimiser les conseils spécialisés requis. PowerSC Standard Edition permet d'automatiser le processus de configuration des paramètres, conformément à la définition du département de la défense des Etats-Unis.

Remarque : Tous les fichiers script personnalisés qui sont fournis pour gérer la conformité imposée par le département de la défense des Etats-Unis se trouvent dans le répertoire `/etc/security/pscexpert/dodv2`.

PowerSC Standard Edition prend en charge les exigences de la version 1, édition 2, du guide STIG du département de la défense des Etats-Unis (Department of Defense Security Technical Implementation Guide) pour AIX. Un récapitulatif des exigences relatives à la sécurité et des instructions permettant d'assurer la conformité est fourni dans les tableaux ci-après.

Tableau 3. Exigences générales du département de la défense des Etats-Unis

ID de point de contrôle du guide STIG (Department of Defense Security Technical Implemen- tation Guide)	Catégorie de la règle du guide STIG (Department of Defense Security Technical Implemen- tation Guide)	Description	Emplacement du script dans lequel l'action est définie et résultats de l'action assurant la conformité
AIX00020	2	Le logiciel AIX Trusted Computing Base doit être implémenté.	**Emplacement** `/etc/security/pscexpert/dodv2/trust` **Action de conformité** Garantit que le système satisfait les exigences spécifiées.
AIX00040	2	La commande **securetcpip** doit être utilisée.	**Emplacement** `/etc/security/pscexpert/dodv2/dodsecuretcpip` **Action de conformité** Garantit que le système satisfait les exigences spécifiées.

Tableau 3. Exigences générales du département de la défense des Etats-Unis (suite)

ID de point de contrôle du guide STIG (Department of Defense Security Technical Implemen- tation Guide)	Catégorie de la règle du guide STIG (Department of Defense Security Technical Implemen- tation Guide)	Description	Emplacement du script dans lequel l'action est définie et résultats de l'action assurant la conformité
AIX00060	2	Les fichiers `setuid` non autorisés doivent être identifiés toutes les semaines sur le système, de même que la modification non autorisée des fichiers `setuid` autorisés.	**Emplacement** `/etc/security/pscexpert/dodv2/trust` **Action de conformité** Identifie toutes les semaines les modifications apportées aux fichiers spécifiés.
AIX00080	1	L'attribut `SYSTEM` ne doit pas être associé à la valeur *none* pour un compte.	**Emplacement** `/etc/security/pscexpert/dodv2/SYSattr` **Action de conformité** Garantit que l'attribut spécifié a pour valeur une valeur autre que *none*. **Remarque :** Ce paramètre n'est pas modifié automatiquement lorsque la stratégie AIX par défaut est restaurée avec le fichier `DoDv2_to_AIXDefault.xml`. Vous devez le changer manuellement.
AIX00200	2	Le système ne doit pas autoriser de diffusion directe via la passerelle.	**Emplacement** `/etc/security/pscexpert/dodv2/ntwkoptsdod` **Action de conformité** Associe l'option de réseau `direct_broadcast` à la valeur *0*.
AIX00210	2	Le système doit fournir une protection contre les attaques ICMP (Internet Control Message Protocol) sur les connexions TCP.	**Emplacement** `/etc/security/pscexpert/dodv2/ntwkoptsdod` **Action de conformité** Associe l'option de réseau `tcp_icmpsecure` à la valeur *1*.
AIX00220	2	Le système doit fournir une protection pour la pile TCP contre les réinitialisations de connexion, les attaques par synchronisation (SYN) et les attaques par injection de données.	**Emplacement** `/etc/security/pscexpert/dodv2/ntwkoptsdod` **Action de conformité** Garantit que l'option de réseau `tcp_tcpsecure` est associée à la valeur *7*.
AIX00230	2	Le système doit fournir une protection contre les attaques par fragmentation d'IP.	**Emplacement** `/etc/security/pscexpert/dodv2/ntwkoptsdod` **Action de conformité** Associez l'option de réseau `ip_nfrag` à la valeur *200*.
AIX00300	1,2,3	Le service `bootp` ne doit pas être actif sur le système.	**Emplacement** `/etc/security/pscexpert/dodv2/inetdservices` **Action de conformité** Désactive le service spécifié.

Tableau 3. Exigences générales du département de la défense des Etats-Unis (suite)

ID de point de contrôle du guide STIG (Department of Defense Security Technical Implemen- tation Guide)	Catégorie de la règle du guide STIG (Department of Defense Security Technical Implemen- tation Guide)	Description	Emplacement du script dans lequel l'action est définie et résultats de l'action assurant la conformité
AIX00310	2	Les fichiers `/etc/ftpaccess.ctl` doivent exister.	**Emplacement** `/etc/security/pscexpert/dodv2/dodv2loginherald` **Action de conformité** Garantit que le fichier existe.
GEN000020	2	Le système doit demander l'authentification en cas de démarrage en mode utilisateur unique.	**Emplacement** `/etc/security/pscexpert/dodv2/rootpasswd_home` **Action de conformité** Garantit que le compte root pour les partitions amorçables possède un mot de passe dans le fichier `/etc/security/passwd`. **Remarque :** Ce paramètre n'est pas modifié automatiquement lorsque la stratégie AIX par défaut est restaurée avec le fichier `DoDv2_to_AIXDefault.xml`. Vous devez le changer manuellement.
GEN000100	1	L'édition du système d'exploitation doit être prise en charge.	**Emplacement** `/etc/security/pscexpert/dodv2/dodv2cat1` **Action de conformité** Affiche les résultats des tests de règle spécifiés.

GEN000120	2	Les mises à jour et les correctifs de sécurité du système les plus récents doivent être installés.	**Emplacement**
			`/usr/sbin/instfix -i`
			`/etc/security/pscexpert/dodv2/dodv2cat1`
			Action de conformité
			Configurez ce paramètre avec la fonction Trusted Network Connect.

GEN000140	2	Les fichiers `setuid` non autorisés doivent être identifiés toutes les semaines sur le système, de même que la modification non autorisée des fichiers `setuid` autorisés.	**Emplacement** `/etc/security/pscexpert/dodv2/trust` **Action de conformité** Identifie toutes les semaines les modifications apportées aux fichiers spécifiés.
GEN000220	2	Les fichiers `setuid` non autorisés doivent être identifiés toutes les semaines sur le système, de même que la modification non autorisée des fichiers `setuid` autorisés.	**Emplacement** `/etc/security/pscexpert/dodv2/trust` **Action de conformité** Identifie toutes les semaines les modifications apportées aux fichiers spécifiés.

Tableau 3. Exigences générales du département de la défense des Etats-Unis (suite)

ID de point de contrôle du guide STIG (Department of Defense Security Technical Implemen- tation Guide)	Catégorie de la règle du guide STIG (Department of Defense Security Technical Implemen- tation Guide)	Description	Emplacement du script dans lequel l'action est définie et résultats de l'action assurant la conformité
GEN000240	2	L'horloge système doit être synchronisée avec une source horaire du département de la défense des Etats-Unis faisant autorité.	**Emplacement** `/etc/security/pscexpert/dodv2/dodv2cmntrows` **Action de conformité** Garantit que l'horloge système est compatible.
GEN000241	2	L'horloge système doit être synchronisée en permanence, ou au moins quotidiennement.	**Emplacement** `/etc/security/pscexpert/dodv2/dodv2cmntrows` **Action de conformité** Garantit que l'horloge système est compatible.
GEN000242	2	Le système doit utiliser au moins deux sources horaires pour la synchronisation de l'horloge.	**Emplacement** `/etc/security/pscexpert/dodv2/dodv2netrules` **Action de conformité** Garantit que plusieurs sources horaires sont utilisées pour la synchronisation de l'horloge.
GEN000280	2	Les connexions directes aux types suivants de compte ne doivent pas être autorisées : • application • par défaut • partagé • utilitaire	**Emplacement** `/etc/security/pscexpert/dodv2/lockacc_rlogin` **Action de conformité** Empêche les connexions directes aux comptes spécifiés.
GEN000290	2	Le système ne doit pas comporter de comptes inutiles.	**Emplacement** `/etc/security/pscexpert/dodv2/lockacc_rlogin` **Action de conformité** Garantit qu'il n'existe pas de comptes non utilisés.
GEN000300 (lié à GEN000320, GEN000380, GEN000880)	2	Tous les comptes sur le système doivent être associés à des noms de compte ou d'utilisateur uniques et à des mots de passe de compte ou d'utilisateur uniques.	**Emplacement** `/etc/security/pscexpert/dodv2/grpusrpass_chk` **Action de conformité** Garantit que tous les comptes satisfont les exigences spécifiées. **Remarque :** Ce paramètre n'est pas modifié automatiquement lorsque la stratégie AIX par défaut est restaurée avec le fichier `DoDv2_to_AIXDefault.xml`. Vous devez le changer manuellement.

Tableau 3. Exigences générales du département de la défense des Etats-Unis (suite)

ID de point de contrôle du guide STIG (Department of Defense Security Technical Implemen- tation Guide)	Catégorie de la règle du guide STIG (Department of Defense Security Technical Implemen- tation Guide)	Description	Emplacement du script dans lequel l'action est définie et résultats de l'action assurant la conformité
GEN000320 (lié à GEN000300, GEN000380, GEN000880)	2	Tous les comptes sur le système doivent être associés à des noms de compte ou d'utilisateur uniques et à des mots de passe de compte ou d'utilisateur uniques.	**Emplacement** `/etc/security/pscexpert/dodv2/grpusrpass_chk` **Action de conformité** Garantit que tous les comptes satisfont les exigences spécifiées. **Remarque :** Ce paramètre n'est pas modifié automatiquement lorsque la stratégie AIX par défaut est restaurée avec le fichier `DoDv2_to_AIXDefault.xml`. Vous devez le changer manuellement.
GEN000340	2	Les ID utilisateur et les ID groupe qui sont réservés pour les comptes système ne doivent pas être affectés à des comptes autres que des comptes système ou à des groupes autres que des groupes système.	**Emplacement** `/etc/security/pscexpert/dodv2/account` **Action de conformité** Ce paramètre est activé automatiquement pour l'application de cette règle.
GEN000360	2	Les ID utilisateur et les ID groupe qui sont réservés pour les comptes système ne doivent pas être affectés à des comptes autres que des comptes système ou à des groupes autres que des groupes système.	**Emplacement** `/etc/security/pscexpert/dodv2/account` **Action de conformité** Ce paramètre est activé automatiquement pour l'application de cette règle.
GEN000380 (lié à GEN000300, GEN000320, GEN000880)	2	Tous les comptes sur le système doivent être associés à des noms de compte ou d'utilisateur uniques et à des mots de passe de compte ou d'utilisateur uniques.	**Emplacement** `/etc/security/pscexpert/dodv2/grpusrpass_chk` **Action de conformité** Garantit que tous les comptes satisfont les exigences spécifiées.
GEN000400	2	La bannière de connexion du département de la défense des Etats-Unis doit être affichée immédiatement avant ou dans les invites de connexion de la console.	**Emplacement** `/etc/security/pscexpert/dodv2/dodv2loginherald` **Action de conformité** Affiche la bannière requise.
GEN000402	2	La bannière de connexion du département de la défense des Etats-Unis doit être affichée immédiatement avant ou dans les invites de connexion de l'environnement de bureau graphique.	**Emplacement** `/etc/security/pscexpert/dodv2/dodv2loginherald` **Action de conformité** La bannière de connexion est la bannière du département de la défense des Etats-Unis.
GEN000410	2	Le service FTPS (File Transfer Protocol over SSL) ou FTP (File Transfer Protocol) sur le système doit être configuré avec la bannière de connexion du département de la défense des Etats-Unis.	**Emplacement** `/etc/security/pscexpert/dodv2/dodv2loginherald` **Action de conformité** Affiche la bannière lorsque vous utilisez FTP.

Tableau 3. Exigences générales du département de la défense des Etats-Unis (suite)

ID de point de contrôle du guide STIG (Department of Defense Security Technical Implemen- tation Guide)	Catégorie de la règle du guide STIG (Department of Defense Security Technical Implemen- tation Guide)	Description	Emplacement du script dans lequel l'action est définie et résultats de l'action assurant la conformité
GEN000440	2	Les tentatives de connexion et de déconnexion ayant réussi et ayant échoué doivent être enregistrées.	**Emplacement** `/etc/security/pscexpert/dodv2/loginout` **Action de conformité** Active la journalisation requise.
GEN000452	2	Le système doit afficher la date et l'heure de la dernière connexion au compte réussie à chaque connexion.	**Emplacement** `/etc/security/pscexpert/dodv2/sshDoDconfig` **Action de conformité** Affiche les informations requises.
GEN000460	2	Cette règle désactive un compte après trois échecs de connexion consécutifs.	**Emplacement** `/etc/security/pscexpert/dodv2/chusrattrdod` **Action de conformité** Définit la valeur spécifiée comme nombre maximal de tentatives de connexion.
GEN000480	2	Cette règle associe le délai de connexion à 4 secondes.	**Emplacement** `/etc/security/pscexpert/dodv2/chdefstanzadod` **Action de conformité** Définit la valeur requise pour le délai de connexion.
GEN000540	2	Cette règle garantit que les fichiers de configuration des mots de passe globaux du système sont configurés conformément aux exigences relatives aux mots de passe.	**Emplacement** `/etc/security/pscexpert/dodv2/chusrattrdod` **Action de conformité** Définit les paramètres de mot de passe requis.
GEN000560	1	Tous les comptes sur le système doivent être associés à des mots de passe valides.	**Emplacement** `/etc/security/pscexpert/dodv2/grpusrpass_chk` **Action de conformité** Garantit que les comptes sont associés à des mots de passe.
GEN000580	2	Cette règle garantit que tous les mots de passe contiennent au moins 14 caractères.	**Emplacement** `/etc/security/pscexpert/dodv2/chusrattrdod` **Action de conformité** Définit la longueur minimale des mots de passe à 14 caractères.
GEN000585	2	Le système doit utiliser un algorithme de hachage cryptographique approuvé par la norme FIPS 140-2 (Federal Information Processing Standards) pour la génération des hachages de mot de passe de compte.	**Emplacement** `/etc/security/pscexpert/dodv2/fipspasswd` **Action de conformité** Garantit que les hachages de mot de passe utilisent un algorithme de hachage approuvé.

Tableau 3. Exigences générales du département de la défense des Etats-Unis (suite)

ID de point de contrôle du guide STIG (Department of Defense Security Technical Implemen- tation Guide)	Catégorie de la règle du guide STIG (Department of Defense Security Technical Implemen- tation Guide)	Description	Emplacement du script dans lequel l'action est définie et résultats de l'action assurant la conformité
GEN000590	2	Le système doit utiliser un algorithme de hachage cryptographique approuvé par la norme FIPS 140-2 pour la génération des hachages de mot de passe de compte.	**Emplacement** `/etc/security/pscexpert/dodv2/fipspasswd` **Action de conformité** Garantit que les hachages de mot de passe utilisent un algorithme de hachage approuvé.
GEN000595	2	Utilisez un algorithme de hachage cryptographique approuvé par la norme FIPS 140-2 lors de la génération des hachages de mot de passe qui sont stockés sur le système.	**Emplacement** `/etc/security/pscexpert/dodv2/fipspasswd` **Action de conformité** Garantit que les hachages de mot de passe utilisent un algorithme de hachage approuvé.
GEN000640	2	Cette règle requiert que les mots de passe contiennent un caractère non-alphanumérique au moins.	**Emplacement** `/etc/security/pscexpert/dodv2/chusrattrdod` **Action de conformité** Définit le nombre minimal de caractères non-alphabétiques dans un mot de passe à 1.
GEN000680	2	Cette règle garantit que les mots de passe ne contiennent pas plus de trois caractères identiques consécutifs.	**Emplacement** `/etc/security/pscexpert/dodv2/chusrattrdod` **Action de conformité** Définit le nombre maximal de caractères identiques dans un mot de passe à 3.
GEN000700	2	Cette règle garantit que les fichiers de configuration des mots de passe globaux du système sont configurés conformément aux exigences relatives aux mots de passe.	**Emplacement** `/etc/security/pscexpert/dodv2/chusrattrdod` **Action de conformité** Garantit que les fichiers de configuration des mots de passe satisfont les exigences.

GEN000740	2	Tous les mots de passe de compte non interactifs et de traitement automatisé doivent être verrouillés (GEN000280). Les connexions directes ne doivent pas être autorisées pour les comptes de type partagé, par défaut, application ou utilitaire. (GEN002640) Les comptes système par défaut doivent être désactivés ou supprimés.	**Emplacement**
			`/etc/security/pscexpert/dodv2/loginout`
			`/etc/security/pscexpert/dodv2/lockacc_rlogin`
			Action de conformité
			Ce paramètre est activé automatiquement.

GEN000740	2	Tous les mots de passe de compte non interactifs et de traitement automatisé doivent être changés au moins une fois par an ou verrouillés.	**Emplacement** `/etc/security/pscexpert/dodv2/lockacc_rlogin` **Action de conformité** Garantit que le mots de passe spécifiés sont changés annuellement ou verrouillés.

Tableau 3. Exigences générales du département de la défense des Etats-Unis (suite)

ID de point de contrôle du guide STIG (Department of Defense Security Technical Implemen- tation Guide)	Catégorie de la règle du guide STIG (Department of Defense Security Technical Implemen- tation Guide)	Description	Emplacement du script dans lequel l'action est définie et résultats de l'action assurant la conformité
GEN000750	2	Cette règle requiert qu'un nouveau mot de passe contienne au moins quatre caractères que ne figuraient pas dans l'ancien mot de passe.	**Emplacement** `/etc/security/pscexpert/dodv2/chusrattrdod` **Action de conformité** Définit le nombre minimal de nouveaux caractères requis dans un nouveau mot de passe à 4.
GEN000760	2	Les comptes doivent être verrouillés après 35 jours d'inactivité.	**Emplacement** `/etc/security/pscexpert/dodv2/disableacctdod` **Action de conformité** Verrouille les comptes après 35 jours d'inactivité.
GEN000790	2	Le système doit empêcher l'utilisation de mots du dictionnaire comme mots de passe.	**Emplacement** `/etc/security/pscexpert/dodv2/chuserstanzadod` **Action de conformité** Garantit que le mot de passe par défaut en cours de définition n'est pas faible.
GEN000800	2	Cette règle garantit que les cinq derniers mots de passe ne sont pas réutilisés.	**Emplacement** `/etc/security/pscexpert/dodv2/chusrattrdod` **Action de conformité** Garantit que le nouveau mot de passe n'est pas identique à l'un des cinq derniers mots de passe.
GEN000880 (lié à GEN000300, GEN000320, GEN000380)	2	Tous les comptes sur le système doivent être associés à des noms de compte ou d'utilisateur uniques et à des mots de passe de compte ou d'utilisateur uniques.	**Emplacement** `/etc/security/pscexpert/dodv2/grpusrpass_chk` **Action de conformité** Garantit que tous les comptes satisfont les exigences spécifiées.
GEN000900	3	Le répertoire de base de l'utilisateur root ne doit pas être le répertoire racine (/).	**Emplacement** `/etc/security/pscexpert/dodv2/rootpasswd_home` **Action de conformité** Garantit que le système satisfait l'exigence spécifiée. **Remarque :** Ce paramètre n'est pas modifié automatiquement lorsque la stratégie AIX par défaut est restaurée avec le fichier `DoDv2_to_AIXDefault.xml`. Vous devez le changer manuellement.

Tableau 3. Exigences générales du département de la défense des Etats-Unis (suite)

ID de point de contrôle du guide STIG (Department of Defense Security Technical Implemen- tation Guide)	Catégorie de la règle du guide STIG (Department of Defense Security Technical Implemen- tation Guide)	Description	Emplacement du script dans lequel l'action est définie et résultats de l'action assurant la conformité
GEN000940	2	Le chemin de recherche du fichier exécutable du compte root doit être le chemin par défaut du fournisseur et ne doit contenir que des chemins d'accès absolus.	**Emplacement** `/etc/security/pscexpert/dodv2/fixpathvars` **Action de conformité** Garantit que le système satisfait les exigences spécifiées. **Remarque :** Ce paramètre n'est pas modifié automatiquement lorsque la stratégie AIX par défaut est restaurée avec le fichier `DoDv2_to_AIXDefault.xml`. Vous devez le changer manuellement.
GEN000945	2	Le chemin de recherche de la bibliothèque du compte root doit être le chemin par défaut du système et ne doit contenir que des chemins d'accès absolus.	**Emplacement** `/etc/security/pscexpert/dodv2/fixpathvars` **Action de conformité** Garantit que le système satisfait les exigences spécifiées. **Remarque :** Ce paramètre n'est pas modifié automatiquement lorsque la stratégie AIX par défaut est restaurée avec le fichier `DoDv2_to_AIXDefault.xml`. Vous devez le changer manuellement.
GEN000950	2	La liste des bibliothèques préchargées du compte root doit être vide.	**Emplacement** `/etc/security/pscexpert/dodv2/fixpathvars` **Action de conformité** Garantit que le système satisfait les exigences spécifiées. **Remarque :** Ce paramètre n'est pas modifié automatiquement lorsque la stratégie AIX par défaut est restaurée avec le fichier `DoDv2_to_AIXDefault.xml`. Vous devez le changer manuellement.
GEN000960 (lié à GEN003000, GEN003020, GEN003160, GEN003360, GEN003380)	2	Le chemin de recherche du fichier exécutable du compte root ne doit pas comporter de répertoires accessibles en écriture par tout le monde.	**Emplacement** `/etc/security/pscexpert/dodv2/rmwwpaths` **Action de conformité** Garantit que le système satisfait les exigences spécifiées. **Remarque :** Ce paramètre n'est pas modifié automatiquement lorsque la stratégie AIX par défaut est restaurée avec le fichier `DoDv2_to_AIXDefault.xml`. Vous devez le changer manuellement.
GEN000980	2	Le système doit empêcher le compte root de se connecter directement, sauf pour la console système.	**Emplacement** `/etc/security/pscexpert/dodv2/chuserstanzadod` **Action de conformité** Garantit que le système satisfait les exigences spécifiées.

Tableau 3. Exigences générales du département de la défense des Etats-Unis (suite)

ID de point de contrôle du guide STIG (Department of Defense Security Technical Implemen- tation Guide)	Catégorie de la règle du guide STIG (Department of Defense Security Technical Implemen- tation Guide)	Description	Emplacement du script dans lequel l'action est définie et résultats de l'action assurant la conformité
GEN001000	2	Les consoles distantes doivent être désactivées ou protégées contre les accès non autorisés.	**Emplacement** `/etc/security/pscexpert/dodv2/remoteconsole` **Action de conformité** Garantit que les consoles spécifiées sont désactivées.
GEN001020	2	Le compte root ne doit pas être utilisé pour la connexion directe.	**Emplacement** `/etc/security/pscexpert/dodv2/sshDoDconfig` **Action de conformité** Désactive la connexion directe du compte root.
GEN001060	2	Le système doit journaliser les tentatives d'accès au compte root ayant réussi et ayant échoué.	**Emplacement** `/etc/security/pscexpert/dodv2/loginout` **Action de conformité** Garantit que le système satisfait les exigences spécifiées.
GEN001100	1	Les mots de passe root ne doivent jamais être transmis sur un réseau au format texte.	**Emplacement** `/etc/security/pscexpert/dodv2/chuserstanzadod` **Action de conformité** Garantit que le système satisfait les exigences spécifiées.
GEN001120	2	Le système ne doit pas autoriser la connexion root à l'aide du protocole `SSH`.	**Emplacement** `/etc/security/pscexpert/dodv2/sshDoDconfig` **Action de conformité** Désactive la connexion root pour `SSH`.
GEN001440	3	Tous les utilisateurs interactifs doivent être associés à un répertoire de base dans le fichier `/etc/passwd`.	**Emplacement** `/etc/security/pscexpert/dodv2/grpusrpass_chk` **Action de conformité** Garantit que tous les utilisateurs interactifs sont associés au répertoire spécifié.
GEN001475	2	Le fichier `/etc/group` ne doit contenir aucun hachage de mot de passe de groupe.	**Emplacement** `/etc/security/pscexpert/dodv2/passwdhash` **Action de conformité** Garantit qu'il n'existe pas de hachage de mot de passe de groupe dans le fichier spécifié. **Remarque :** Ce paramètre n'est pas modifié automatiquement lorsque la stratégie AIX par défaut est restaurée avec le fichier `DoDv2_to_AIXDefault.xml`. Vous devez le changer manuellement.

Tableau 3. Exigences générales du département de la défense des Etats-Unis (suite)

ID de point de contrôle du guide STIG (Department of Defense Security Technical Implemen- tation Guide)	Catégorie de la règle du guide STIG (Department of Defense Security Technical Implemen- tation Guide)	Description	Emplacement du script dans lequel l'action est définie et résultats de l'action assurant la conformité
GEN001600	2	Les chemins de recherche du fichier exécutable des scripts de contrôle d'exécution ne doivent contenir que des chemins d'accès absolus.	**Emplacement** `/etc/security/pscexpert/dodv2/fixpathvars` **Action de conformité** Garantit que le système satisfait les exigences spécifiées. **Remarque :** Ce paramètre n'est pas modifié automatiquement lorsque la stratégie AIX par défaut est restaurée avec le fichier `DoDv2_to_AIXDefault.xml`. Vous devez le changer manuellement.
GEN001605	2	Les chemins de recherche de la bibliothèque des scripts de contrôle d'exécution ne doivent contenir que des chemins d'accès absolus.	**Emplacement** `/etc/security/pscexpert/dodv2/fixpathvars` **Action de conformité** Garantit que le système satisfait les exigences spécifiées. **Remarque :** Ce paramètre n'est pas modifié automatiquement lorsque la stratégie AIX par défaut est restaurée avec le fichier `DoDv2_to_AIXDefault.xml`. Vous devez le changer manuellement.
GEN001610	2	Les listes de bibliothèques préchargées des scripts de contrôle d'exécution ne doivent contenir que des chemins d'accès absolus.	**Emplacement** `/etc/security/pscexpert/dodv2/fixpathvars` **Action de conformité** Garantit que le système satisfait les exigences spécifiées. **Remarque :** Ce paramètre n'est pas modifié automatiquement lorsque la stratégie AIX par défaut est restaurée avec le fichier `DoDv2_to_AIXDefault.xml`. Vous devez le changer manuellement.
GEN001840	2	Les chemins de recherche du fichier exécutable des fichiers d'initialisation globaux ne doivent contenir que des chemins d'accès absolus.	**Emplacement** `/etc/security/pscexpert/dodv2/fixpathvars` **Action de conformité** Garantit que le système satisfait les exigences spécifiées. **Remarque :** Ce paramètre n'est pas modifié automatiquement lorsque la stratégie AIX par défaut est restaurée avec le fichier `DoDv2_to_AIXDefault.xml`. Vous devez le changer manuellement.

Tableau 3. Exigences générales du département de la défense des Etats-Unis (suite)

ID de point de contrôle du guide STIG (Department of Defense Security Technical Implemen- tation Guide)	Catégorie de la règle du guide STIG (Department of Defense Security Technical Implemen- tation Guide)	Description	Emplacement du script dans lequel l'action est définie et résultats de l'action assurant la conformité
GEN001845	2	Les chemins de recherche de la bibliothèque des fichiers d'initialisation globaux ne doivent contenir que des chemins d'accès absolus.	**Emplacement** `/etc/security/pscexpert/dodv2/fixpathvars` **Action de conformité** Garantit que le système satisfait les exigences spécifiées. **Remarque :** Ce paramètre n'est pas modifié automatiquement lorsque la stratégie AIX par défaut est restaurée avec le fichier `DoDv2_to_AIXDefault.xml`. Vous devez le changer manuellement.
GEN001850	2	Les listes des bibliothèques préchargées des fichiers d'initialisation globaux ne doivent contenir que des chemins d'accès absolus.	**Emplacement** `/etc/security/pscexpert/dodv2/fixpathvars` **Action de conformité** Garantit que le système satisfait les exigences spécifiées. **Remarque :** Ce paramètre n'est pas modifié automatiquement lorsque la stratégie AIX par défaut est restaurée avec le fichier `DoDv2_to_AIXDefault.xml`. Vous devez le changer manuellement.
GEN001900	2	Les chemins de recherche du fichier exécutable des fichiers d'initialisation locaux ne doivent contenir que des chemins d'accès absolus.	**Emplacement** `/etc/security/pscexpert/dodv2/fixpathvars` **Action de conformité** Garantit que le système satisfait les exigences spécifiées. **Remarque :** Ce paramètre n'est pas modifié automatiquement lorsque la stratégie AIX par défaut est restaurée avec le fichier `DoDv2_to_AIXDefault.xml`. Vous devez le changer manuellement.
GEN001901	2	Les chemins de recherche de la bibliothèque des fichiers d'initialisation locaux ne doivent contenir que des chemins d'accès absolus.	**Emplacement** `/etc/security/pscexpert/dodv2/fixpathvars` **Action de conformité** Garantit que le système satisfait les exigences spécifiées. **Remarque :** Ce paramètre n'est pas modifié automatiquement lorsque la stratégie AIX par défaut est restaurée avec le fichier `DoDv2_to_AIXDefault.xml`. Vous devez le changer manuellement.

Tableau 3. Exigences générales du département de la défense des Etats-Unis (suite)

ID de point de contrôle du guide STIG (Department of Defense Security Technical Implemen- tation Guide)	Catégorie de la règle du guide STIG (Department of Defense Security Technical Implemen- tation Guide)	Description	Emplacement du script dans lequel l'action est définie et résultats de l'action assurant la conformité
GEN001902	2	Les listes des bibliothèques préchargées des fichiers d'initialisation locaux ne doivent contenir que des chemins d'accès absolus.	**Emplacement** `/etc/security/pscexpert/dodv2/fixpathvars` **Action de conformité** Garantit que le système satisfait les exigences spécifiées. **Remarque :** Ce paramètre n'est pas modifié automatiquement lorsque la stratégie AIX par défaut est restaurée avec le fichier `DoDv2_to_AIXDefault.xml`. Vous devez le changer manuellement.
GEN001940	2	Les fichiers d'initialisation utilisateur ne doivent pas être des programmes accessibles en écriture par tout le monde.	**Emplacement** `/etc/security/pscexpert/dodv2/rmwwpaths` **Action de conformité** Garantit que le système satisfait les exigences spécifiées.
GEN001980	2	Les fichiers `.rhosts`, `.shosts`, `hosts.equiv`, `shosts.equiv`, `/etc/passwd`, `/etc/shadow` et `/etc/group` ne doivent pas contenir le signe plus (+) s'ils ne définissent pas les entrées pour les groupes réseau NIS+.	**Emplacement** `/etc/security/pscexpert/dodv2/dodv2netrules` **Action de conformité** Garantit que les fichiers spécifiés satisfont les exigences spécifiées.
GEN002000	2	Il ne doit pas y avoir de fichier `.netrc` sur le système.	**Emplacement** `/etc/security/pscexpert/dodv2/dodv2netrules` **Action de conformité** Garantit que les fichiers spécifiés n'existent pas sur le système. **Remarque :** Ce paramètre n'est pas modifié automatiquement lorsque la stratégie AIX par défaut est restaurée avec le fichier `DoDv2_to_AIXDefault.xml`. Vous devez le changer manuellement.
GEN002020	2	Les fichiers `.rhosts`, `.shosts` et `hosts.equiv` ne doivent contenir que des paires hôte sécurisé-utilisateur.	**Emplacement** `/etc/security/pscexpert/dodv2/dodv2netrules` **Action de conformité** Garantit que les fichiers spécifiés satisfont cette exigence.
GEN002040	1	Cette règle désactive les fichiers `.rhosts`, `.shosts` et `hosts.equiv` ou les fichiers `shosts.equiv`.	**Emplacement** `/etc/security/pscexpert/dodv2/mvhostsfilesdod` **Action de conformité** Désactive les fichiers spécifiés.

Tableau 3. Exigences générales du département de la défense des Etats-Unis (suite)

ID de point de contrôle du guide STIG (Department of Defense Security Technical Implemen- tation Guide)	Catégorie de la règle du guide STIG (Department of Defense Security Technical Implemen- tation Guide)	Description	Emplacement du script dans lequel l'action est définie et résultats de l'action assurant la conformité
GEN002120	1,2	Cette règle vérifie et configure les shells utilisateur.	**Emplacement** `/etc/security/pscexpert/dodv2/usershells` **Action de conformité** Crée les shells requis. **Remarque :** Ce paramètre n'est pas modifié automatiquement lorsque la stratégie AIX par défaut est restaurée avec le fichier `DoDv2_to_AIXDefault.xml`. Vous devez le changer manuellement.
GEN002140	1,2	Tous les shells qui sont référencés dans la liste `/etc/passwd` doivent être répertoriés dans le fichier `/etc/shells`, sauf ceux pour lesquels les connexions sont empêchées.	**Emplacement** `/etc/security/pscexpert/dodv2/usershells` **Action de conformité** Garantit que les shells sont répertoriés dans les fichiers appropriés. **Remarque :** Ce paramètre n'est pas modifié automatiquement lorsque la stratégie AIX par défaut est restaurée avec le fichier `DoDv2_to_AIXDefault.xml`. Vous devez le changer manuellement.
GEN002280	2	Les fichiers d'unité et les répertoires doivent être accessibles en écriture par les utilisateurs ayant un compte système uniquement, ou conformément à la configuration du système par le fournisseur.	**Emplacement** `/etc/security/pscexpert/dodv2/wwdevfiles` **Action de conformité** Affiche les fichiers d'unité, les répertoires et tout autre fichier sur le système qui sont accessibles en écriture par tout le monde et qui se trouvent dans des répertoires non publics.
GEN002300	2	Les fichiers d'unité qui sont utilisés pour la sauvegarde doivent être accessibles en lecture et/ou en écriture uniquement par l'utilisateur root ou l'utilisateur effectuant la sauvegarde.	**Emplacement** `/etc/security/pscexpert/dodv2/wwdevfiles` **Action de conformité** Affiche les fichiers d'unité, les répertoires et tout autre fichier sur le système qui sont accessibles en écriture par tout le monde et qui se trouvent dans des répertoires non publics.

Tableau 3. Exigences générales du département de la défense des Etats-Unis (suite)

ID de point de contrôle du guide STIG (Department of Defense Security Technical Implemen- tation Guide)	Catégorie de la règle du guide STIG (Department of Defense Security Technical Implemen- tation Guide)	Description	Emplacement du script dans lequel l'action est définie et résultats de l'action assurant la conformité
GEN002400	2	Les fichiers `setuid` non autorisés doivent être identifiés toutes les semaines sur le système, de même que la modification non autorisée des fichiers `setuid` autorisés.	**Emplacement** `/etc/security/pscexpert/dodv2/trust` **Action de conformité** Identifie toutes les semaines les modifications apportées aux fichiers spécifiés. **Remarque :** Comparez les deux journaux hebdomadaires les plus récents qui sont créés dans le répertoire `/var/security/pscexpert` afin de vérifier qu'aucune activité non autorisée n'a eu lieu.
GEN002420	2	Les supports amovibles, les systèmes de fichiers distants et tout système de fichiers ne contenant pas de fichier `setuid` approuvé doivent être montés avec l'option *nosuid*.	**Emplacement** `/etc/security/pscexpert/dodv2/fsmntoptions` **Action de conformité** Garantit que les options spécifiées sont sélectionnées pour les systèmes de fichiers montés à distance. **Remarque :** Ce paramètre n'est pas modifié automatiquement lorsque la stratégie AIX par défaut est restaurée avec le fichier `DoDv2_to_AIXDefault.xml`. Vous devez le changer manuellement.
GEN002430	2	Les supports amovibles, les systèmes de fichiers distants et tout système de fichiers ne contenant pas de fichier d'unité approuvé doivent être montés avec l'option *nodev*.	**Emplacement** `/etc/security/pscexpert/dodv2/fsmntoptions` **Action de conformité** Garantit que les options spécifiées sont sélectionnées pour les systèmes de fichiers montés à distance. **Remarque :** Ce paramètre n'est pas modifié automatiquement lorsque la stratégie AIX par défaut est restaurée avec le fichier `DoDv2_to_AIXDefault.xml`. Vous devez le changer manuellement.

GEN002480	2	Les répertoires publics doivent être les seuls répertoires accessibles en écriture par tout le monde, et les fichiers accessibles en écriture par tout le monde doivent se trouver uniquement dans des répertoires publics.	**Emplacement**
			`/etc/security/pscexpert/dodv2/wwdevfiles`
			`/etc/security/pscexpert/dodv2/fpmdodfiles`
			Action de conformité
			Prévient lorsque des fichiers accessibles en écriture par tout le monde ne se trouvent pas dans des répertoires publics.

Tableau 3. Exigences générales du département de la défense des Etats-Unis (suite)

ID de point de contrôle du guide STIG (Department of Defense Security Technical Implemen- tation Guide)	Catégorie de la règle du guide STIG (Department of Defense Security Technical Implemen- tation Guide)	Description	Emplacement du script dans lequel l'action est définie et résultats de l'action assurant la conformité

GEN002640	2	Les comptes système par défaut doivent être désactivés ou supprimés.	**Emplacement**
			`/etc/security/pscexpert/dodv2/lockacc_rlogin`
			`/etc/security/pscexpert/dodv2/loginout`
			Action de conformité
			Désactive les comptes système par défaut.

GEN002660	2	La fonction d'audit doit être activée.	**Emplacement** `/etc/security/pscexpert/dodv2/dodaudit` **Action de conformité** Active la commande `dodaudit`, qui active la fonction d'audit.
GEN002720	2	Le système d'audit doit être configuré pour effectuer un audit des échecs d'accès à des fichiers et des programmes.	**Emplacement** `/etc/security/pscexpert/dodv2/dodaudit` **Action de conformité** Active automatiquement la fonction d'audit spécifiée.
GEN002740	2	Le système d'audit doit être configuré pour effectuer un audit des suppressions de fichier.	**Emplacement** `/etc/security/pscexpert/dodv2/dodaudit` **Action de conformité** Active automatiquement la fonction d'audit spécifiée.
GEN002750	3	Le système d'audit doit être configuré pour effectuer un audit de la création de compte.	**Emplacement** `/etc/security/pscexpert/dodv2/dodaudit` **Action de conformité** Active automatiquement la fonction d'audit spécifiée.
GEN002751	3	Le système d'audit doit être configuré pour effectuer un audit de la modification de compte.	**Emplacement** `/etc/security/pscexpert/dodv2/dodaudit` **Action de conformité** Active automatiquement la fonction d'audit spécifiée.
GEN002752	3	Le système d'audit doit être configuré pour effectuer un audit des comptes désactivés.	**Emplacement** `/etc/security/pscexpert/dodv2/dodaudit` **Action de conformité** Active automatiquement la fonction d'audit spécifiée.

Tableau 3. Exigences générales du département de la défense des Etats-Unis (suite)

ID de point de contrôle du guide STIG (Department of Defense Security Technical Implemen- tation Guide)	Catégorie de la règle du guide STIG (Department of Defense Security Technical Implemen- tation Guide)	Description	Emplacement du script dans lequel l'action est définie et résultats de l'action assurant la conformité
GEN002753	3	Le système d'audit doit être configuré pour effectuer un audit de la résiliation de compte.	**Emplacement** `/etc/security/pscexpert/dodv2/dodaudit` **Action de conformité** Active automatiquement la fonction d'audit spécifiée.
GEN002760	2	Le système d'audit doit être configuré pour effectuer un audit de toutes les actions administratives, privilégiées et de sécurité.	**Emplacement** `/etc/security/pscexpert/dodv2/dodaudit` **Action de conformité** Active automatiquement la fonction d'audit spécifiée.
GEN002800	2	Le système d'audit doit être configuré pour effectuer un audit des connexions, des déconnexions et des ouvertures de session.	**Emplacement** `/etc/security/pscexpert/dodv2/dodaudit` **Action de conformité** Active automatiquement la fonction d'audit spécifiée.
GEN002820	2	Le système d'audit doit être configuré pour effectuer un audit de toutes les modifications portant sur les autorisations de contrôle d'accès discrétionnaire.	**Emplacement** `/etc/security/pscexpert/dodv2/dodaudit` **Action de conformité** Active automatiquement la fonction d'audit spécifiée.
GEN002825	2	Le système d'audit doit être configuré pour effectuer un audit du chargement et du déchargement des modules de noyau dynamiques.	**Emplacement** `/etc/security/pscexpert/dodv2/dodaudit` **Action de conformité** Active automatiquement la fonction d'audit spécifiée.
GEN002860	2	Les journaux d'audit doivent faire l'objet d'une rotation quotidienne.	**Emplacement** `/etc/security/pscexpert/dodv2/rotateauditdod` **Action de conformité** Garantit que les journaux d'audit font l'objet d'une rotation.
GEN002960	2	L'accès à l'utilitaire `cron` doit être contrôlé avec le fichier `cron.allow` et/ou le fichier `cron.deny`.	**Emplacement** `/etc/security/pscexpert/dodv2/limitsysacc` **Action de conformité** Garantit que les limites de conformité sont activées.

Tableau 3. Exigences générales du département de la défense des Etats-Unis (suite)

ID de point de contrôle du guide STIG (Department of Defense Security Technical Implemen- tation Guide)	Catégorie de la règle du guide STIG (Department of Defense Security Technical Implemen- tation Guide)	Description	Emplacement du script dans lequel l'action est définie et résultats de l'action assurant la conformité
GEN003000 (lié à GEN000960, GEN003020, GEN003160, GEN003360, GEN003380)	2	`Cron` ne doit pas exécuter de programmes accessibles en écriture par des groupes ou par tout le monde.	**Emplacement** `/etc/security/pscexpert/dodv2/rmwwpaths` **Action de conformité** Garantit que les limites de conformité sont activées. **Remarque :** Ce paramètre n'est pas modifié automatiquement lorsque la stratégie AIX par défaut est restaurée avec le fichier `DoDv2_to_AIXDefault.xml`. Vous devez le changer manuellement.
GEN003020 (lié à GEN000960, GEN003000, GEN003160, GEN003360, GEN003380)	2	`Cron` ne doit pas exécuter de programmes qui se trouvent dans des répertoires accessibles en écriture par tout le monde, ou qui y sont subordonnés.	**Emplacement** `/etc/security/pscexpert/dodv2/rmwwpaths` **Action de conformité** Supprime le droit d'accès en écriture par tout le monde pour les répertoires du programme `cron`. **Remarque :** Ce paramètre n'est pas modifié automatiquement lorsque la stratégie AIX par défaut est restaurée avec le fichier `DoDv2_to_AIXDefault.xml`. Vous devez le changer manuellement.
GEN003060	2	Les comptes système par défaut (sauf pour root) ne doivent pas être répertoriés dans le fichier `cron.allow` ou doivent être inclus dans le fichier `cron.deny` si le fichier `cron.allow` n'existe pas.	**Emplacement** `cron.allow` ou `cron.deny` **Action de conformité** Garantit que le système satisfait les exigences spécifiées.
GEN003160 (lié à GEN000960, GEN003000, GEN003020, GEN003360, GEN003380)	2	La journalisation `Cron` doit être démarrée.	**Emplacement** `/etc/security/pscexpert/dodv2/rmwwpaths` **Action de conformité** Garantit que le système satisfait les exigences spécifiées.
GEN003280	2	L'accès à l'utilitaire `at` doit être contrôlé à l'aide des fichiers `at.allow` et `at.deny`.	**Emplacement** `/etc/security/pscexpert/dodv2/chcronfilesdod` **Action de conformité** Garantit que le système satisfait les exigences spécifiées.
GEN003300	2	Le fichier `at.deny` ne doit pas être vide, s'il existe.	**Emplacement** `/etc/security/pscexpert/dodv2/chcronfilesdod` **Action de conformité** Garantit que le système satisfait les exigences spécifiées.

Tableau 3. Exigences générales du département de la défense des Etats-Unis (suite)

ID de point de contrôle du guide STIG (Department of Defense Security Technical Implemen- tation Guide)	Catégorie de la règle du guide STIG (Department of Defense Security Technical Implemen- tation Guide)	Description	Emplacement du script dans lequel l'action est définie et résultats de l'action assurant la conformité
GEN003320	2	Les comptes système par défaut autres que root ne doivent pas être répertoriés dans le fichier `at.allow` ou doivent être inclus dans le fichier `at.deny` si le fichier `at.allow` n'existe pas.	**Emplacement** `/etc/security/pscexpert/dodv2/chcronfilesdod` **Action de conformité** Garantit que le système satisfait les exigences spécifiées.
GEN003360 (lié à GEN000960, GEN003000, GEN003020, GEN003160, GEN003380)	2	Le démon `at` ne doit pas exécuter de programmes accessibles en écriture par des groupes ou par tout le monde.	**Emplacement** `/etc/security/pscexpert/dodv2/rmwwpaths` **Action de conformité** Garantit que le système satisfait les exigences spécifiées. **Remarque :** Ce paramètre n'est pas modifié automatiquement lorsque la stratégie AIX par défaut est restaurée avec le fichier `DoDv2_to_AIXDefault.xml`. Vous devez le changer manuellement.
GEN003380 (lié à GEN000960, GEN003000, GEN003020, GEN003160, GEN003360)	2	Le démon `at` ne doit pas exécuter de programmes qui se trouvent dans des répertoires accessibles en écriture par tout le monde, ou qui y sont subordonnés.	**Emplacement** `/etc/security/pscexpert/dodv2/rmwwpaths` **Action de conformité** Garantit que le système satisfait les exigences spécifiées. **Remarque :** Ce paramètre n'est pas modifié automatiquement lorsque la stratégie AIX par défaut est restaurée avec le fichier `DoDv2_to_AIXDefault.xml`. Vous devez le changer manuellement.
GEN003510	2	Les clichés du processus core du noyau doivent être désactivés sauf s'ils sont requis.	**Emplacement** `/etc/security/pscexpert/dodv2/coredumpdev` **Action de conformité** Désactive les clichés du processus core du noyau.
GEN003540	2	Le système doit utiliser des piles d'appels non exécutables.	**Emplacement** `/etc/security/pscexpert/dodv2/sedconfigdod` **Action de conformité** Impose l'utilisation de piles d'appels non exécutables.
GEN003600	2	Le système ne doit pas transmettre de paquet IPv4 acheminé par la source.	**Emplacement** `/etc/security/pscexpert/dodv2/ntwkoptsdod` **Action de conformité** Associe l'option de réseau `ipsrcforward` à la valeur *0*.

Tableau 3. Exigences générales du département de la défense des Etats-Unis (suite)

ID de point de contrôle du guide STIG (Department of Defense Security Technical Implemen- tation Guide)	Catégorie de la règle du guide STIG (Department of Defense Security Technical Implemen- tation Guide)	Description	Emplacement du script dans lequel l'action est définie et résultats de l'action assurant la conformité
GEN003601	2	Les tailles des files d'attente de retards TCP doivent être définies de manière appropriée.	**Emplacement** `/etc/security/pscexpert/dodv2/ntwkoptsdod` **Action de conformité** Associe l'option de réseau `clean_partial_conns` à la valeur *1*.
GEN003603	2	Le système ne doit pas répondre aux commandes echo d'Internet Control Message Protocol version 4 (ICMPv4) qui sont envoyées à une adresse de diffusion.	**Emplacement** `/etc/security/pscexpert/dodv2/ntwkoptsdod` **Action de conformité** Associe l'option de réseau `bcastping` à la valeur *0*.
GEN003604	2	Le système ne doit pas répondre au demandes d'horodatage ICMP qui sont envoyées à une adresse de diffusion.	**Emplacement** `/etc/security/pscexpert/dodv2/ntwkoptsdod` **Action de conformité** Associe l'option de réseau `bcastping` à la valeur *0*.
GEN003605	2	Le système ne doit pas appliquer le routage par la source inversé aux réponses TCP.	**Emplacement** `/etc/security/pscexpert/dodv2/ntwkoptsdod` **Action de conformité** Associe l'option de réseau `nonlocsrcroute` à la valeur *0*.
GEN003606	2	Le système doit empêcher les applications locales de générer des paquets acheminés par la source.	**Emplacement** `/etc/security/pscexpert/dodv2/ntwkoptsdod` **Action de conformité** Associe l'option de réseau `ipsrcroutesend` à la valeur *0*.
GEN003607	2	Le système ne doit pas accepter de paquet IPv4 acheminé par la source.	**Emplacement** `/etc/security/pscexpert/dodv2/ntwkoptsdod` **Action de conformité** Désactive la possibilité d'accepter des paquets IPv4 acheminés par la source.
GEN003609	2	Le système doit ignorer les messages de redirection ICMP IPv4.	**Emplacement** `/etc/security/pscexpert/dodv2/ntwkoptsdod` **Action de conformité** Associe l'option de réseau `ipignoreredirects` à la valeur *1*.
GEN003610	2	Le système ne doit pas envoyer de message de redirection ICMP IPv4.	**Emplacement** `/etc/security/pscexpert/dodv2/ntwkoptsdod` **Action de conformité** Associe l'option de réseau `ipsendredirects` à la valeur *0*.

Tableau 3. Exigences générales du département de la défense des Etats-Unis (suite)

ID de point de contrôle du guide STIG (Department of Defense Security Technical Implemen- tation Guide)	Catégorie de la règle du guide STIG (Department of Defense Security Technical Implemen- tation Guide)	Description	Emplacement du script dans lequel l'action est définie et résultats de l'action assurant la conformité
GEN003612	2	Le système doit être configuré pour utiliser des syncookies TCP lorsqu'une attaque de type SYN flood survient.	**Emplacement** `/etc/security/pscexpert/dodv2/ntwkoptsdod` **Action de conformité** Associe l'option de réseau `clean_partial_conns` à la valeur *1*.
GEN003640	2	Le système de fichiers racine doit utiliser la journalisation ou une autre méthode assurant la cohérence du système de fichiers.	**Emplacement** `/etc/security/pscexpert/dodv2/chkjournal` **Action de conformité** Active la journalisation du système de fichiers racine.
GEN003660	2	Le système doit journaliser les informations sur l'authentification.	**Emplacement** `/etc/security/pscexpert/dodv2/chsyslogdod` **Action de conformité** Active la journalisation des données `auth` et `info`.
GEN003700	2	`inetd` et `xinetd` doivent être désactivés ou supprimés si aucun service de réseau ne les utilise.	**Emplacement** `/etc/security/pscexpert/dodv2/dodv2services` **Action de conformité** Garantit que le système satisfait les exigences spécifiées.
GEN003810	2	Les services `portmap` ou `rpcbind` ne doivent pas être démarrés sauf s'ils sont requis.	**Emplacement** `/etc/security/pscexpert/dodv2/dodv2services` **Action de conformité** Garantit que le système satisfait les exigences spécifiées.
GEN003815	2	Les services `portmap` ou `rpcbind` ne doivent pas être installés sauf s'ils sont utilisés.	**Emplacement** `/etc/security/pscexpert/dodv2/dodv2services` **Action de conformité** Garantit que le système satisfait les exigences spécifiées.
GEN003820-3860	1,2,3	Les démons `rsh`, `rexexec` et `telnet` ainsi que le service `rlogind` ne doivent pas être démarrés.	**Emplacement** `/etc/security/pscexpert/dodv2/inetdservices` **Action de conformité** Désactive les démons et les services requis en mettant en commentaire les entrées dans le fichier `/etc/inetd.conf`.
GEN003865	2	Vous ne devez pas installer d'outils d'analyse du réseau.	**Emplacement** `/etc/security/pscexpert/dodv2/dodv2services` **Action de conformité** Garantit que le système satisfait les exigences spécifiées.

Tableau 3. Exigences générales du département de la défense des Etats-Unis (suite)

ID de point de contrôle du guide STIG (Department of Defense Security Technical Implemen- tation Guide)	Catégorie de la règle du guide STIG (Department of Defense Security Technical Implemen- tation Guide)	Description	Emplacement du script dans lequel l'action est définie et résultats de l'action assurant la conformité
GEN003900	2	Le fichier `hosts.lpd` (ou un équivalent) ne doit pas contenir le signe plus (+).	**Emplacement** `/etc/security/pscexpert/dodv2/printers` **Action de conformité** Garantit que le système satisfait les exigences spécifiées.
GEN004220	1	des comptes d'administration ne doivent pas exécuter de navigateur Web, sauf si nécessaire pour l'administration des services locaux.	**Emplacement** `/etc/security/pscexpert/dodv2/dodv2cat1` **Action de conformité** Affiche les résultats des tests de règle spécifiés.
GEN004460	2	Cette règle journalise les données `auth` et `info`.	**Emplacement** `/etc/security/pscexpert/dodv2/chsyslogdod` **Action de conformité** Active la journalisation des données `auth` et `info`.

GEN004540	2	Cette règle désactive la commande d'aide `sendmail`.	**Emplacement**
			`/etc/security/pscexpert/dodv2/sendmailhelp`
			`/etc/security/pscexpert/dodv2/dodv2cmntrows`
			Action de conformité
			Désactive la commande spécifiée.

GEN004580	2	Le système ne doit pas utiliser de fichier `.forward`.	**Emplacement** `/etc/security/pscexpert/dodv2/forward` **Action de conformité** Désactive les fichiers spécifiés. **Remarque :** Ce paramètre n'est pas modifié automatiquement lorsque la stratégie AIX par défaut est restaurée avec le fichier `DoDv2_to_AIXDefault.xml`. Vous devez le changer manuellement.
GEN004600	1	La version du service `SMTP` doit être la plus récente.	**Emplacement** `/etc/security/pscexpert/dodv2/SMTP_ver` **Action de conformité** Garantit que la version la plus récente du service spécifié est démarrée. **Remarque :** Ce paramètre n'est pas modifié automatiquement lorsque la stratégie AIX par défaut est restaurée avec le fichier `DoDv2_to_AIXDefault.xml`. Vous devez le changer manuellement.

Tableau 3. Exigences générales du département de la défense des Etats-Unis (suite)

ID de point de contrôle du guide STIG (Department of Defense Security Technical Implemen- tation Guide)	Catégorie de la règle du guide STIG (Department of Defense Security Technical Implemen- tation Guide)	Description	Emplacement du script dans lequel l'action est définie et résultats de l'action assurant la conformité
GEN004620	2	La fonction de débogage doit être désactivée sur le serveur `sendmail`.	**Emplacement** `/etc/security/pscexpert/dodv2/SMTP_ver` **Action de conformité** Désactive la fonction de débogage `sendmail`.
GEN004640	1	Le service `SMTP` ne doit pas présenter d'alias `uudecode` actif.	**Emplacement** `/etc/security/pscexpert/dodv2/SMTPuucode` **Action de conformité** Désactive l'alias `uudecode`.
GEN004710	2	Le relais de courrier doit être restreint.	**Emplacement** `/etc/security/pscexpert/dodv2/sendmaildod` **Action de conformité** Restreint le relais de courrier.
GEN004800	1,2,3	Le protocole FTP non chiffré ne doit pas être utilisé sur le système.	**Emplacement** `/etc/security/pscexpert/dodv2/inetdservices` **Action de conformité** Désactive les démons et les services requis en mettant en commentaire les entrées dans le fichier `/etc/inetd.conf`.
GEN004820	2	Le serveur FTP anonyme ne doit pas être actif sur le système sauf s'il est autorisé.	**Emplacement** `/etc/security/pscexpert/dodv2/anonuser` **Action de conformité** Désactive le serveur FTP anonyme sur le système. **Remarque :** Ce paramètre n'est pas modifié automatiquement lorsque la stratégie AIX par défaut est restaurée avec le fichier `DoDv2_to_AIXDefault.xml`. Vous devez le changer manuellement.
GEN004840	2	Si le système est un serveur FTP anonyme, il doit être isolé sur le réseau dans une zone démilitarisée.	**Emplacement** `/etc/security/pscexpert/dodv2/anonuser` **Action de conformité** Garantit qu'un serveur FTP anonyme sur le système se trouve sur le réseau dans une zone démilitarisée.
GEN004880	2	Le fichier `ftpusers` doit exister.	**Emplacement** `/etc/security/pscexpert/dodv2/chdodftpusers` **Action de conformité** Garantit que le fichier spécifié se trouve sur le système.

Tableau 3. Exigences générales du département de la défense des Etats-Unis (suite)

ID de point de contrôle du guide STIG (Department of Defense Security Technical Implemen- tation Guide)	Catégorie de la règle du guide STIG (Department of Defense Security Technical Implemen- tation Guide)	Description	Emplacement du script dans lequel l'action est définie et résultats de l'action assurant la conformité
GEN004900	2	Le fichier `ftpusers` doit contenir les noms de compte qui ne sont pas autorisés à utiliser le protocole FTP.	**Emplacement** `/etc/security/pscexpert/dodv2/chdodftpusers` **Action de conformité** Garantit que le fichier contient les noms de compte requis.
GEN005000	1	Les comptes FTP anonymes ne doivent pas posséder de shell fonctionnel.	**Emplacement** `/etc/security/pscexpert/dodv2/usershells` **Action de conformité** Supprime les shells des comptes FTP anonymes. **Remarque :** Ce paramètre n'est pas modifié automatiquement lorsque la stratégie AIX par défaut est restaurée avec le fichier `DoDv2_to_AIXDefault.xml`. Vous devez le changer manuellement.
GEN005080	1	Le démon `TFTP` doit fonctionner en mode sécurisé ; ce dernier fournit l'accès à un seul répertoire sur le système de fichiers hôte.	**Emplacement** `/etc/security/pscexpert/dodv2/tftpdod` **Action de conformité** Garantit que le démon satisfait les exigences spécifiées.
GEN005120	2	Le démon TFTP doit être configuré conformément aux spécifications du fournisseur, comprenant un compte utilisateur TFTP dédié, un shell sans connexion, par exemple `/bin/false`, et un répertoire de base appartenant à l'utilisateur TFTP.	**Emplacement** `/etc/security/pscexpert/dodv2/tftpdod` **Action de conformité** Garantit que le système satisfait les exigences spécifiées.
GEN005140	1,2,3	Tout démon TFTP actif doit être autorisé et approuvé dans le module d'accréditation du système.	**Emplacement** `/etc/security/pscexpert/dodv2/inetdservices` **Action de conformité** Garantit que le démon est autorisé.
GEN005160	1,2	Tout hôte du système X Window doit écrire des fichiers `.Xauthority`.	**Emplacement** `/etc/security/pscexpert/dodv2/dodv2disableX` **Action de conformité** Garantit que l'hôte a écrit les fichiers spécifiés.
GEN005200	1,2	Aucun affichage du système X Window ne peut être exporté publiquement.	**Emplacement** `/etc/security/pscexpert/dodv2/dodv2disableX` **Action de conformité** Désactive la dissémination des programmes spécifiés.

Tableau 3. Exigences générales du département de la défense des Etats-Unis (suite)

ID de point de contrôle du guide STIG (Department of Defense Security Technical Implemen- tation Guide)	Catégorie de la règle du guide STIG (Department of Defense Security Technical Implemen- tation Guide)	Description	Emplacement du script dans lequel l'action est définie et résultats de l'action assurant la conformité
GEN005220	1,2	Les fichiers `.Xauthority` ou `X*.hosts` (ou des équivalents) doivent être utilisés pour restreindre l'accès au serveur du système X Window.	**Emplacement** `/etc/security/pscexpert/dodv2/dodv2disableX` **Action de conformité** Garantit que les fichiers spécifiés sont disponibles pour restreindre l'accès au serveur.
GEN005240	1,2	L'utilitaire .Xauthority doit accorder l'accès aux hôtes autorisés seulement.	**Emplacement** `/etc/security/pscexpert/dodv2/dodv2disableX` **Action de conformité** Garantit que l'accès est limité aux hôtes autorisés.
GEN005260	2	Cette règle désactive les connexions du système X Window et le gestionnaire de connexion du serveur X.	**Emplacement** `/etc/security/pscexpert/dodv2/dodv2cmntrows` **Action de conformité** Désactive les connexions requises et le gestionnaire de connexion.
GEN005280	1,2,3	Le service `UUCP` ne doit pas être actif sur le système.	**Emplacement** `/etc/security/pscexpert/dodv2/inetdservices` **Action de conformité** Désactive les démons et les services requis en mettant en commentaire les entrées dans le fichier `/etc/inetd.conf`.
GEN005300	2	Les paramètres par défaut des communautés SNMP doivent être changés.	**Emplacement** `/etc/security/pscexpert/dodv2/chsnmp` **Action de conformité** Garantit que le système satisfait les exigences spécifiées.
GEN005305	2	Le service SNMP doit utiliser SNMPv3 ou une version ultérieure seulement.	**Emplacement** `/etc/security/pscexpert/dodv2/chsnmp` **Action de conformité** Garantit que le système satisfait les exigences spécifiées.
GEN005306	2	Le service SNMP doit exiger l'utilisation d'une norme FIPS 140-2.	**Emplacement** `/etc/security/pscexpert/dodv2/chsnmp` **Action de conformité** Garantit que le système satisfait les exigences spécifiées.

Tableau 3. Exigences générales du département de la défense des Etats-Unis (suite)

ID de point de contrôle du guide STIG (Department of Defense Security Technical Implemen- tation Guide)	Catégorie de la règle du guide STIG (Department of Defense Security Technical Implemen- tation Guide)	Description	Emplacement du script dans lequel l'action est définie et résultats de l'action assurant la conformité
GEN005440	2	Le système doit utiliser un serveur syslog distant (hôte de journal).	**Emplacement** `/etc/security/pscexpert/dodv2/EnableTrustedLogging` **Action de conformité** Garantit que le système utilise un serveur syslog distant.
GEN005450	2	Le système doit utiliser un serveur syslog distant (hôte de journal).	**Emplacement** `/etc/security/pscexpert/dodv2/EnableTrustedLogging` **Action de conformité** Garantit que le système utilise un serveur syslog distant.
GEN005460	2	Le système doit utiliser un serveur syslog distant (hôte de journal).	**Emplacement** `/etc/security/pscexpert/dodv2/EnableTrustedLogging` **Action de conformité** Garantit que le système utilise un serveur syslog distant.
GEN005480	2	Le système doit utiliser un serveur syslog distant (hôte de journal).	**Emplacement** `/etc/security/pscexpert/dodv2/EnableTrustedLogging` **Action de conformité** Garantit que le système utilise un serveur syslog distant.
GEN005500	2	Le démon `SSH` doit être configuré pour n'utiliser que le protocole Secure Shell version 2 (SSHv2).	**Emplacement** `/etc/security/pscexpert/dodv2/sshDoDconfig` **Action de conformité** Garantit que le système satisfait les exigences spécifiées.
GEN005501	2	Le client `SSH` doit être configuré pour n'utiliser que le protocole SSHv2.	**Emplacement** `/etc/security/pscexpert/dodv2/sshDoDconfig` **Action de conformité** Garantit que le système satisfait les exigences spécifiées.
GEN005504	2	Le démon `SSH` doit être à l'écoute des adresses réseau de gestion seulement, sauf s'il est autorisé pour des utilisations autres que la gestion.	**Emplacement** `/etc/security/pscexpert/dodv2/sshDoDconfig` **Action de conformité** Garantit que le système satisfait les exigences spécifiées.
GEN005505	2	Le démon `SSH` doit être configuré pour n'utiliser que des chiffrements conformes aux normes FIPS 140-2 (Federal Information Processing Standards).	**Emplacement** `/etc/security/pscexpert/dodv2/sshDoDconfig` **Action de conformité** Garantit que le système satisfait les exigences spécifiées.

Tableau 3. Exigences générales du département de la défense des Etats-Unis (suite)

ID de point de contrôle du guide STIG (Department of Defense Security Technical Implemen- tation Guide)	Catégorie de la règle du guide STIG (Department of Defense Security Technical Implemen- tation Guide)	Description	Emplacement du script dans lequel l'action est définie et résultats de l'action assurant la conformité
GEN005506	2	Le démon SSH doit être configuré pour n'utiliser que des chiffrements conformes aux normes FIPS 140-2.	**Emplacement** /etc/security/pscexpert/dodv2/sshDoDconfig **Action de conformité** Garantit que le système satisfait les exigences spécifiées.
GEN005507	2	Le démon SSH doit être configuré pour n'utiliser que des codes d'authentification de message avec des algorithmes de hachage cryptographique conformes aux normes FIPS 140-2.	**Emplacement** /etc/security/pscexpert/dodv2/sshDoDconfig **Action de conformité** Garantit que le système satisfait les exigences spécifiées.
GEN005510	2	Le client SSH doit être configuré pour n'utiliser que des codes d'authentification de message avec des chiffrements conformes aux normes FIPS 140-2.	**Emplacement** /etc/security/pscexpert/dodv2/sshDoDconfig **Action de conformité** Garantit que le système satisfait les exigences spécifiées.
GEN005511	2	Le client SSH doit être configuré pour n'utiliser que des codes d'authentification de message avec des chiffrements conformes aux normes FIPS 140-2.	**Emplacement** /etc/security/pscexpert/dodv2/sshDoDconfig **Action de conformité** Garantit que le système satisfait les exigences spécifiées.
GEN005512	2	Le démon SSH doit être configuré pour n'utiliser que des codes d'authentification de message avec des algorithmes de hachage cryptographique conformes aux normes FIPS 140-2.	**Emplacement** /etc/security/pscexpert/dodv2/sshDoDconfig **Action de conformité** Garantit que le système satisfait les exigences spécifiées.
GEN005521	2	Le démon SSH doit restreindre la connexion à des utilisateurs et/ou à des groupes spécifiques.	**Emplacement** /etc/security/pscexpert/dodv2/sshDoDconfig **Action de conformité** Garantit que le système satisfait les exigences spécifiées.
GEN005536	2	Le démon SSH doit procéder à une vérification en mode strict des fichiers de configuration du répertoire de base.	**Emplacement** /etc/security/pscexpert/dodv2/sshDoDconfig **Action de conformité** Garantit que le système satisfait les exigences spécifiées.
GEN005537	2	Le démon SSH doit utiliser la séparation des privilèges.	**Emplacement** /etc/security/pscexpert/dodv2/sshDoDconfig **Action de conformité** Garantit que le système satisfait les exigences spécifiées.

Tableau 3. Exigences générales du département de la défense des Etats-Unis (suite)

ID de point de contrôle du guide STIG (Department of Defense Security Technical Implemen- tation Guide)	Catégorie de la règle du guide STIG (Department of Defense Security Technical Implemen- tation Guide)	Description	Emplacement du script dans lequel l'action est définie et résultats de l'action assurant la conformité
GEN005538	2	Le démon SSH ne doit pas autoriser rhosts à s'authentifier avec le système de cryptographie Rivest-Shamir-Adleman (RSA).	**Emplacement** /etc/security/pscexpert/dodv2/sshDoDconfig **Action de conformité** Garantit que le système satisfait les exigences spécifiées.
GEN005539	2	Le démon SSH ne doit pas autoriser la compression ou ne doit l'autoriser qu'après une authentification réussie.	**Emplacement** /etc/security/pscexpert/dodv2/sshDoDconfig **Action de conformité** Garantit que le système satisfait les exigences spécifiées.
GEN005550	2	Le démon SSH doit être configuré avec la bannière de connexion du département de la défense des Etats-Unis.	**Emplacement** /etc/security/pscexpert/dodv2/sshDoDconfig **Action de conformité** Garantit que le système satisfait les exigences spécifiées.
GEN005560	2	Déterminez si une passerelle par défaut est configurée pour IPv4.	**Emplacement** /etc/security/pscexpert/dodv2/chkgtway **Action de conformité** Garantit que le système satisfait les exigences spécifiées. **Remarque :** Ce paramètre n'est pas modifié automatiquement lorsque la stratégie AIX par défaut est restaurée avec le fichier DoDv2_to_AIXDefault.xml. Vous devez le changer manuellement. **Remarque :** Si votre système exécute le protocole IPv6, assurez-vous que le paramètre *ipv6_enabled* dans le fichier /etc/security/pscexpert/ipv6.conf a pour valeur yes. S'il n'utilise pas IPv6, assurez-vous que le paramètre *ipv6_enabled* a pour valeur no.

Tableau 3. Exigences générales du département de la défense des Etats-Unis (suite)

ID de point de contrôle du guide STIG (Department of Defense Security Technical Implemen- tation Guide)	Catégorie de la règle du guide STIG (Department of Defense Security Technical Implemen- tation Guide)	Description	Emplacement du script dans lequel l'action est définie et résultats de l'action assurant la conformité
GEN005570	2	Déterminez si une passerelle par défaut est configurée pour IPv6.	**Emplacement** `/etc/security/pscexpert/dodv2/chkgtway` **Action de conformité** Garantit que le système satisfait les exigences spécifiées. **Remarque :** Ce paramètre n'est pas modifié automatiquement lorsque la stratégie AIX par défaut est restaurée avec le fichier `DoDv2_to_AIXDefault.xml`. Vous devez le changer manuellement. **Remarque :** Si votre système exécute le protocole IPv6, assurez-vous que le paramètre *ipv6_enabled* dans le fichier `/etc/security/pscexpert/ipv6.conf` a pour valeur `yes`. S'il n'utilise pas IPv6, assurez-vous que le paramètre *ipv6_enabled* a pour valeur `no`.
GEN005590	2	Le système ne doit pas exécuter de démon de protocole de routage sauf s'il s'agit d'un routeur.	**Emplacement** `/etc/security/pscexpert/dodv2/dodv2cmntrows` **Action de conformité** Garantit que le système satisfait les exigences spécifiées.
GEN005590	2	Le système ne doit pas exécuter de démon de protocole de routage sauf s'il s'agit d'un routeur.	**Emplacement** `/etc/security/pscexpert/dodv2/dodv2cmntrows` **Action de conformité** Garantit que le système satisfait les exigences spécifiées.
GEN005600	2	Le réacheminement IP pour IPv4 ne doit pas être activé sauf si le système est un routeur.	**Emplacement** `/etc/security/pscexpert/dodv2/ntwkoptsdod` **Action de conformité** Associe l'option de réseau `ipforwarding` à la valeur *0*.
GEN005610	2	Le réacheminement IP pour IPv6 ne doit pas être activé pour le système sauf si ce dernier est un routeur IPv6.	**Emplacement** `/etc/security/pscexpert/dodv2/ntwkoptsdod` **Action de conformité** Associe l'option de réseau `ip6forwarding` à la valeur *1*.
GEN005820	2	L'ID groupe et l'ID utilisateur anonyme du système NFS doivent être associés à des valeurs sans droit.	**Emplacement** `/etc/security/pscexpert/dodv2/nfsoptions` **Action de conformité** Garantit que les ID spécifiés ne disposent pas de droits.

Tableau 3. Exigences générales du département de la défense des Etats-Unis (suite)

ID de point de contrôle du guide STIG (Department of Defense Security Technical Implemen- tation Guide)	Catégorie de la règle du guide STIG (Department of Defense Security Technical Implemen- tation Guide)	Description	Emplacement du script dans lequel l'action est définie et résultats de l'action assurant la conformité
GEN005840	2	Le serveur NFS doit être configuré pour restreindre l'accès au système de fichiers aux hôtes locaux.	**Emplacement** `/etc/security/pscexpert/dodv2/nfsoptions` **Action de conformité** Configure le serveur NFS pour restreindre l'accès aux hôtes locaux.
GEN005880	2	Le serveur NFS ne doit pas autoriser l'accès root à distance.	**Emplacement** `/etc/security/pscexpert/dodv2/nfsoptions` **Action de conformité** Désactive l'accès root à distance sur le serveur NFS.
GEN005900	2	L'option *nosuid* doit être activée sur tous les montages de client NFS.	**Emplacement** `/etc/security/pscexpert/dodv2/nosuid` **Action de conformité** Active l'option *nosuid* sur tous les montages de client NFS.
GEN006060	2	Le système ne doit pas exécuter `Samba` sauf s'il est requis.	**Emplacement** `/etc/security/pscexpert/dodv2/dodv2services` **Action de conformité** Garantit que le système satisfait les exigences spécifiées.
GEN006380	1	Le système ne doit pas utiliser UDP pour NIS ou NIS+.	**Emplacement** `/etc/security/pscexpert/dodv2/dodv2cat1` **Action de conformité** Affiche les résultats des tests de règle spécifiés.
GEN006400	2	Le protocole Network Information System (NIS) ne doit pas être utilisé.	**Emplacement** `/etc/security/pscexpert/dodv2/nisplus` **Action de conformité** Désactive le protocole spécifié. **Remarque :** Ce paramètre n'est pas modifié automatiquement lorsque la stratégie AIX par défaut est restaurée avec le fichier `DoDv2_to_AIXDefault.xml`. Vous devez le changer manuellement.
GEN006420	2	Les mappes NIS doivent être protégées par des noms de domaine difficiles à deviner.	**Emplacement** `/etc/security/pscexpert/dodv2/nisplus` **Action de conformité** Garantit que les noms de domaine ne sont pas faciles à déterminer.

Tableau 3. Exigences générales du département de la défense des Etats-Unis (suite)

ID de point de contrôle du guide STIG (Department of Defense Security Technical Implemen- tation Guide)	Catégorie de la règle du guide STIG (Department of Defense Security Technical Implemen- tation Guide)	Description	Emplacement du script dans lequel l'action est définie et résultats de l'action assurant la conformité
GEN006460	2	Un serveur NIS+ doit s'exécuter avec le niveau de sécurité 2.	**Emplacement** `/etc/security/pscexpert/dodv2/nisplus` **Action de conformité** Garantit que le niveau de sécurité du serveur correspond au niveau de sécurité minimal spécifié. **Remarque :** Ce paramètre n'est pas modifié automatiquement lorsque la stratégie AIX par défaut est restaurée avec le fichier `DoDv2_to_AIXDefault.xml`. Vous devez le changer manuellement.
GEN006480	2	Les fichiers `setuid` non autorisés doivent être identifiés toutes les semaines sur le système, de même que la modification non autorisée des fichiers `setuid` autorisés.	**Emplacement** `/etc/security/pscexpert/dodv2/trust` **Action de conformité** Identifie toutes les semaines les modifications apportées aux fichiers spécifiés.
GEN006560	2	Les fichiers `setuid` non autorisés doivent être identifiés toutes les semaines sur le système, de même que la modification non autorisée des fichiers `setuid` autorisés.	**Emplacement** `/etc/security/pscexpert/dodv2/trust` **Action de conformité** Identifie toutes les semaines les modifications apportées aux fichiers spécifiés.
GEN006580	2	Le système doit utiliser un programme de contrôle d'accès.	**Emplacement** `/etc/security/pscexpert/dodv2/checktcpd` **Action de conformité** Garantit que le système satisfait les exigences spécifiées.
GEN006600	2	Le programme de contrôle d'accès du système doit journaliser chaque tentative d'accès au système.	**Emplacement** `/etc/security/pscexpert/dodv2/chsyslogdod` **Action de conformité** Garantit que les tentatives d'accès sont journalisées.
GEN006620	2	Le programme d'accès au système doit être configuré pour accorder ou refuser l'accès au système à des hôtes spécifiques.	**Emplacement** `/etc/security/pscexpert/dodv2/chetchostsdod` **Action de conformité** Configure les fichiers `hosts.deny` et `hosts.allow` avec les paramètres requis.
GEN007020	2	Le protocole SCTP (Stream Control Transmission Protocol) doit être désactivé.	**Emplacement** `/etc/security/pscexpert/dodv2/dodv2netrules` **Action de conformité** Désactive le protocole spécifié.

Tableau 3. Exigences générales du département de la défense des Etats-Unis (suite)

ID de point de contrôle du guide STIG (Department of Defense Security Technical Implemen- tation Guide)	Catégorie de la règle du guide STIG (Department of Defense Security Technical Implemen- tation Guide)	Description	Emplacement du script dans lequel l'action est définie et résultats de l'action assurant la conformité
GEN007700	2	Le gestionnaire de protocole IPv6 ne doit pas être lié à la pile réseau sauf si nécessaire.	**Emplacement** `/etc/security/pscexpert/dodv2/rminet6` **Action de conformité** Désactive le gestionnaire de protocole IPv6 depuis la pile réseau, sauf s'il est spécifié dans le fichier `/etc/ipv6.conf`. **Remarque :** Si votre système exécute le protocole IPv6, assurez-vous que le paramètre *ipv6_enabled* dans le fichier `/etc/security/pscexpert/ipv6.conf` a pour valeur `yes`. S'il n'utilise pas IPv6, assurez-vous que le paramètre *ipv6_enabled* a pour valeur `no`.
GEN007780	2	Aucun tunnel `6to4` ne doit être activé sur le système.	**Emplacement** `/etc/security/pscexpert/dodv2/rmiface` **Action de conformité** Désactive les tunnels spécifiés. **Remarque :** Ce paramètre n'est pas modifié automatiquement lorsque la stratégie AIX par défaut est restaurée avec le fichier `DoDv2_to_AIXDefault.xml`. Vous devez le changer manuellement.
GEN007820	2	Aucun tunnel IP ne doit être configuré sur le système.	**Emplacement** `/etc/security/pscexpert/dodv2/rmtunnel` **Action de conformité** Désactive les tunnels IP. **Remarque :** Ce paramètre n'est pas modifié automatiquement lorsque la stratégie AIX par défaut est restaurée avec le fichier `DoDv2_to_AIXDefault.xml`. Vous devez le changer manuellement.
GEN007840	2	Le client `DHCP` doit être désactivé s'il n'est pas utilisé.	**Emplacement** `/etc/security/pscexpert/dodv2/dodv2services` **Action de conformité** Garantit que le système satisfait les exigences spécifiées.
GEN007850	2	Le client `DHCP` ne doit pas envoyer de mises à jour DNS dynamiques.	**Emplacement** `/etc/security/pscexpert/dodv2/dodv2services` **Action de conformité** Garantit que le système satisfait les exigences spécifiées.

Tableau 3. Exigences générales du département de la défense des Etats-Unis (suite)

ID de point de contrôle du guide STIG (Department of Defense Security Technical Implemen- tation Guide)	Catégorie de la règle du guide STIG (Department of Defense Security Technical Implemen- tation Guide)	Description	Emplacement du script dans lequel l'action est définie et résultats de l'action assurant la conformité
GEN007860	2	Le système doit ignorer les messages de redirection ICMP IPv6.	**Emplacement** `/etc/security/pscexpert/dodv2/ntwkoptsdod` **Action de conformité** Associe l'option de réseau `ipignoreredirects` à la valeur *1*.
GEN007880	2	Le système ne doit pas envoyer de redirections ICMP IPv6.	**Emplacement** `/etc/security/pscexpert/dodv2/ntwkoptsdod` **Action de conformité** Associe la valeur *0* à l'option de réseau `ipsendredirects`.
GEN007900	2	Le système doit utiliser un filtre de chemin inverse approprié pour le trafic réseau IPv6, s'il utilise IPv6.	**Emplacement** `/etc/security/pscexpert/dodv2/chuserstanzadod` **Action de conformité** Garantit que le système satisfait les exigences spécifiées.
GEN007920	2	Le système ne doit pas transmettre de paquet IPv6 acheminé par la source.	**Emplacement** `/etc/security/pscexpert/dodv2/ntwkoptsdod` **Action de conformité** Associe l'option de réseau `ip6srcrouteforward` à la valeur *0*.
GEN007940: GEN003607	2	Le système ne doit pas accepter de paquet IPv4 ou IPv6 acheminé par la source.	**Emplacement** `/etc/security/pscexpert/dodv2/ntwkoptsdod` **Action de conformité** Associe l'option de réseau `ipsrcrouterecv` à la valeur *0*.
GEN007950	2	Le système ne doit pas répondre au demandes echo ICMPv6 qui sont envoyées à une adresse de diffusion.	**Emplacement** `/etc/security/pscexpert/dodv2/ntwkoptsdod` **Action de conformité** Associe l'option de réseau `bcastping` à la valeur *0*.
GEN008000	2	Si le système utilise Lightweight Directory Access Protocol (LDAP) pour les informations d'authentification ou de compte, les certificats qui sont utilisés pour l'authentification sur le serveur LDAP doivent être fournis depuis l'infrastructure PKI du département de la défense des Etats-Unis ou une méthode approuvée par le département de la défense des Etats-Unis.	**Emplacement** `/etc/security/pscexpert/dodv2/ldap_config` **Action de conformité** Garantit que le système satisfait les exigences spécifiées.
GEN008020	2	Si le système utilise LDAP pour les informations d'authentification ou de compte, la connexion LDAP TLS (Transport Layer Security) doit demander au serveur de fournir un certificat avec un chemin sécurisé valide.	**Emplacement** `/etc/security/pscexpert/dodv2/ldap_config` **Action de conformité** Garantit que le système satisfait les exigences spécifiées.

Tableau 3. Exigences générales du département de la défense des Etats-Unis (suite)

ID de point de contrôle du guide STIG (Department of Defense Security Technical Implemen- tation Guide)	Catégorie de la règle du guide STIG (Department of Defense Security Technical Implemen- tation Guide)	Description	Emplacement du script dans lequel l'action est définie et résultats de l'action assurant la conformité
GEN008050	2	Si le système utilise LDAP pour les informations d'authentification ou de compte, le fichier `/etc/ldap.conf` (ou un équivalent) ne doit pas contenir de mot de passe.	**Emplacement** `/etc/security/pscexpert/dodv2/ldap_config` **Action de conformité** Garantit que le système satisfait les exigences spécifiées.
GEN008380	2	Les fichiers `setuid` non autorisés doivent être identifiés toutes les semaines sur le système, de même que la modification non autorisée des fichiers `setuid` autorisés.	**Emplacement** `/etc/security/pscexpert/dodv2/trust` **Action de conformité** Identifie toutes les semaines les modifications apportées aux fichiers spécifiés.
GEN008520	2	Le système doit utiliser un pare-feu local qui protège l'hôte contre les analyses de port. Le pare-feu doit éviter les ports vulnérables pendant cinq minutes afin de protéger l'hôte contre les analyses de port.	**Emplacement** `/etc/security/pscexpert/dodv2/ipsecshunports` **Action de conformité** Garantit que le système satisfait les exigences spécifiées.
GEN008540	2	Le pare-feu local du système doit implémenter une stratégie *deny-all, allow-by-exception*.	**Emplacement** `/etc/security/pscexpert/dodv2/ipsecshunhosthls` **Action de conformité** Garantit que le système satisfait les exigences spécifiées. **Remarque :** Vous pouvez entrer des règles de filtrage supplémentaires dans le fichier `/etc/security/aixpert/bin/filter.txt`. Ces règles sont intégrées par le script `ipsecshunhosthls.sh` lorsque vous appliquez le profil. Le format des entrées doit être le suivant : *numéro_port*:*adresse_ip*:*action* où les valeurs possibles pour *action* sont `Allow` et `Deny`.
GEN008600	1	Le système doit être configuré pour démarrer uniquement à partir de la configuration d'amorçage du système.	**Emplacement** `/etc/security/pscexpert/dodv2/dodv2cat1` **Action de conformité** Garantit que le démarrage du système utilise la configuration d'amorçage du système seulement.
GEN008640	1	Le système ne doit pas utiliser de support amovible comme chargeur d'amorçage.	**Emplacement** `/etc/security/pscexpert/dodv2/dodv2cat1` **Action de conformité** Garantit que le système n'est pas amorcé depuis une unité amovible.

Tableau 3. Exigences générales du département de la défense des Etats-Unis (suite)

ID de point de contrôle du guide STIG (Department of Defense Security Technical Implemen- tation Guide)	Catégorie de la règle du guide STIG (Department of Defense Security Technical Implemen- tation Guide)	Description	Emplacement du script dans lequel l'action est définie et résultats de l'action assurant la conformité
GEN009140	1,2,3	Le service `chargen` ne doit pas être actif sur le système.	**Emplacement** `/etc/security/pscexpert/dodv2/inetdservices` **Action de conformité** Désactive les démons et les services requis en mettant en commentaire les entrées dans le fichier `/etc/inetd.conf`.
GEN009160	1,2,3	Le service `Calendar Management Service Daemon` (CMSD) ne doit pas être actif sur le système.	**Emplacement** `/etc/security/pscexpert/dodv2/inetdservices` **Action de conformité** Désactive les démons et les services requis en mettant en commentaire les entrées dans le fichier `/etc/inetd.conf`.
GEN009180	1,2,3	Le service `tool-talk database server` (ttdbserver) ne doit pas être actif sur le système.	**Emplacement** `/etc/security/pscexpert/dodv2/inetdservices` **Action de conformité** Désactive les démons et les services requis en mettant en commentaire les entrées dans le fichier `/etc/inetd.conf`.
GEN009190	1,2,3	Le service `comsat` ne doit pas être actif sur le système.	**Emplacement** `/etc/security/pscexpert/dodv2/inetdservices` **Action de conformité** Désactive les démons et les services requis en mettant en commentaire les entrées dans le fichier `/etc/inetd.conf`.
GEN009200-9330	1,2,3	Aucun autre service ou démon ne peut être actif sur le système.	**Emplacement** `/etc/security/pscexpert/dodv2/inetdservices` **Action de conformité** Désactive les démons et les services requis en mettant en commentaire les entrées dans le fichier `/etc/inetd.conf`.
GEN009210	2	Le service `discard` ne doit pas être actif sur le système.	**Emplacement** `/etc/security/pscexpert/dodv2/inetdservices` **Action de conformité** Désactive les démons et les services requis en mettant en commentaire les entrées dans le fichier `/etc/inetd.conf`.

Tableau 3. Exigences générales du département de la défense des Etats-Unis (suite)

ID de point de contrôle du guide STIG (Department of Defense Security Technical Implemen- tation Guide)	Catégorie de la règle du guide STIG (Department of Defense Security Technical Implemen- tation Guide)	Description	Emplacement du script dans lequel l'action est définie et résultats de l'action assurant la conformité
GEN009220	2	Le service `dtspc` ne doit pas être actif sur le système.	**Emplacement** `/etc/security/pscexpert/dodv2/inetdservices` **Action de conformité** Désactive les démons et les services requis en mettant en commentaire les entrées dans le fichier `/etc/inetd.conf`.
GEN009230	2	Le service `echo` ne doit pas être actif sur le système.	**Emplacement** `/etc/security/pscexpert/dodv2/inetdservices` **Action de conformité** Désactive les démons et les services requis en mettant en commentaire les entrées dans le fichier `/etc/inetd.conf`.
GEN009240	2	Le service `Internet Message Access Protocol (IMAP)` ne doit pas être actif sur le système.	**Emplacement** `/etc/security/pscexpert/dodv2/inetdservices` **Action de conformité** Désactive les démons et les services requis en mettant en commentaire les entrées dans le fichier `/etc/inetd.conf`.
GEN009250	2	Le service `PostOffice Protocol (POP3)` ne doit pas être actif sur le système.	**Emplacement** `/etc/security/pscexpert/dodv2/inetdservices` **Action de conformité** Désactive les démons et les services requis en mettant en commentaire les entrées dans le fichier `/etc/inetd.conf`.
GEN009260	2	Les services talk et `ntalk` ne doivent pas être actifs sur le système.	**Emplacement** `/etc/security/pscexpert/dodv2/inetdservices` **Action de conformité** Désactive les démons et les services requis en mettant en commentaire les entrées dans le fichier `/etc/inetd.conf`.
GEN009270	2	Le service `netstat` ne doit pas être actif sur le processus InetD du système.	**Emplacement** `/etc/security/pscexpert/dodv2/inetdservices` **Action de conformité** Désactive les démons et les services requis en mettant en commentaire les entrées dans le fichier `/etc/inetd.conf`.

Tableau 3. Exigences générales du département de la défense des Etats-Unis (suite)

ID de point de contrôle du guide STIG (Department of Defense Security Technical Implemen- tation Guide)	Catégorie de la règle du guide STIG (Department of Defense Security Technical Implemen- tation Guide)	Description	Emplacement du script dans lequel l'action est définie et résultats de l'action assurant la conformité
GEN009280	2	Le service `PCNFS` ne doit pas être actif sur le système.	**Emplacement** `/etc/security/pscexpert/dodv2/inetdservices` **Action de conformité** Désactive les démons et les services requis en mettant en commentaire les entrées dans le fichier `/etc/inetd.conf`.
GEN009290	2	Le service `systat` ne doit pas être actif sur le système.	**Emplacement** `/etc/security/pscexpert/dodv2/inetdservices` **Action de conformité** Désactive les démons et les services requis en mettant en commentaire les entrées dans le fichier `/etc/inetd.conf`.
GEN009300	2	Le service `inetd time` ne doit pas être actif sur le système sur le démon `inetd`.	**Emplacement** `/etc/security/pscexpert/dodv2/inetdservices` **Action de conformité** Désactive les démons et les services requis en mettant en commentaire les entrées dans le fichier `/etc/inetd.conf`.
GEN009310	2	Le service `rusersd` ne doit pas être actif sur le système.	**Emplacement** `/etc/security/pscexpert/dodv2/inetdservices` **Action de conformité** Désactive les démons et les services requis en mettant en commentaire les entrées dans le fichier `/etc/inetd.conf`.
GEN009320	2	Le service `sprayd` ne doit pas être actif sur le système.	**Emplacement** `/etc/security/pscexpert/dodv2/inetdservices` **Action de conformité** Désactive les démons et les services requis en mettant en commentaire les entrées dans le fichier `/etc/inetd.conf`.
GEN009330	2	Le service `rstatd` ne doit pas être actif sur le système.	**Emplacement** `/etc/security/pscexpert/dodv2/inetdservices` **Action de conformité** Désactive les démons et les services requis en mettant en commentaire les entrées dans le fichier `/etc/inetd.conf`.

Tableau 3. Exigences générales du département de la défense des Etats-Unis (suite)

ID de point de contrôle du guide STIG (Department of Defense Security Technical Implemen- tation Guide)	Catégorie de la règle du guide STIG (Department of Defense Security Technical Implemen- tation Guide)	Description	Emplacement du script dans lequel l'action est définie et résultats de l'action assurant la conformité
GEN009340	2	Les gestionnaires de connexion du serveur X ne doivent pas être exécutés sauf s'ils sont nécessaires pour la gestion des sessions X11.	**Emplacement** `/etc/security/pscexpert/dodv2/ dodv2cmntrows` **Action de conformité** Cette règle désactive les connexions du système X Window et le gestionnaire de connexion du serveur X.

Tableau 4. Exigences de propriété du département de la défense des Etats-Unis

ID de point de contrôle du guide STIG (Department of Defense Security Technical Implementation Guide)	Description	Emplacement du script dans lequel l'action est définie et résultats de l'action assurant la conformité
AIX00085	Le fichier `/etc/netsvc.conf` doit appartenir à root.	**Emplacement** `/etc/security/pscexpert/dodv2/ chowndodfiles` **Action de conformité** Garantit que le fichier spécifié appartient à root.
AIX00090	Le fichier `/etc/netsvc.conf` doit appartenir à un groupe tel que bin, sys ou system.	**Emplacement** `/etc/security/pscexpert/dodv2/ chowndodfiles` **Action de conformité** Garantit que le fichier spécifié appartient au groupe bin, sys ou system.
AIX00320	Le fichier `/etc/ftpaccess.ctl` doit appartenir à root.	**Emplacement** `/etc/security/pscexpert/dodv2/ chowndodfiles` **Action de conformité** Garantit que le fichier spécifié appartient à root.
AIX00330	Le fichier `/etc/ftpaccess.ctl` doit appartenir à un groupe tel que bin, sys ou system.	**Emplacement** `/etc/security/pscexpert/dodv2/ chowndodfiles` **Action de conformité** Garantit que le fichier spécifié appartient au groupe bin, sys ou system.
GEN000250	Le fichier de configuration de la synchronisation de l'heure (par exemple `/etc/ntp.conf`) doit appartenir à root.	**Emplacement** `/etc/security/pscexpert/dodv2/ chowndodfiles` **Action de conformité** Garantit que le fichier spécifié appartient à root.

Tableau 4. Exigences de propriété du département de la défense des Etats-Unis (suite)

ID de point de contrôle du guide STIG (Department of Defense Security Technical Implementation Guide)	Description	Emplacement du script dans lequel l'action est définie et résultats de l'action assurant la conformité
GEN000251	Le fichier de configuration de la synchronisation de l'heure (par exemple `/etc/ntp.conf`) doit appartenir à un groupe tel que bin, sys ou system.	**Emplacement** `/etc/security/pscexpert/dodv2/chowndodfiles` **Action de conformité** Garantit que le fichier spécifié appartient au groupe bin, sys ou system.
GEN001160	Tous les fichiers et répertoires doivent avoir un propriétaire valide.	**Emplacement** `/etc/security/pscexpert/dodv2/chowndodfiles` **Action de conformité** Garantit que tous les fichiers et répertoires ont un propriétaire valide.
GEN001170	Tous les fichiers et répertoires doivent avoir un propriétaire de groupe valide.	**Emplacement** `/etc/security/pscexpert/dodv2/chowndodfiles` **Action de conformité** Garantit que tous les fichiers et répertoires ont un propriétaire valide.
GEN001220	Tous les fichiers, programmes et répertoires système doivent appartenir à un compte système.	**Emplacement** `/etc/security/pscexpert/dodv2/chowndodfiles` **Action de conformité** Garantit que les fichiers, programmes et répertoires système appartiennent à un compte système.
GEN001240	Les fichiers, programmes et répertoires système doivent appartenir à un groupe système.	**Emplacement** `/etc/security/pscexpert/dodv2/chowndodfiles` **Action de conformité** Tous les fichiers, programmes et répertoires système doivent appartenir à un groupe système.
GEN001320	Les fichiers Network Information Systems (NIS)/NIS+/yp doivent appartenir à root, sys ou bin.	**Emplacement** `/etc/security/pscexpert/dodv2/chowndodfiles` **Action de conformité** Garantit que les fichiers spécifiés appartiennent à root, sys ou bin.
GEN001340	Les fichiers NIS/NIS+/yp doivent appartenir à un groupe tel que sys, bin, other ou system.	**Emplacement** `/etc/security/pscexpert/dodv2/chowndodfiles` **Action de conformité** Garantit que les fichiers spécifiés appartiennent à sys, bin, other ou system.

Tableau 4. Exigences de propriété du département de la défense des Etats-Unis (suite)

ID de point de contrôle du guide STIG (Department of Defense Security Technical Implementation Guide)	Description	Emplacement du script dans lequel l'action est définie et résultats de l'action assurant la conformité
GEN001362	Le fichier `/etc/resolv.conf` doit appartenir à root.	**Emplacement** `/etc/security/pscexpert/dodv2/chowndodfiles` **Action de conformité** Garantit que le fichier spécifié appartient à root.
GEN001363	Le fichier `/etc/resolv.conf` doit appartenir à un groupe tel que bin, sys ou system.	**Emplacement** `/etc/security/pscexpert/dodv2/chowndodfiles` **Action de conformité** Garantit que le fichier spécifié appartient au groupe bin, sys ou system.
GEN001366	Le fichier `/etc/hosts` doit appartenir à root.	**Emplacement** `/etc/security/pscexpert/dodv2/chowndodfiles` **Action de conformité** Garantit que le fichier spécifié appartient à root.
GEN001367	Le fichier `/etc/hosts` doit appartenir à un groupe tel que bin, sys ou system.	**Emplacement** `/etc/security/pscexpert/dodv2/chowndodfiles` **Action de conformité** Garantit que le fichier spécifié appartient au groupe bin, sys ou system.
GEN001371	Le fichier `/etc/nsswitch.conf` doit appartenir à root.	**Emplacement** `/etc/security/pscexpert/dodv2/chowndodfiles` **Action de conformité** Garantit que le fichier spécifié appartient à root.
GEN001372	Le fichier `/etc/nsswitch.conf` doit appartenir à un groupe tel que root, bin, sys ou system.	**Emplacement** `/etc/security/pscexpert/dodv2/chowndodfiles` **Action de conformité** Garantit que le fichier spécifié appartient au groupe root, bin, sys ou system.
GEN001378	Le fichier `/etc/passwd` doit appartenir à root.	**Emplacement** `/etc/security/pscexpert/dodv2/chowndodfiles` **Action de conformité** Garantit que le fichier spécifié appartient à root.

Tableau 4. Exigences de propriété du département de la défense des Etats-Unis (suite)

ID de point de contrôle du guide STIG (Department of Defense Security Technical Implementation Guide)	Description	Emplacement du script dans lequel l'action est définie et résultats de l'action assurant la conformité
GEN001379	Le fichier `/etc/passwd` doit appartenir à un groupe tel que bin, security, sys ou system.	**Emplacement** `/etc/security/pscexpert/dodv2/chowndodfiles` **Action de conformité** Garantit que le fichier spécifié appartient au groupe bin, security, sys ou system.
GEN001391	Le fichier `/etc/group` doit appartenir à root.	**Emplacement** `/etc/security/pscexpert/dodv2/chowndodfiles` **Action de conformité** Garantit que le fichier spécifié appartient à root.
GEN001392	Le fichier `/etc/group` doit appartenir à un groupe tel que bin, security, sys ou system.	**Emplacement** `/etc/security/pscexpert/dodv2/chowndodfiles` **Action de conformité** Garantit que le fichier spécifié appartient au groupe bin, security, sys ou system.
GEN001400	Le fichier `/etc/security/passwd` doit appartenir à root.	**Emplacement** `/etc/security/pscexpert/dodv2/chowndodfiles` **Action de conformité** Garantit que le fichier spécifié appartient à root.
GEN001410	Le fichier `/etc/security/passwd` doit appartenir à un groupe tel que bin, security, sys ou system.	**Emplacement** `/etc/security/pscexpert/dodv2/chowndodfiles` **Action de conformité** Garantit que le fichier spécifié appartient au groupe bin, security, sys ou system.
GEN001500	Tous les répertoires de base des utilisateurs interactifs doivent appartenir à leurs utilisateurs respectifs.	**Emplacement** `/etc/security/pscexpert/dodv2/chowndodfiles` **Action de conformité** Garantit que tous les répertoires de base des utilisateurs interactifs appartiennent à leurs utilisateurs respectifs.
GEN001520	Tous les répertoires de base des utilisateurs interactifs doivent appartenir au groupe principal du propriétaire du répertoire de base.	**Emplacement** `/etc/security/pscexpert/dodv2/chowndodfiles` **Action de conformité** Garantit que tous les répertoires de base des utilisateurs interactifs appartiennent au groupe principal du propriétaire du répertoire de base.

Tableau 4. Exigences de propriété du département de la défense des Etats-Unis (suite)

ID de point de contrôle du guide STIG (Department of Defense Security Technical Implementation Guide)	Description	Emplacement du script dans lequel l'action est définie et résultats de l'action assurant la conformité
GEN001540	Tous les fichiers et répertoires qui se trouvent dans les répertoires de base de l'utilisateur interactif doivent appartenir au propriétaire du répertoire de base.	**Emplacement** `/etc/security/pscexpert/dodv2/chowndodfiles` **Action de conformité** Garantit que tous les fichiers et répertoires qui se trouvent dans les répertoires de base de l'utilisateur interactif appartiennent au propriétaire du répertoire de base.
GEN001550	Tous les fichiers et répertoires qui se trouvent dans les répertoires de base de l'utilisateur doivent appartenir à un groupe duquel le propriétaire du répertoire de base est membre.	**Emplacement** `/etc/security/pscexpert/dodv2/chowndodfiles` **Action de conformité** Garantit que tous les fichiers et répertoires qui se trouvent dans les répertoires de base de l'utilisateur appartiennent à un groupe duquel le propriétaire du répertoire de base est membre.
GEN001660	Tous les fichiers de démarrage système doivent appartenir à root.	**Emplacement** `/etc/security/pscexpert/dodv2/chowndodfiles` **Action de conformité** Garantit que les fichiers spécifiés appartiennent à root.
GEN001680	Tous les fichiers de démarrage système doivent appartenir à un groupe tel que sys, bin, other ou system.	**Emplacement** `/etc/security/pscexpert/dodv2/chowndodfiles` **Action de conformité** Garantit que les fichiers spécifiés appartiennent au groupe sys, bin, other ou system.
GEN001740	Tous les fichiers d'initialisation globaux doivent appartenir à root.	**Emplacement** `/etc/security/pscexpert/dodv2/chowndodfiles` **Action de conformité** Garantit que les fichiers spécifiés appartiennent à root.
GEN001760	Tous les fichiers d'initialisation globaux doivent appartenir à un groupe tel que sys, bin, system ou security.	**Emplacement** `/etc/security/pscexpert/dodv2/chowndodfiles` **Action de conformité** Garantit que les fichiers spécifiés appartiennent au groupe sys, bin, system ou security.

Tableau 4. Exigences de propriété du département de la défense des Etats-Unis (suite)

ID de point de contrôle du guide STIG (Department of Defense Security Technical Implementation Guide)	Description	Emplacement du script dans lequel l'action est définie et résultats de l'action assurant la conformité
GEN001820	Les répertoires et les fichiers modèle (en général dans `/etc/skel`) doivent appartenir à root ou bin.	**Emplacement** `/etc/security/pscexpert/dodv2/chowndodfiles` **Action de conformité** Garantit que les fichiers et répertoires spécifiés appartiennent à root ou bin.
GEN001830	Tous les fichiers modèle (en général dans `/etc/skel`) doivent appartenir au groupe security.	**Emplacement** `/etc/security/pscexpert/dodv2/chowndodfiles` **Action de conformité** Garantit que les fichiers spécifiés appartiennent au groupe security.
GEN001860	Tous les fichiers d'initialisation locaux doivent appartenir à l'utilisateur ou à root.	**Emplacement** `/etc/security/pscexpert/dodv2/chowndodfiles` **Action de conformité** Garantit que les fichiers spécifiés appartiennent à l'utilisateur ou à root.
GEN001870	Les fichiers d'initialisation locaux doit appartenir au groupe principal de l'utilisateur ou à root.	**Emplacement** `/etc/security/pscexpert/dodv2/chowndodfiles` **Action de conformité** Garantit que les fichiers d'initialisation locaux appartiennent au groupe principal de l'utilisateur ou à root.

GEN002060	Tous les fichiers `.rhosts`, `.shosts`, `.netrc` et `hosts.equiv` ne doivent être accessibles que par root ou le propriétaire.	**Emplacement**
		`/etc/security/pscexpert/dodv2/chowndodfiles`
		`/etc/security/pscexpert/dodv2/fpmdodfiles`
		Action de conformité
		Garantit que root ou le propriétaire seulement peuvent accéder aux fichiers spécifiés.

GEN002100	Le fichier `.rhosts` ne doit pas être pris en charge par le module PAM (Pluggable Authentication Module).	**Emplacement** `/etc/security/pscexpert/dodv2/chowndodfiles` **Action de conformité** Garantit que le fichier spécifié n'est pas disponible via PAM.
GEN002200	Tous les fichiers shell doivent appartenir à root ou bin.	**Emplacement** `/etc/security/pscexpert/dodv2/chowndodfiles` **Action de conformité** Garantit que les fichiers spécifiés appartiennent à root ou bin.

Tableau 4. Exigences de propriété du département de la défense des Etats-Unis (suite)

ID de point de contrôle du guide STIG (Department of Defense Security Technical Implementation Guide)	Description	Emplacement du script dans lequel l'action est définie et résultats de l'action assurant la conformité
GEN002210	Tous les fichiers shell doivent appartenir à un groupe tel que root, bin, sys ou system.	**Emplacement** `/etc/security/pscexpert/dodv2/chowndodfiles` **Action de conformité** Garantit que les fichiers spécifiés appartiennent au groupe root, bin, sys ou system.
GEN002340	Le périphériques audio doivent appartenir à root.	**Emplacement** `/etc/security/pscexpert/dodv2/chowndodfiles` **Action de conformité** Garantit que tous les périphériques audio appartiennent à root.
GEN002360	Les périphériques audio doivent appartenir à un groupe tel que root, sys, bin ou system.	**Emplacement** `/etc/security/pscexpert/dodv2/chowndodfiles` **Action de conformité** Garantit que tous les périphériques audio appartiennent au groupe root, sys, bin ou system.
GEN002520	Tous les répertoires publics doivent appartenir à root ou à un compte de type application.	**Emplacement** `/etc/security/pscexpert/dodv2/chowndodfiles` **Action de conformité** Garantit que tous les répertoires publics appartiennent à root ou à un compte de type application.
GEN002540	Tous les répertoires publics doivent appartenir à un groupe tel que system ou à un groupe de type application.	**Emplacement** `/etc/security/pscexpert/dodv2/chowndodfiles` **Action de conformité** Garantit que tous les répertoires publics appartiennent au groupe system ou à un groupe de type application.
GEN002680	Les journaux d'audit du système doivent appartenir à root.	**Emplacement** `/etc/security/pscexpert/dodv2/chowndodfiles` **Action de conformité** Garantit que les fichiers spécifiés appartiennent à root.
GEN002690	Les journaux d'audit du système doivent appartenir à un groupe tel que bin, sys ou system.	**Emplacement** `/etc/security/pscexpert/dodv2/chowndodfiles` **Action de conformité** Garantit que les fichiers spécifiés appartiennent au groupe bin, sys ou system.

Tableau 4. Exigences de propriété du département de la défense des Etats-Unis (suite)

ID de point de contrôle du guide STIG (Department of Defense Security Technical Implementation Guide)	Description	Emplacement du script dans lequel l'action est définie et résultats de l'action assurant la conformité
GEN003020	`Cron` ne doit pas exécuter de programmes qui se trouvent dans des répertoires accessibles en écriture par tout le monde, ou qui y sont subordonnés.	**Emplacement** `/etc/security/pscexpert/dodv2/chowndodfiles` **Action de conformité** Empêche `cron` d'exécuter des programmes dans des répertoires accessibles en écriture par tout le monde, ou qui y sont subordonnés.
GEN003040	Les fichiers `crontab` doit appartenir à root ou au créateur du fichier crontab.	**Emplacement** `/etc/security/pscexpert/dodv2/chowndodfiles` **Action de conformité** Garantit que les fichiers crontab appartiennent à root ou au créateur du fichier crontab.
GEN003050	Les fichiers `crontab` doivent appartenir à un groupe tel que system, cron ou le groupe principal du créateur du fichier crontab.	**Emplacement** `/etc/security/pscexpert/dodv2/chowndodfiles` **Action de conformité** Garantit que les fichiers `crontab` appartiennent au groupe system ou cron ou au groupe principal du créateur du fichier crontab.
GEN003110	Les répertoires `cron` et `crontab` ne doivent pas comporter de listes de contrôle d'accès étendues.	**Emplacement** `/etc/security/pscexpert/dodv2/chowndodfiles` **Action de conformité** Garantit que les répertoires spécifiés ne comportent pas de listes de contrôle d'accès étendues.
GEN003120	Les répertoires `cron` et `crontab` doivent appartenir à root ou bin.	**Emplacement** `/etc/security/pscexpert/dodv2/chowndodfiles` **Action de conformité** Garantit que les répertoires cron et crontab appartiennent à root ou bin.
GEN003140	Les répertoires `cron` et `crontab` doivent appartenir à un groupe tel que system, sys, bin ou cron.	**Emplacement** `/etc/security/pscexpert/dodv2/chowndodfiles` **Action de conformité** Garantit que les répertoires spécifiés appartiennent au groupe system, sys, bin ou cron.
GEN003160	La journalisation cron doit être implémentée.	**Emplacement** `/etc/security/pscexpert/dodv2/chowndodfiles` **Action de conformité** Garantit que la journalisation cron est implémentée.

Tableau 4. Exigences de propriété du département de la défense des Etats-Unis (suite)

ID de point de contrôle du guide STIG (Department of Defense Security Technical Implementation Guide)	Description	Emplacement du script dans lequel l'action est définie et résultats de l'action assurant la conformité
GEN003240	Le fichier `cron.allow` doit appartenir à root, bin ou sys.	**Emplacement** `/etc/security/pscexpert/dodv2/chowndodfiles` **Action de conformité** Garantit que le fichier spécifié appartient à root, bin ou sys.
GEN003250	Le fichier `cron.allow` doit appartenir à un groupe tel que system, bin, sys ou cron.	**Emplacement** `/etc/security/pscexpert/dodv2/chowndodfiles` **Action de conformité** Garantit que le fichier spécifié appartient au groupe system, bin, sys ou cron.
GEN003260	Le fichier `cron.deny` doit appartenir à root, bin ou sys.	**Emplacement** `/etc/security/pscexpert/dodv2/chowndodfiles` **Action de conformité** Garantit que le fichier spécifié appartient à root, bin ou sys.
GEN003270	Le fichier `cron.deny` doit appartenir à un groupe tel que system, bin, sys ou cron.	**Emplacement** `/etc/security/pscexpert/dodv2/chowndodfiles` **Action de conformité** Garantit que le fichier spécifié appartient au groupe system, bin, sys ou cron.
GEN003420	Le répertoire `at` doit appartenir à root, bin, daemon ou cron.	**Emplacement** `/etc/security/pscexpert/dodv2/chowndodfiles` **Action de conformité** Garantit que le répertoire spécifié appartient à root, sys, daemon ou cron.
GEN003430	Le répertoire `at` doit appartenir à un groupe tel que system, bin, sys ou cron.	**Emplacement** `/etc/security/pscexpert/dodv2/chowndodfiles` **Action de conformité** Garantit que le répertoire spécifié appartient au groupe system, bin, sys ou cron.
GEN003460	Le fichier `at.allow` doit appartenir à root, bin ou sys.	**Emplacement** `/etc/security/pscexpert/dodv2/chowndodfiles` **Action de conformité** Garantit que le fichier spécifié appartient à root, bin ou sys.

Tableau 4. Exigences de propriété du département de la défense des Etats-Unis (suite)

ID de point de contrôle du guide STIG (Department of Defense Security Technical Implementation Guide)	Description	Emplacement du script dans lequel l'action est définie et résultats de l'action assurant la conformité
GEN003470	Le fichier `at.allow` doit appartenir à un groupe tel que system, bin, sys ou cron.	**Emplacement** `/etc/security/pscexpert/dodv2/chowndodfiles` **Action de conformité** Garantit que le fichier spécifié appartient au groupe system, bin, sys ou cron.
GEN003480	Le fichier `at.deny` doit appartenir à root, bin ou sys.	**Emplacement** `/etc/security/pscexpert/dodv2/chowndodfiles` **Action de conformité** Garantit que le fichier spécifié appartient à root, bin ou sys.
GEN003490	Le fichier `at.deny` doit appartenir à un groupe tel que system, bin, sys ou cron.	**Emplacement** `/etc/security/pscexpert/dodv2/chowndodfiles` **Action de conformité** Garantit que le fichier spécifié appartient au groupe system, bin, sys ou cron.
GEN003720	Le fichier `inetd.conf`, le fichier `xinetd.conf` et le répertoire `xinetd.d` doivent appartenir à root ou bin.	**Emplacement** `/etc/security/pscexpert/dodv2/chowndodfiles` **Action de conformité** Garantit que les fichiers et le répertoire spécifiés appartiennent à root ou bin.
GEN003730	Le fichier `inetd.conf`, le fichier `xinetd.conf` et le répertoire `xinetd.d` doivent appartenir à un groupe tel que bin, sys ou system.	**Emplacement** `/etc/security/pscexpert/dodv2/chowndodfiles` **Action de conformité** Garantit que les fichiers et le répertoire spécifiés appartiennent au groupe bin, sys ou system.
GEN003760	Le fichier `services` doit appartenir à root ou bin.	**Emplacement** `/etc/security/pscexpert/dodv2/chowndodfiles` **Action de conformité** Garantit que le fichier spécifié appartient à root ou bin.
GEN003770	Le fichier `services` doit appartenir à un groupe tel que bin, sys ou system.	**Emplacement** `/etc/security/pscexpert/dodv2/chowndodfiles` **Action de conformité** Garantit que le fichier spécifié appartient au groupe bin, sys ou system.

Tableau 4. Exigences de propriété du département de la défense des Etats-Unis (suite)

ID de point de contrôle du guide STIG (Department of Defense Security Technical Implementation Guide)	Description	Emplacement du script dans lequel l'action est définie et résultats de l'action assurant la conformité
GEN003920	Le fichier `hosts.lpd` (ou un équivalent) doit appartenir à root, bin, sys ou lp.	**Emplacement** `/etc/security/pscexpert/dodv2/chowndodfiles` **Action de conformité** Garantit que le fichier spécifié appartient à root, bin, sys ou lp.
GEN003930	Le fichier `hosts.lpd` (ou un équivalent) doit appartenir à un groupe tel que bin, sys ou system.	**Emplacement** `/etc/security/pscexpert/dodv2/chowndodfiles` **Action de conformité** Garantit que le fichier spécifié appartient au groupe bin, sys ou system.
GEN003960	Le propriétaire de la commande **traceroute** doit être root.	**Emplacement** `/etc/security/pscexpert/dodv2/chowndodfiles` **Action de conformité** Garantit que le propriétaire de la commande est root.
GEN003980	La commande **traceroute** doit appartenir à un groupe tel que sys, bin ou system.	**Emplacement** `/etc/security/pscexpert/dodv2/chowndodfiles` **Action de conformité** Garantit que la commande appartient au groupe sys, bin ou system.
GEN004360	Le fichier `alias` doit appartenir à root.	**Emplacement** `/etc/security/pscexpert/dodv2/chowndodfiles` **Action de conformité** Garantit que le fichier spécifié appartient à root.
GEN004370	Le fichier `aliases` doit appartenir à un groupe tel que sys, bin ou system.	**Emplacement** `/etc/security/pscexpert/dodv2/chowndodfiles` **Action de conformité** Garantit que le fichier spécifié appartient au groupe sys, bin ou system.
GEN004400	Les fichiers qui sont exécutés par le biais d'un fichier `aliases` de courrier doivent appartenir à root et se trouver dans un répertoire qui appartient à root et pour lequel seul root dispose du droit d'accès en écriture.	**Emplacement** `/etc/security/pscexpert/dodv2/chowndodfiles` **Action de conformité** Garantit que les fichiers qui sont exécutés par le biais d'un fichier `aliases` de courrier appartiennent à root et se trouvent dans un répertoire qui appartient à root et pour lequel seul root dispose du droit d'accès en écriture.

Tableau 4. Exigences de propriété du département de la défense des Etats-Unis (suite)

ID de point de contrôle du guide STIG (Department of Defense Security Technical Implementation Guide)	Description	Emplacement du script dans lequel l'action est définie et résultats de l'action assurant la conformité
GEN004410	Les fichiers qui sont exécutés par le biais d'un fichier `aliases` de courrier doivent appartenir à un groupe tel que root, bin, sys ou other. Ils doivent également se trouver dans un répertoire qui appartient à un groupe tel que root, bin, sys ou other.	**Emplacement** `/etc/security/pscexpert/dodv2/chowndodfiles` **Action de conformité** Garantit que les fichiers qui sont exécutés par le biais d'un fichier `aliases` de courrier appartiennent au groupe root, bin, sys ou other et se trouvent dans un répertoire qui appartient au groupe root, bin, sys ou other.
GEN004480	Le fichier journal du service SMTP doit appartenir à root.	**Emplacement** `/etc/security/pscexpert/dodv2/chowndodfiles` **Action de conformité** Garantit que le fichier spécifié appartient à root.
GEN004920	Le fichier `ftpusers` doit appartenir à root.	**Emplacement** `/etc/security/pscexpert/dodv2/chowndodfiles` **Action de conformité** Garantit que le fichier spécifié appartient à root.
GEN004930	Le fichier `ftpusers` doit appartenir à un groupe tel que bin, sys ou system.	**Emplacement** `/etc/security/pscexpert/dodv2/chowndodfiles` **Action de conformité** Garantit que le fichier spécifié appartient au groupe bin, sys ou system.
GEN005360	Le fichier `snmpd.conf` doit appartenir à root.	**Emplacement** `/etc/security/pscexpert/dodv2/chowndodfiles` **Action de conformité** Garantit que le fichier spécifié appartient à root.
GEN005365	Le fichier `snmpd.conf` doit appartenir à un groupe tel que bin, sys ou system.	**Emplacement** `/etc/security/pscexpert/dodv2/chowndodfiles` **Action de conformité** Garantit que le fichier spécifié appartient au groupe bin, sys ou system.
GEN005400	Le fichier `/etc/syslog.conf` doit appartenir à root.	**Emplacement** `/etc/security/pscexpert/dodv2/chowndodfiles` **Action de conformité** Garantit que le fichier spécifié appartient à root.

Tableau 4. Exigences de propriété du département de la défense des Etats-Unis (suite)

ID de point de contrôle du guide STIG (Department of Defense Security Technical Implementation Guide)	Description	Emplacement du script dans lequel l'action est définie et résultats de l'action assurant la conformité
GEN005420	Le fichier `/etc/syslog.conf` doit appartenir à un groupe tel que bin, sys ou system.	**Emplacement** `/etc/security/pscexpert/dodv2/chowndodfiles` **Action de conformité** Garantit que le fichier spécifié appartient au groupe bin, sys ou system.
GEN005610	Le réacheminement IP pour IPv6 ne doit pas être activé pour le système sauf si ce dernier est un routeur IPv6.	**Emplacement** `/etc/security/pscexpert/dodv2/chowndodfiles` **Action de conformité** Garantit que le réacheminement IP pour IPv6 n'est pas activé sauf si le système est utilisé comme routeur IPv6.
GEN005740	Le fichier de configuration de l'exportation NFS doit appartenir à root.	**Emplacement** `/etc/security/pscexpert/dodv2/chowndodfiles` **Action de conformité** Garantit que le fichier spécifié appartient à root.
GEN005750	Le fichier de configuration de l'exportation NFS doit appartenir à un groupe tel que root, bin, sys ou system.	**Emplacement** `/etc/security/pscexpert/dodv2/chowndodfiles` **Action de conformité** Garantit que le fichier spécifié appartient au groupe root, bin, sys ou system.
GEN005800	Tous les fichiers et répertoires système exportés par NFS doivent appartenir à root.	**Emplacement** `/etc/security/pscexpert/dodv2/chowndodfiles` **Action de conformité** Garantit que le fichier spécifié appartient à root.
GEN005810	Tous les fichiers et répertoires système exportés par NFS doivent appartenir à un groupe tel que root, bin, sys ou system.	**Emplacement** `/etc/security/pscexpert/dodv2/chowndodfiles` **Action de conformité** Garantit que les fichiers et répertoires spécifiés appartiennent au groupe root, bin, sys ou system.
GEN006100	Le fichier `/usr/lib/smb.conf` doit appartenir à root.	**Emplacement** `/etc/security/pscexpert/dodv2/chowndodfiles` **Action de conformité** Garantit que le fichier spécifié appartient à root.

Tableau 4. Exigences de propriété du département de la défense des Etats-Unis (suite)

ID de point de contrôle du guide STIG (Department of Defense Security Technical Implementation Guide)	Description	Emplacement du script dans lequel l'action est définie et résultats de l'action assurant la conformité
GEN006120	Le fichier `/usr/lib/smb.conf` doit appartenir à un groupe tel que bin, sys ou system.	**Emplacement** `/etc/security/pscexpert/dodv2/chowndodfiles` **Action de conformité** Garantit que le fichier spécifié appartient au groupe bin, sys ou system.
GEN006160	Le fichier `/var/private/smbpasswd` doit appartenir à root.	**Emplacement** `/etc/security/pscexpert/dodv2/chowndodfiles` **Action de conformité** Garantit que le fichier spécifié appartient à root.
GEN006180	Le fichier `/var/private/smbpasswd` doit appartenir à un groupe tel que sys ou system.	**Emplacement** `/etc/security/pscexpert/dodv2/chowndodfiles` **Action de conformité** Garantit que le fichier spécifié appartient au groupe sys ou system.
GEN006340	Les fichiers qui se trouvent dans le répertoire `/etc/news` doivent appartenir à root ou news.	**Emplacement** `/etc/security/pscexpert/dodv2/chowndodfiles` **Action de conformité** Garantit que le répertoire spécifié appartient à root ou news.
GEN006360	Les fichiers qui se trouvent dans `/etc/news` doivent appartenir à un groupe tel que system ou news.	**Emplacement** `/etc/security/pscexpert/dodv2/chowndodfiles` **Action de conformité** Garantit que les fichiers spécifiés appartiennent au groupe system ou news.
GEN008080	Si le système utilise LDAP pour les informations d'authentification ou de compte, le fichier `/etc/ldap.conf` (ou un équivalent) doit appartenir à root.	**Emplacement** `/etc/security/pscexpert/dodv2/chowndodfiles` **Action de conformité** Garantit que le fichier spécifié appartient à root.
GEN008100	Si le système utilise LDAP pour les informations d'authentification ou de compte, le fichier `/etc/ldap.conf` (ou un équivalent) doit appartenir à un groupe tel que security, bin, sys ou system.	**Emplacement** `/etc/security/pscexpert/dodv2/chowndodfiles` **Action de conformité** Garantit que le fichier spécifié appartient au groupe bin, sys ou system.

Tableau 4. Exigences de propriété du département de la défense des Etats-Unis (suite)

ID de point de contrôle du guide STIG (Department of Defense Security Technical Implementation Guide)	Description	Emplacement du script dans lequel l'action est définie et résultats de l'action assurant la conformité
GEN008140	Si le système utilise LDAP pour les informations d'authentification ou de compte, le fichier ou le répertoire de l'autorité de certification TLS doit appartenir à root.	**Emplacement** `/etc/security/pscexpert/dodv2/chowndodfiles` **Action de conformité** Garantit que le fichier spécifié appartient à root.
GEN008160	Si le système utilise LDAP pour les informations d'authentification ou de compte, le fichier ou le répertoire de l'autorité de certification TLS doit appartenir à un groupe tel que root, bin, sys ou system.	**Emplacement** `/etc/security/pscexpert/dodv2/chowndodfiles` **Action de conformité** Garantit que le fichier spécifié appartient au groupe bin, sys ou system.

Tableau 5. Normes du département de la défense des Etats-Unis pour les droits d'accès aux fichiers

ID de point de contrôle du guide STIG (Department of Defense Security Technical Implementation Guide)	Description	Emplacement du script dans lequel l'action est définie et résultats de l'action assurant la conformité
AIX00100	Le fichier `/etc/netsvc.conf` doit être associé au mode 0644 ou à un mode moins permissif.	**Emplacement** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Action de conformité** Garantit que le fichier est associé au mode de droits d'accès spécifié ou à un mode moins permissif.
AIX00340	Le fichier `/etc/ftpaccess.ctl` doit être associé au mode 0640 ou à un mode moins permissif.	**Emplacement** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Action de conformité** Garantit que le fichier est associé au mode de droits d'accès spécifié ou à un mode moins permissif.
GEN000252	Le fichier de configuration de la synchronisation de l'heure (par exemple `/etc/ntp.conf`) doit être associé au mode 0640 ou à un mode moins permissif.	**Emplacement** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Action de conformité** Garantit que le fichier est associé au mode de droits d'accès spécifié ou à un mode moins permissif.

Tableau 5. Normes du département de la défense des Etats-Unis pour les droits d'accès aux fichiers (suite)

ID de point de contrôle du guide STIG (Department of Defense Security Technical Implementation Guide)	Description	Emplacement du script dans lequel l'action est définie et résultats de l'action assurant la conformité
GEN000920	Le répertoire de base (autre que /) du compte root doit être associé au mode 0700.	**Emplacement** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Action de conformité** Garantit que le répertoire est associé au mode de droits d'accès spécifié ou à un mode moins permissif.
GEN001140	Les répertoires et les fichiers système ne doivent pas être associés à des droits d'accès inégaux.	**Emplacement** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Action de conformité** Garantit que les droits d'accès sont cohérents.
GEN001180	Tous les fichiers de démon des services réseau doivent être associés au mode 0755 ou à un mode moins permissif.	**Emplacement** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Action de conformité** Garantit que les fichiers sont associés au mode de droits d'accès spécifié ou à un mode moins permissif.
GEN001200	Tous les fichiers de commandes système doivent être associés au mode 0755 ou à un mode moins permissif.	**Emplacement** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Action de conformité** Garantit que les fichiers sont associés au mode de droits d'accès spécifié ou à un mode moins permissif.
GEN001260	Les fichiers journaux du système doivent être associés au mode 0640 ou à un mode moins permissif.	**Emplacement** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Action de conformité** Garantit que les fichiers sont associés au mode de droits d'accès spécifié ou à un mode moins permissif.
GEN001280	Les fichiers des pages d'aide (man) doivent être associés au mode 0644 ou à un mode moins permissif.	**Emplacement** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Action de conformité** Garantit que les fichiers sont associés au mode de droits d'accès spécifié ou à un mode moins permissif.

Tableau 5. Normes du département de la défense des Etats-Unis pour les droits d'accès aux fichiers (suite)

ID de point de contrôle du guide STIG (Department of Defense Security Technical Implementation Guide)	Description	Emplacement du script dans lequel l'action est définie et résultats de l'action assurant la conformité
GEN001300	Les fichiers de bibliothèque doivent être associés au mode 0755 ou à un mode moins permissif.	**Emplacement** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Action de conformité** Garantit que les fichiers sont associés au mode de droits d'accès spécifié ou à un mode moins permissif.
GEN001360	Les fichiers NIS/NIS+/yp doivent être associés au mode 0755 ou à un mode moins permissif.	**Emplacement** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Action de conformité** Garantit que les fichiers sont associés au mode de droits d'accès spécifié ou à un mode moins permissif.
GEN001364	Le fichier `/etc/resolv.conf` doit être associé au mode 0644 ou à un mode moins permissif.	**Emplacement** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Action de conformité** Garantit que le fichier est associé au mode de droits d'accès spécifié ou à un mode moins permissif.
GEN001368	Le fichier `/etc/hosts` doit être associé au mode 0644 ou à un mode moins permissif.	**Emplacement** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Action de conformité** Garantit que le fichier est associé au mode de droits d'accès spécifié ou à un mode moins permissif.
GEN001373	Le fichier `/etc/nsswitch.conf` doit être associé au mode 0644 ou à un mode moins permissif.	**Emplacement** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Action de conformité** Garantit que le fichier est associé au mode de droits d'accès spécifié ou à un mode moins permissif.
GEN001380	Le fichier `/etc/passwd` doit être associé au mode 0644 ou à un mode moins permissif.	**Emplacement** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Action de conformité** Garantit que le fichier est associé au mode de droits d'accès spécifié ou à un mode moins permissif.

Tableau 5. Normes du département de la défense des Etats-Unis pour les droits d'accès aux fichiers (suite)

ID de point de contrôle du guide STIG (Department of Defense Security Technical Implementation Guide)	Description	Emplacement du script dans lequel l'action est définie et résultats de l'action assurant la conformité
GEN001393	Le fichier `/etc/group` doit être associé au mode 0644 ou à un mode moins permissif.	**Emplacement** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Action de conformité** Garantit que le fichier est associé au mode de droits d'accès spécifié ou à un mode moins permissif.
GEN001420	Le fichier `/etc/security/passwd` doit être associé au mode 0400.	**Emplacement** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Action de conformité** Garantit que le fichier est associé au mode de droits d'accès spécifié ou à un mode moins permissif.
GEN001480	Tous les répertoires de base d'un utilisateur doivent être associés au mode 0750 ou à un mode moins permissif.	**Emplacement** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Action de conformité** Garantit que le fichier est associé au mode de droits d'accès spécifié ou à un mode moins permissif.
GEN001560	Tous les fichiers et répertoires qui se trouvent dans les répertoires de base d'un utilisateur doivent être associés au mode 0750 ou à un mode moins permissif.	**Emplacement** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Action de conformité** Garantit que les fichiers sont associés au mode de droits d'accès spécifié ou à un mode moins permissif.
GEN001580	Tous les scripts de contrôle d'exécution doivent être associés au mode 0755 ou à un mode moins permissif.	**Emplacement** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Action de conformité** Garantit que les fichiers sont associés au mode de droits d'accès spécifié ou à un mode moins permissif.
GEN001640	Les scripts de contrôle d'exécution ne doivent pas exécuter de programmes ou de scripts accessibles en écriture par tout le monde.	**Emplacement** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Action de conformité** Vérifie les programmes, par exemple `cron`, pour déterminer s'il existe des programmes ou des scripts accessibles en écriture par tout le monde.

Tableau 5. Normes du département de la défense des Etats-Unis pour les droits d'accès aux fichiers (suite)

ID de point de contrôle du guide STIG (Department of Defense Security Technical Implementation Guide)	Description	Emplacement du script dans lequel l'action est définie et résultats de l'action assurant la conformité
GEN001720	Les fichiers d'initialisation globaux doivent être associés au mode 0644 ou à un mode moins permissif.	**Emplacement** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Action de conformité** Garantit que les fichiers sont associés au mode de droits d'accès spécifié ou à un mode moins permissif.
GEN001800	Tous les fichiers modèle (par exemple les fichiers qui se trouvent dans `/etc/skel`) doivent être associés au mode 0644 ou à un mode moins permissif.	**Emplacement** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Action de conformité** Garantit que les fichiers sont associés au mode de droits d'accès spécifié ou à un mode moins permissif.
GEN001880	Les fichiers d'initialisation locaux doivent être associés au mode 0740 ou à un mode moins permissif.	**Emplacement** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Action de conformité** Garantit que les fichiers sont associés au mode de droits d'accès spécifié ou à un mode moins permissif.
GEN002220	Les fichiers shell doivent être associés au mode 0755 ou à un mode moins permissif.	**Emplacement** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Action de conformité** Garantit que les fichiers sont associés au mode de droits d'accès spécifié ou à un mode moins permissif.
GEN002320	Les périphériques audio doivent être associés au mode 0660 ou à un mode moins permissif.	**Emplacement** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Action de conformité** Garantit que les périphériques audio sont associés au mode de droits d'accès spécifié ou à un mode moins permissif.
GEN002560	Les paramètres **umask** utilisateur par défaut et système doivent avoir la valeur 077.	**Emplacement** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Action de conformité** Garantit que les paramètres spécifiés ont pour valeur *077*.

Tableau 5. Normes du département de la défense des Etats-Unis pour les droits d'accès aux fichiers (suite)

ID de point de contrôle du guide STIG (Department of Defense Security Technical Implementation Guide)	Description	Emplacement du script dans lequel l'action est définie et résultats de l'action assurant la conformité
GEN002700	Les journaux d'audit du système doivent être associés au mode 0640 ou à un mode moins permissif.	**Emplacement** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Action de conformité** Garantit que les fichiers sont associés au mode de droits d'accès spécifié ou à un mode moins permissif.
GEN002717	Les fichiers exécutables de l'outil d'audit du système doivent être associés au mode 0750 ou à un mode moins permissif.	**Emplacement** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Action de conformité** Garantit que les fichiers sont associés au mode de droits d'accès spécifié ou à un mode moins permissif.
GEN002980	Le fichier `cron.allow` doit être associé au mode 0600 ou à un mode moins permissif.	**Emplacement** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Action de conformité** Garantit que le fichier est associé au mode de droits d'accès spécifié ou à un mode moins permissif.
GEN003080	Les fichiers crontab doivent être associés au mode 0600 ou à un mode moins permissif.	**Emplacement** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Action de conformité** Garantit que les fichiers sont associés au mode de droits d'accès spécifié ou à un mode moins permissif.
GEN003090	Les fichiers `Crontab` ne doivent pas avoir de listes de contrôle d'accès étendues.	**Emplacement** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Action de conformité** Garantit que les fichiers spécifiés n'ont pas de listes de contrôle d'accès étendues.
GEN003100	Les répertoires cron et crontab doivent être associés au mode 0755 ou à un mode moins permissif.	**Emplacement** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Action de conformité** Garantit que les répertoires spécifiés sont associés au mode de droits d'accès spécifié ou à un mode moins permissif.

Tableau 5. Normes du département de la défense des Etats-Unis pour les droits d'accès aux fichiers (suite)

ID de point de contrôle du guide STIG (Department of Defense Security Technical Implementation Guide)	Description	Emplacement du script dans lequel l'action est définie et résultats de l'action assurant la conformité
GEN003180	Le fichier `cronlog` doit être associé au mode 0600 ou à un mode moins permissif.	**Emplacement** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Action de conformité** Garantit que le fichier est associé au mode de droits d'accès spécifié ou à un mode moins permissif.
GEN003200	Le fichier `cron.deny` doit être associé au mode 0600 ou à un mode moins permissif.	**Emplacement** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Action de conformité** Garantit que le fichier est associé au mode de droits d'accès spécifié ou à un mode moins permissif.
GEN003252	Le fichier `at.deny` doit être associé au mode 0640 ou à un mode moins permissif.	**Emplacement** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Action de conformité** Garantit que le fichier est associé au mode de droits d'accès spécifié ou à un mode moins permissif.
GEN003340	Le fichier `at.allow` doit être associé au mode 0600 ou à un mode moins permissif.	**Emplacement** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Action de conformité** Garantit que le fichier est associé au mode de droits d'accès spécifié ou à un mode moins permissif.
GEN003400	Le répertoire `at` doit être associé au mode 0755 ou à un mode moins permissif.	**Emplacement** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Action de conformité** Garantit que le répertoire est associé au mode de droits d'accès spécifié ou à un mode moins permissif.
GEN003440	Les travaux `At` ne doivent pas définir le paramètre **`umask`** avec une valeur moins restrictive que 077.	**Emplacement** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Action de conformité** Garantit que le paramètre est associé au mode de droits d'accès spécifié ou à un mode moins permissif.

Tableau 5. Normes du département de la défense des Etats-Unis pour les droits d'accès aux fichiers (suite)

ID de point de contrôle du guide STIG (Department of Defense Security Technical Implementation Guide)	Description	Emplacement du script dans lequel l'action est définie et résultats de l'action assurant la conformité
GEN003740	Les fichiers `inetd.conf` et `xinetd.conf` doivent être associés au mode 0440 ou à un mode moins permissif.	**Emplacement** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Action de conformité** Garantit que les fichiers sont associés au mode de droits d'accès spécifié ou à un mode moins permissif.
GEN003780	Le fichier `services` doit être associé au mode 0444 ou à un mode moins permissif.	**Emplacement** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Action de conformité** Garantit que le fichier est associé au mode de droits d'accès spécifié ou à un mode moins permissif.
GEN003940	Le fichier `hosts.lpd` (ou un équivalent) doit être associé au mode 0644 ou à un mode moins permissif.	**Emplacement** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Action de conformité** Garantit que le fichier est associé au mode de droits d'accès spécifié ou à un mode moins permissif.
GEN004000	Le fichier `traceroute` doit être associé au mode 0700 ou à un mode moins permissif.	**Emplacement** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Action de conformité** Garantit que le fichier est associé au mode de droits d'accès spécifié ou à un mode moins permissif.
GEN004380	Le fichier `alias` doit être associé au mode 0644 ou à un mode moins permissif.	**Emplacement** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Action de conformité** Garantit que le fichier est associé au mode de droits d'accès spécifié ou à un mode moins permissif.
GEN004420	Les fichiers qui sont exécutés par le biais d'un fichier `aliases` doivent être associés au mode 0755 ou à un mode moins permissif.	**Emplacement** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Action de conformité** Garantit que les fichiers sont associés au mode de droits d'accès spécifié ou à un mode moins permissif.

Tableau 5. Normes du département de la défense des Etats-Unis pour les droits d'accès aux fichiers (suite)

ID de point de contrôle du guide STIG (Department of Defense Security Technical Implementation Guide)	Description	Emplacement du script dans lequel l'action est définie et résultats de l'action assurant la conformité
GEN004500	Le fichier journal du service SMTP doit être associé au mode 0644 ou à un mode moins permissif.	**Emplacement** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Action de conformité** Garantit que le fichier est associé au mode de droits d'accès spécifié ou à un mode moins permissif.
GEN004940	Le fichier `ftpusers` doit être associé au mode 0640 ou à un mode moins permissif.	**Emplacement** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Action de conformité** Garantit que le fichier est associé au mode de droits d'accès spécifié ou à un mode moins permissif.
GEN005040	Tous les utilisateurs FTP doivent être associés au paramètre **umask** par défaut 077.	**Emplacement** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Action de conformité** Garantit que le paramètre est correct.
GEN005100	Le démon `TFTP` doit être associé au mode 0755 ou à un mode moins permissif.	**Emplacement** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Action de conformité** Garantit que le démon est associé au mode spécifié ou à un mode moins permissif.
GEN005180	Tous les fichiers `.Xauthority` doivent être associés au mode 0600 ou à un mode moins permissif.	**Emplacement** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Action de conformité** Garantit que les fichiers sont associés au mode de droits d'accès spécifié ou à un mode moins permissif.
GEN005320	Le fichier `snmpd.conf` doit être associé au mode 0600 ou à un mode moins permissif.	**Emplacement** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Action de conformité** Garantit que le fichier est associé au mode de droits d'accès spécifié ou à un mode moins permissif.
GEN005340	Les fichiers de base d'informations de gestion (MIB) doivent être associés au mode 0640 ou à un mode moins permissif.	**Emplacement** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Action de conformité** Garantit que les fichiers sont associés au mode de droits d'accès spécifié ou à un mode moins permissif.

Tableau 5. Normes du département de la défense des Etats-Unis pour les droits d'accès aux fichiers (suite)

ID de point de contrôle du guide STIG (Department of Defense Security Technical Implementation Guide)	Description	Emplacement du script dans lequel l'action est définie et résultats de l'action assurant la conformité
GEN005390	Le fichier `/etc/syslog.conf` doit être associé au mode 0640 ou à un mode moins permissif.	**Emplacement** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Action de conformité** Garantit que le fichier est associé au mode de droits d'accès spécifié ou à un mode moins permissif.
GEN005522	Les fichiers de clés d'hôte publiques SSH doivent être associés au mode 0644 ou à un mode moins permissif.	**Emplacement** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Action de conformité** Garantit que les fichiers sont associés au mode de droits d'accès spécifié ou à un mode moins permissif.
GEN005523	Les fichiers de clés d'hôte privées SSH doivent être associés au mode 0600 ou à un mode moins permissif.	**Emplacement** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Action de conformité** Garantit que les fichiers sont associés au mode de droits d'accès spécifié ou à un mode moins permissif.
GEN006140	Le fichier `/usr/lib/smb.conf` doit être associé au mode 0644 ou à un mode moins permissif.	**Emplacement** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Action de conformité** Garantit que le fichier est associé au mode de droits d'accès spécifié ou à un mode moins permissif.
GEN006200	Le fichier `/var/private/smbpasswd` doit être associé au mode 0600 ou à un mode moins permissif.	**Emplacement** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Action de conformité** Garantit que le fichier est associé au mode de droits d'accès spécifié ou à un mode moins permissif.
GEN006260	Le fichier `/etc/news/hosts.nntp` (ou un équivalent) doit être associé au mode 0600 ou à un mode moins permissif.	**Emplacement** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Action de conformité** Garantit que le fichier est associé au mode de droits d'accès spécifié ou à un mode moins permissif.

Tableau 5. Normes du département de la défense des Etats-Unis pour les droits d'accès aux fichiers (suite)

ID de point de contrôle du guide STIG (Department of Defense Security Technical Implementation Guide)	Description	Emplacement du script dans lequel l'action est définie et résultats de l'action assurant la conformité
GEN006280	Le fichier `/etc/news/hosts.nntp.nolimit` (ou un équivalent) doit être associé au mode 0600 ou à un mode moins permissif.	**Emplacement** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Action de conformité** Garantit que le fichier est associé au mode de droits d'accès spécifié ou à un mode moins permissif.
GEN006300	Le fichier `/etc/news/nnrp.access` (ou un équivalent) doit être associé au mode 0600 ou à un mode moins permissif.	**Emplacement** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Action de conformité** Garantit que le fichier est associé au mode de droits d'accès spécifié ou à un mode moins permissif.
GEN006320	Le fichier `/etc/news/passwd.nntp` (ou un équivalent) doit être associé au mode 0600 ou à un mode moins permissif.	**Emplacement** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Action de conformité** Garantit que le fichier est associé au mode de droits d'accès spécifié ou à un mode moins permissif.
GEN008060	Si le système utilise LDAP pour les informations d'authentification ou de compte, le fichier `/etc/ldap.conf` (ou un équivalent) doit être associé au mode 0644 ou à un mode moins permissif.	**Emplacement** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Action de conformité** Garantit que le fichier est associé au mode de droits d'accès spécifié ou à un mode moins permissif.
GEN008180	Si le système utilise LDAP pour les informations d'authentification ou de compte, le fichier et/ou le répertoire de l'autorité de certification doivent être associé au mode 0644 (0755 pour les répertoires) ou à un mode moins permissif.	**Emplacement** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Action de conformité** Garantit que le fichier et/ou les répertoires spécifiés sont associés au mode de droits d'accès spécifié ou à un mode moins permissif.

Tableau 6. Exigences de liste de contrôle d'accès (ACL) du département de la défense des Etats-Unis

ID de point de contrôle du guide STIG (Department of Defense Security Technical Implementation Guide)	Description	Emplacement du script dans lequel l'action est définie et résultats de l'action assurant la conformité
AIX00110	Le fichier `/etc/netsvc.conf` ne doit pas avoir de liste de contrôle d'accès étendue.	**Emplacement** `/etc/security/pscexpert/dodv2/acldodfiles` **Action de conformité** Désactive la liste de contrôle d'accès étendue spécifiée. **Remarque :** Ce paramètre n'est pas modifié automatiquement lorsque la stratégie AIX par défaut est restaurée avec le fichier `DoDv2_to_AIXDefault.xml`. Vous devez le changer manuellement.
AIX00350	Le fichier `/etc/ftpaccess.ctl` ne doit pas avoir de liste de contrôle d'accès étendue.	**Emplacement** `/etc/security/pscexpert/dodv2/acldodfiles` **Action de conformité** Désactive la liste de contrôle d'accès étendue spécifiée. **Remarque :** Ce paramètre n'est pas modifié automatiquement lorsque la stratégie AIX par défaut est restaurée avec le fichier `DoDv2_to_AIXDefault.xml`. Vous devez le changer manuellement.
GEN000253	Le fichier de configuration de la synchronisation de l'heure (par exemple `/etc/ntp.conf`) ne doit pas avoir de liste de contrôle d'accès étendue.	**Emplacement** `/etc/security/pscexpert/dodv2/acldodfiles` **Action de conformité** Désactive la liste de contrôle d'accès étendue spécifiée. **Remarque :** Ce paramètre n'est pas modifié automatiquement lorsque la stratégie AIX par défaut est restaurée avec le fichier `DoDv2_to_AIXDefault.xml`. Vous devez le changer manuellement.
GEN000930	Le répertoire de base du compte root ne doit pas avoir de liste de contrôle d'accès étendue.	**Emplacement** `/etc/security/pscexpert/dodv2/acldodfiles` **Action de conformité** Désactive la liste de contrôle d'accès étendue spécifiée. **Remarque :** Ce paramètre n'est pas modifié automatiquement lorsque la stratégie AIX par défaut est restaurée avec le fichier `DoDv2_to_AIXDefault.xml`. Vous devez le changer manuellement.

Tableau 6. Exigences de liste de contrôle d'accès (ACL) du département de la défense des Etats-Unis (suite)

ID de point de contrôle du guide STIG (Department of Defense Security Technical Implementation Guide)	Description	Emplacement du script dans lequel l'action est définie et résultats de l'action assurant la conformité
GEN001190	Les fichiers de démon des services réseau ne doivent pas avoir de listes de contrôle d'accès étendues.	**Emplacement** `/etc/security/pscexpert/dodv2/acldodfiles` **Action de conformité** Désactive la liste de contrôle d'accès étendue spécifiée. **Remarque :** Ce paramètre n'est pas modifié automatiquement lorsque la stratégie AIX par défaut est restaurée avec le fichier `DoDv2_to_AIXDefault.xml`. Vous devez le changer manuellement.
GEN001210	Les fichiers de commandes système ne doivent pas avoir de listes de contrôle d'accès étendues.	**Emplacement** `/etc/security/pscexpert/dodv2/acldodfiles` **Action de conformité** Désactive la liste de contrôle d'accès étendue spécifiée. **Remarque :** Ce paramètre n'est pas modifié automatiquement lorsque la stratégie AIX par défaut est restaurée avec le fichier `DoDv2_to_AIXDefault.xml`. Vous devez le changer manuellement.
GEN001270	Les fichiers journaux du système ne doivent pas avoir de listes de contrôle d'accès étendues, sauf si nécessaire pour la prise en charge des logiciels autorisés.	**Emplacement** `/etc/security/pscexpert/dodv2/acldodfiles` **Action de conformité** Désactive la liste de contrôle d'accès étendue spécifiée. **Remarque :** Ce paramètre n'est pas modifié automatiquement lorsque la stratégie AIX par défaut est restaurée avec le fichier `DoDv2_to_AIXDefault.xml`. Vous devez le changer manuellement.
GEN001310	Les fichiers de bibliothèque ne doivent pas avoir de listes de contrôle d'accès étendues.	**Emplacement** `/etc/security/pscexpert/dodv2/acldodfiles` **Action de conformité** Désactive la liste de contrôle d'accès étendue spécifiée. **Remarque :** Ce paramètre n'est pas modifié automatiquement lorsque la stratégie AIX par défaut est restaurée avec le fichier `DoDv2_to_AIXDefault.xml`. Vous devez le changer manuellement.

Tableau 6. Exigences de liste de contrôle d'accès (ACL) du département de la défense des Etats-Unis (suite)

ID de point de contrôle du guide STIG (Department of Defense Security Technical Implementation Guide)	Description	Emplacement du script dans lequel l'action est définie et résultats de l'action assurant la conformité
GEN001361	Les fichiers de commandes système NIS/NIS+/yp ne doivent pas avoir de listes de contrôle d'accès étendues.	**Emplacement** `/etc/security/pscexpert/dodv2/acldodfiles` **Action de conformité** Désactive la liste de contrôle d'accès étendue spécifiée. **Remarque :** Ce paramètre n'est pas modifié automatiquement lorsque la stratégie AIX par défaut est restaurée avec le fichier `DoDv2_to_AIXDefault.xml`. Vous devez le changer manuellement.
GEN001365	Le fichier `/etc/resolv.conf` ne doit pas avoir de liste de contrôle d'accès étendue.	**Emplacement** `/etc/security/pscexpert/dodv2/acldodfiles` **Action de conformité** Désactive la liste de contrôle d'accès étendue spécifiée. **Remarque :** Ce paramètre n'est pas modifié automatiquement lorsque la stratégie AIX par défaut est restaurée avec le fichier `DoDv2_to_AIXDefault.xml`. Vous devez le changer manuellement.
GEN001369	Le fichier `/etc/hosts` ne doit pas avoir de liste de contrôle d'accès étendue.	**Emplacement** `/etc/security/pscexpert/dodv2/acldodfiles` **Action de conformité** Désactive la liste de contrôle d'accès étendue spécifiée. **Remarque :** Ce paramètre n'est pas modifié automatiquement lorsque la stratégie AIX par défaut est restaurée avec le fichier `DoDv2_to_AIXDefault.xml`. Vous devez le changer manuellement.
GEN001374	Le fichier `/etc/nsswitch.conf` ne doit pas avoir de liste de contrôle d'accès étendue.	**Emplacement** `/etc/security/pscexpert/dodv2/acldodfiles` **Action de conformité** Désactive la liste de contrôle d'accès étendue spécifiée. **Remarque :** Ce paramètre n'est pas modifié automatiquement lorsque la stratégie AIX par défaut est restaurée avec le fichier `DoDv2_to_AIXDefault.xml`. Vous devez le changer manuellement.

Tableau 6. Exigences de liste de contrôle d'accès (ACL) du département de la défense des Etats-Unis (suite)

ID de point de contrôle du guide STIG (Department of Defense Security Technical Implementation Guide)	Description	Emplacement du script dans lequel l'action est définie et résultats de l'action assurant la conformité
GEN001390	Le fichier `/etc/passwd` ne doit pas avoir de liste de contrôle d'accès étendue.	**Emplacement** `/etc/security/pscexpert/dodv2/acldodfiles` **Action de conformité** Désactive la liste de contrôle d'accès étendue spécifiée. **Remarque :** Ce paramètre n'est pas modifié automatiquement lorsque la stratégie AIX par défaut est restaurée avec le fichier `DoDv2_to_AIXDefault.xml`. Vous devez le changer manuellement.
GEN001394	Le fichier `/etc/group` ne doit pas avoir de liste de contrôle d'accès étendue.	**Emplacement** `/etc/security/pscexpert/dodv2/acldodfiles` **Action de conformité** Désactive la liste de contrôle d'accès étendue spécifiée. **Remarque :** Ce paramètre n'est pas modifié automatiquement lorsque la stratégie AIX par défaut est restaurée avec le fichier `DoDv2_to_AIXDefault.xml`. Vous devez le changer manuellement.
GEN001430	Le fichier `/etc/security/passwd` ne doit pas avoir de liste de contrôle d'accès étendue.	**Emplacement** `/etc/security/pscexpert/dodv2/acldodfiles` **Action de conformité** Désactive la liste de contrôle d'accès étendue spécifiée. **Remarque :** Ce paramètre n'est pas modifié automatiquement lorsque la stratégie AIX par défaut est restaurée avec le fichier `DoDv2_to_AIXDefault.xml`. Vous devez le changer manuellement.
GEN001570	Les fichiers et les répertoires qui se trouvent dans les répertoires de base de l'utilisateur ne doivent pas avoir de listes de contrôle d'accès étendues.	**Emplacement** `/etc/security/pscexpert/dodv2/acldodfiles` **Action de conformité** Désactive la liste de contrôle d'accès étendue spécifiée. **Remarque :** Ce paramètre n'est pas modifié automatiquement lorsque la stratégie AIX par défaut est restaurée avec le fichier `DoDv2_to_AIXDefault.xml`. Vous devez le changer manuellement.

Tableau 6. Exigences de liste de contrôle d'accès (ACL) du département de la défense des Etats-Unis (suite)

ID de point de contrôle du guide STIG (Department of Defense Security Technical Implementation Guide)	Description	Emplacement du script dans lequel l'action est définie et résultats de l'action assurant la conformité
GEN001590	Les scripts de contrôle d'exécution ne doivent pas avoir de listes de contrôle d'accès étendues.	**Emplacement** `/etc/security/pscexpert/dodv2/acldodfiles` **Action de conformité** Désactive la liste de contrôle d'accès étendue spécifiée. **Remarque :** Ce paramètre n'est pas modifié automatiquement lorsque la stratégie AIX par défaut est restaurée avec le fichier `DoDv2_to_AIXDefault.xml`. Vous devez le changer manuellement.
GEN001730	Les fichiers d'initialisation globaux ne doivent pas avoir de listes de contrôle d'accès étendues.	**Emplacement** `/etc/security/pscexpert/dodv2/acldodfiles` **Action de conformité** Désactive la liste de contrôle d'accès étendue spécifiée. **Remarque :** Ce paramètre n'est pas modifié automatiquement lorsque la stratégie AIX par défaut est restaurée avec le fichier `DoDv2_to_AIXDefault.xml`. Vous devez le changer manuellement.
GEN001810	Les fichiers modèle ne doivent pas avoir de listes de contrôle d'accès étendues.	**Emplacement** `/etc/security/pscexpert/dodv2/acldodfiles` **Action de conformité** Désactive la liste de contrôle d'accès étendue spécifiée. **Remarque :** Ce paramètre n'est pas modifié automatiquement lorsque la stratégie AIX par défaut est restaurée avec le fichier `DoDv2_to_AIXDefault.xml`. Vous devez le changer manuellement.
GEN001890	Les fichiers d'initialisation locaux ne doivent pas avoir de listes de contrôle d'accès étendues.	**Emplacement** `/etc/security/pscexpert/dodv2/acldodfiles` **Action de conformité** Désactive la liste de contrôle d'accès étendue spécifiée. **Remarque :** Ce paramètre n'est pas modifié automatiquement lorsque la stratégie AIX par défaut est restaurée avec le fichier `DoDv2_to_AIXDefault.xml`. Vous devez le changer manuellement.

Tableau 6. Exigences de liste de contrôle d'accès (ACL) du département de la défense des Etats-Unis (suite)

ID de point de contrôle du guide STIG (Department of Defense Security Technical Implementation Guide)	Description	Emplacement du script dans lequel l'action est définie et résultats de l'action assurant la conformité
GEN002230	Les fichiers shell ne doivent pas avoir de listes de contrôle d'accès étendues.	**Emplacement** `/etc/security/pscexpert/dodv2/acldodfiles` **Action de conformité** Désactive la liste de contrôle d'accès étendue spécifiée. **Remarque :** Ce paramètre n'est pas modifié automatiquement lorsque la stratégie AIX par défaut est restaurée avec le fichier `DoDv2_to_AIXDefault.xml`. Vous devez le changer manuellement.
GEN002330	Les périphériques audio ne doivent pas avoir de listes de contrôle d'accès étendues.	**Emplacement** `/etc/security/pscexpert/dodv2/acldodfiles` **Action de conformité** Désactive la liste de contrôle d'accès étendue spécifiée. **Remarque :** Ce paramètre n'est pas modifié automatiquement lorsque la stratégie AIX par défaut est restaurée avec le fichier `DoDv2_to_AIXDefault.xml`. Vous devez le changer manuellement.
GEN002710	Les fichiers d'audit du système ne doivent pas avoir de listes de contrôle d'accès étendues.	**Emplacement** `/etc/security/pscexpert/dodv2/acldodfiles` **Action de conformité** Désactive la liste de contrôle d'accès étendue spécifiée. **Remarque :** Ce paramètre n'est pas modifié automatiquement lorsque la stratégie AIX par défaut est restaurée avec le fichier `DoDv2_to_AIXDefault.xml`. Vous devez le changer manuellement.
GEN002990	Les listes de contrôle d'accès étendues doivent être désactivées pour les fichiers `cron.allow` et `cron.deny`.	**Emplacement** `/etc/security/pscexpert/dodv2/acldodfiles` **Action de conformité** Désactive la liste de contrôle d'accès étendue spécifiée. **Remarque :** Ce paramètre n'est pas modifié automatiquement lorsque la stratégie AIX par défaut est restaurée avec le fichier `DoDv2_to_AIXDefault.xml`. Vous devez le changer manuellement.

Tableau 6. Exigences de liste de contrôle d'accès (ACL) du département de la défense des Etats-Unis (suite)

ID de point de contrôle du guide STIG (Department of Defense Security Technical Implementation Guide)	Description	Emplacement du script dans lequel l'action est définie et résultats de l'action assurant la conformité
GEN003090	Les fichiers crontab ne doivent pas avoir de listes de contrôle d'accès étendues.	**Emplacement** `/etc/security/pscexpert/dodv2/acldodfiles` **Action de conformité** Désactive la liste de contrôle d'accès étendue spécifiée. **Remarque :** Ce paramètre n'est pas modifié automatiquement lorsque la stratégie AIX par défaut est restaurée avec le fichier `DoDv2_to_AIXDefault.xml`. Vous devez le changer manuellement.
GEN003110	Les répertoires cron et crontab ne doivent pas avoir de listes de contrôle d'accès étendues.	**Emplacement** `/etc/security/pscexpert/dodv2/acldodfiles` **Action de conformité** Désactive la liste de contrôle d'accès étendue spécifiée. **Remarque :** Ce paramètre n'est pas modifié automatiquement lorsque la stratégie AIX par défaut est restaurée avec le fichier `DoDv2_to_AIXDefault.xml`. Vous devez le changer manuellement.
GEN003190	Les fichiers journaux cron ne doivent pas avoir de listes de contrôle d'accès étendues.	**Emplacement** `/etc/security/pscexpert/dodv2/acldodfiles` **Action de conformité** Désactive la liste de contrôle d'accès étendue spécifiée. **Remarque :** Ce paramètre n'est pas modifié automatiquement lorsque la stratégie AIX par défaut est restaurée avec le fichier `DoDv2_to_AIXDefault.xml`. Vous devez le changer manuellement.
GEN003210	Le fichier `cron.deny` ne doit pas avoir de liste de contrôle d'accès étendue.	**Emplacement** `/etc/security/pscexpert/dodv2/acldodfiles` **Action de conformité** Désactive la liste de contrôle d'accès étendue spécifiée. **Remarque :** Ce paramètre n'est pas modifié automatiquement lorsque la stratégie AIX par défaut est restaurée avec le fichier `DoDv2_to_AIXDefault.xml`. Vous devez le changer manuellement.

Tableau 6. Exigences de liste de contrôle d'accès (ACL) du département de la défense des Etats-Unis (suite)

ID de point de contrôle du guide STIG (Department of Defense Security Technical Implementation Guide)	Description	Emplacement du script dans lequel l'action est définie et résultats de l'action assurant la conformité
GEN003245	Le fichier `at.allow` ne doit pas avoir de liste de contrôle d'accès étendue.	**Emplacement** `/etc/security/pscexpert/dodv2/acldodfiles` **Action de conformité** Désactive la liste de contrôle d'accès étendue spécifiée. **Remarque :** Ce paramètre n'est pas modifié automatiquement lorsque la stratégie AIX par défaut est restaurée avec le fichier `DoDv2_to_AIXDefault.xml`. Vous devez le changer manuellement.
GEN003255	Le fichier `at.deny` ne doit pas avoir de liste de contrôle d'accès étendue.	**Emplacement** `/etc/security/pscexpert/dodv2/acldodfiles` **Action de conformité** Désactive la liste de contrôle d'accès étendue spécifiée. **Remarque :** Ce paramètre n'est pas modifié automatiquement lorsque la stratégie AIX par défaut est restaurée avec le fichier `DoDv2_to_AIXDefault.xml`. Vous devez le changer manuellement.
GEN003410	Le répertoire `at` ne doit pas avoir de liste de contrôle d'accès étendue.	**Emplacement** `/etc/security/pscexpert/dodv2/acldodfiles` **Action de conformité** Désactive la liste de contrôle d'accès étendue spécifiée. **Remarque :** Ce paramètre n'est pas modifié automatiquement lorsque la stratégie AIX par défaut est restaurée avec le fichier `DoDv2_to_AIXDefault.xml`. Vous devez le changer manuellement.
GEN003745	Les fichiers `inetd.conf` et `xinetd.conf` ne doivent pas avoir de listes de contrôle d'accès étendues.	**Emplacement** `/etc/security/pscexpert/dodv2/acldodfiles` **Action de conformité** Désactive la liste de contrôle d'accès étendue spécifiée. **Remarque :** Ce paramètre n'est pas modifié automatiquement lorsque la stratégie AIX par défaut est restaurée avec le fichier `DoDv2_to_AIXDefault.xml`. Vous devez le changer manuellement.

Tableau 6. Exigences de liste de contrôle d'accès (ACL) du département de la défense des Etats-Unis (suite)

ID de point de contrôle du guide STIG (Department of Defense Security Technical Implementation Guide)	Description	Emplacement du script dans lequel l'action est définie et résultats de l'action assurant la conformité
GEN003790	Le fichier services ne doit pas avoir de liste de contrôle d'accès étendue.	**Emplacement** `/etc/security/pscexpert/dodv2/acldodfiles` **Action de conformité** Désactive la liste de contrôle d'accès étendue spécifiée. **Remarque :** Ce paramètre n'est pas modifié automatiquement lorsque la stratégie AIX par défaut est restaurée avec le fichier `DoDv2_to_AIXDefault.xml`. Vous devez le changer manuellement.
GEN003950	Le fichier `hosts.lpd` (ou un équivalent) ne doit pas avoir de liste de contrôle d'accès étendue.	**Emplacement** `/etc/security/pscexpert/dodv2/acldodfiles` **Action de conformité** Désactive la liste de contrôle d'accès étendue spécifiée. **Remarque :** Ce paramètre n'est pas modifié automatiquement lorsque la stratégie AIX par défaut est restaurée avec le fichier `DoDv2_to_AIXDefault.xml`. Vous devez le changer manuellement.
GEN004010	Le fichier `traceroute` ne doit pas avoir de liste de contrôle d'accès étendue.	**Emplacement** `/etc/security/pscexpert/dodv2/acldodfiles` **Action de conformité** Désactive la liste de contrôle d'accès étendue spécifiée. **Remarque :** Ce paramètre n'est pas modifié automatiquement lorsque la stratégie AIX par défaut est restaurée avec le fichier `DoDv2_to_AIXDefault.xml`. Vous devez le changer manuellement.
GEN004390	Le fichier `alias` ne doit pas avoir de liste de contrôle d'accès étendue.	**Emplacement** `/etc/security/pscexpert/dodv2/acldodfiles` **Action de conformité** Désactive la liste de contrôle d'accès étendue spécifiée. **Remarque :** Ce paramètre n'est pas modifié automatiquement lorsque la stratégie AIX par défaut est restaurée avec le fichier `DoDv2_to_AIXDefault.xml`. Vous devez le changer manuellement.

Tableau 6. Exigences de liste de contrôle d'accès (ACL) du département de la défense des Etats-Unis (suite)

ID de point de contrôle du guide STIG (Department of Defense Security Technical Implementation Guide)	Description	Emplacement du script dans lequel l'action est définie et résultats de l'action assurant la conformité
GEN004430	Les fichiers qui sont exécutés par le biais d'un fichier `aliases` ne doivent pas avoir de listes de contrôle d'accès étendues.	**Emplacement** `/etc/security/pscexpert/dodv2/acldodfiles` **Action de conformité** Désactive la liste de contrôle d'accès étendue spécifiée. **Remarque :** Ce paramètre n'est pas modifié automatiquement lorsque la stratégie AIX par défaut est restaurée avec le fichier `DoDv2_to_AIXDefault.xml`. Vous devez le changer manuellement.
GEN004510	Le fichier journal du service SMTP ne doit pas avoir de liste de contrôle d'accès étendue.	**Emplacement** `/etc/security/pscexpert/dodv2/acldodfiles` **Action de conformité** Désactive la liste de contrôle d'accès étendue spécifiée. **Remarque :** Ce paramètre n'est pas modifié automatiquement lorsque la stratégie AIX par défaut est restaurée avec le fichier `DoDv2_to_AIXDefault.xml`. Vous devez le changer manuellement.
GEN004950	Le fichier `ftpusers` ne doit pas avoir de liste de contrôle d'accès étendue.	**Emplacement** `/etc/security/pscexpert/dodv2/acldodfiles` **Action de conformité** Désactive la liste de contrôle d'accès étendue spécifiée. **Remarque :** Ce paramètre n'est pas modifié automatiquement lorsque la stratégie AIX par défaut est restaurée avec le fichier `DoDv2_to_AIXDefault.xml`. Vous devez le changer manuellement.
GEN005190	Les fichiers `.Xauthority` ne doivent pas avoir de listes de contrôle d'accès étendues.	**Emplacement** `/etc/security/pscexpert/dodv2/acldodfiles` **Action de conformité** Désactive la liste de contrôle d'accès étendue spécifiée. **Remarque :** Ce paramètre n'est pas modifié automatiquement lorsque la stratégie AIX par défaut est restaurée avec le fichier `DoDv2_to_AIXDefault.xml`. Vous devez le changer manuellement.

Tableau 6. Exigences de liste de contrôle d'accès (ACL) du département de la défense des Etats-Unis (suite)

ID de point de contrôle du guide STIG (Department of Defense Security Technical Implementation Guide)	Description	Emplacement du script dans lequel l'action est définie et résultats de l'action assurant la conformité
GEN005350	Les fichiers de base d'informations de gestion (MIB) ne doivent pas avoir de listes de contrôle d'accès étendues.	**Emplacement** `/etc/security/pscexpert/dodv2/acldodfiles` **Action de conformité** Désactive la liste de contrôle d'accès étendue spécifiée. **Remarque :** Ce paramètre n'est pas modifié automatiquement lorsque la stratégie AIX par défaut est restaurée avec le fichier `DoDv2_to_AIXDefault.xml`. Vous devez le changer manuellement.
GEN005375	Le fichier `snmpd.conf` ne doit pas avoir de liste de contrôle d'accès étendue.	**Emplacement** `/etc/security/pscexpert/dodv2/acldodfiles` **Action de conformité** Désactive la liste de contrôle d'accès étendue spécifiée. **Remarque :** Ce paramètre n'est pas modifié automatiquement lorsque la stratégie AIX par défaut est restaurée avec le fichier `DoDv2_to_AIXDefault.xml`. Vous devez le changer manuellement.
GEN005395	Le fichier `/etc/syslog.conf` ne doit pas avoir de liste de contrôle d'accès étendue.	**Emplacement** `/etc/security/pscexpert/dodv2/acldodfiles` **Action de conformité** Désactive la liste de contrôle d'accès étendue spécifiée. **Remarque :** Ce paramètre n'est pas modifié automatiquement lorsque la stratégie AIX par défaut est restaurée avec le fichier `DoDv2_to_AIXDefault.xml`. Vous devez le changer manuellement.
GEN006150	Le fichier `/usr/lib/smb.conf` ne doit pas avoir de liste de contrôle d'accès étendue.	**Emplacement** `/etc/security/pscexpert/dodv2/acldodfiles` **Action de conformité** Désactive la liste de contrôle d'accès étendue spécifiée. **Remarque :** Ce paramètre n'est pas modifié automatiquement lorsque la stratégie AIX par défaut est restaurée avec le fichier `DoDv2_to_AIXDefault.xml`. Vous devez le changer manuellement.

Tableau 6. Exigences de liste de contrôle d'accès (ACL) du département de la défense des Etats-Unis (suite)

ID de point de contrôle du guide STIG (Department of Defense Security Technical Implementation Guide)	Description	Emplacement du script dans lequel l'action est définie et résultats de l'action assurant la conformité
GEN006210	Le fichier `/var/private/smbpasswd` ne doit pas avoir de liste de contrôle d'accès étendue.	**Emplacement** `/etc/security/pscexpert/dodv2/acldodfiles` **Action de conformité** Désactive la liste de contrôle d'accès étendue spécifiée. **Remarque :** Ce paramètre n'est pas modifié automatiquement lorsque la stratégie AIX par défaut est restaurée avec le fichier `DoDv2_to_AIXDefault.xml`. Vous devez le changer manuellement.
GEN006270	Le fichier `/etc/news/hosts.nntp` ne doit pas avoir de liste de contrôle d'accès étendue.	**Emplacement** `/etc/security/pscexpert/dodv2/acldodfiles` **Action de conformité** Désactive la liste de contrôle d'accès étendue spécifiée. **Remarque :** Ce paramètre n'est pas modifié automatiquement lorsque la stratégie AIX par défaut est restaurée avec le fichier `DoDv2_to_AIXDefault.xml`. Vous devez le changer manuellement.
GEN006290	Le fichier `/etc/news/hosts.nntp.nolimit` ne doit pas avoir de liste de contrôle d'accès étendue.	**Emplacement** `/etc/security/pscexpert/dodv2/acldodfiles` **Action de conformité** Désactive la liste de contrôle d'accès étendue spécifiée. **Remarque :** Ce paramètre n'est pas modifié automatiquement lorsque la stratégie AIX par défaut est restaurée avec le fichier `DoDv2_to_AIXDefault.xml`. Vous devez le changer manuellement.
GEN006310	Le fichier `/etc/news/nnrp.access` ne doit pas avoir de liste de contrôle d'accès étendue.	**Emplacement** `/etc/security/pscexpert/dodv2/acldodfiles` **Action de conformité** Désactive la liste de contrôle d'accès étendue spécifiée. **Remarque :** Ce paramètre n'est pas modifié automatiquement lorsque la stratégie AIX par défaut est restaurée avec le fichier `DoDv2_to_AIXDefault.xml`. Vous devez le changer manuellement.

Tableau 6. Exigences de liste de contrôle d'accès (ACL) du département de la défense des Etats-Unis (suite)

ID de point de contrôle du guide STIG (Department of Defense Security Technical Implementation Guide)	Description	Emplacement du script dans lequel l'action est définie et résultats de l'action assurant la conformité
GEN006330	Le fichier `/etc/news/passwd.nntp` ne doit pas avoir de liste de contrôle d'accès étendue.	**Emplacement** `/etc/security/pscexpert/dodv2/acldodfiles` **Action de conformité** Désactive la liste de contrôle d'accès étendue spécifiée. **Remarque :** Ce paramètre n'est pas modifié automatiquement lorsque la stratégie AIX par défaut est restaurée avec le fichier `DoDv2_to_AIXDefault.xml`. Vous devez le changer manuellement.
GEN008120	Si le système utilise LDAP pour les informations d'authentification ou de compte, le fichier `/etc/ldap.conf` (ou un équivalent) ne doit pas avoir de liste de contrôle d'accès étendue.	**Emplacement** `/etc/security/pscexpert/dodv2/acldodfiles` **Action de conformité** Garantit que les fichiers spécifiés n'ont pas de liste de contrôle d'accès étendue. **Remarque :** Ce paramètre n'est pas modifié automatiquement lorsque la stratégie AIX par défaut est restaurée avec le fichier `DoDv2_to_AIXDefault.xml`. Vous devez le changer manuellement.
GEN008200	Si le système utilise LDAP pour les informations d'authentification ou de compte, le fichier ou le répertoire de l'autorité de certification LDAP TLS (selon le cas) ne doit pas avoir de liste de contrôle d'accès étendue.	**Emplacement** `/etc/security/pscexpert/dodv2/acldodfiles` **Action de conformité** Garantit que le fichier ou le répertoire spécifié n'a pas de liste de contrôle d'accès étendue. **Remarque :** Ce paramètre n'est pas modifié automatiquement lorsque la stratégie AIX par défaut est restaurée avec le fichier `DoDv2_to_AIXDefault.xml`. Vous devez le changer manuellement.

Information associée:

Conformité au guide STIG du département de la défense des Etats-Unis (Department of Defense Security Technical Implementation Guide)

Conformité au standard PCI-DSS (Payment Card Industry Data Security Standard)

Le standard PCI-DSS (Payment Card Industry Data Security Standard) catégorise la sécurité informatique dans 12 sections qui constituent les 12 exigences et procédures d'évaluation de la sécurité.

Les 12 exigences et procédures d'évaluation de la sécurité informatique qui sont définies par le standard PCI-DSS sont les suivantes :

Exigence 1 : installez et gérez une configuration de pare-feu afin de protéger les données du titulaire de la carte.

Liste documentée des services et des ports nécessaires à l'activité. Vous pouvez implémenter cette exigence en désactivant les services inutiles et non sécurisés.

Exigence 2 : n'utilisez pas de valeurs par défaut définies par le fournisseur pour les mots de passe du système et d'autre paramètres de sécurité.

Changez systématiquement les valeurs par défaut définies par le fournisseur avant d'installer un système sur le réseau. Vous pouvez implémenter cette exigence en désactivant le démon SNMP (Simple Network Management Protocol).

Exigence 3 : protégez les données stockées du titulaire de la carte.

Vous pouvez implémenter cette exigence en activant la fonction Encrypted File System (EFS) qui est fournie avec le système d'exploitation AIX.

Exigence 4 : chiffrez les données du titulaire de la carte lorsque vous les transmettez sur des réseaux publics ouverts.

Vous pouvez implémenter cette exigence en activant la fonction IP Security (IPSEC) qui est fournie avec le système d'exploitation AIX.

Exigence 5 : utilisez des logiciels antivirus et mettez-les à jour régulièrement.

Vous pouvez implémenter cette exigence en utilisant le programme de stratégie Trusted Execution. Trusted Execution est le logiciel antivirus recommandé natif du système d'exploitation AIX. PCI requiert que vous capturiez les journaux depuis le programme Trusted Execution en activant la gestion des événements et des informations de sécurité (SIEM) afin de surveiller les alertes. Si vous exécutez le programme Trusted Execution en mode journal seul, la vérification n'est pas arrêtée lorsqu'une erreur est causée par une non-concordance de hachage.

Exigence 6 : développez et gérez des systèmes et des applications sécurisés.

Pour implémenter cette exigence, vous devez installer les correctifs requis sur votre système manuellement. Si vous avez acheté PowerSC Standard Edition, vous pouvez utiliser la fonction Trusted Network Connect (TNC).

Exigence 7 : restreignez l'accès aux données du titulaire de la carte en fonction des besoins d'affaires à connaître.

Vous pouvez implémenter des mesures de contrôle d'accès strictes à l'aide de la fonction RBAC permettant d'activer des règles et des rôles. La fonction RBAC ne peut pas être automatisée car son activation requiert l'intervention d'un administrateur.

`RbacEnablement` vérifie le système afin de déterminer si les propriétés isso, so et sa pour les rôles existent sur le système. Si elles n'existent pas, le script les crée. Ce script est également exécuté dans le cadre des vérifications pscexpert auxquelles il procède lorsqu'il exécute des commandes, comme la commande `pscxpert -c`.

Exigence 8 : affectez un ID unique à chaque personne ayant accès à l'ordinateur.

Vous pouvez implémenter cette exigence en activant des profils PCI. Les règles suivantes s'appliquent aux profils PCI :

- Les mots de passe utilisateur doivent être changés tous les 90 jours au moins.
- La longueur minimale d'un mot de passe est de 7 caractères.
- Les mots de passe doivent comporter des caractères numériques et alphabétiques.
- Un individu ne doit pas pouvoir soumettre un nouveau mot de passe s'il est identique aux quatre mots de passe précédents ayant été utilisés.
- Les tentatives d'accès répétées doivent être limitées via le verrouillage de l'ID utilisateur après six échecs.
- La durée de verrouillage doit être de 30 minutes ou le verrouillage peut durer jusqu'à ce qu'un administrateur réactive l'ID utilisateur.
- Un utilisateur doit être obligé de saisir à nouveau son mot de passe pour réactiver un terminal si ce dernier est en veille depuis 15 minutes ou plus.

Exigence 9 : restreignez l'accès physique aux données du titulaire de la carte.
Stockez les référentiels contenant des données sensibles sur les titulaires de carte dans une salle dont l'accès est restreint.

Exigence 10 : suivez et contrôlez les accès aux ressources du réseau et aux données des titulaires de carte. Vous implémentez cette exigence en journalisant l'accès aux composants système en activant les journaux automatiques sur les composants système.

Exigence 11 : testez régulièrement les processus et les systèmes de sécurité.
Cette exigence est implémentée avec la fonction Real-Time Compliance.

Exigence 12 : gérez une stratégie de sécurité incluant la sécurité des informations pour les employés et les sous-traitants.
Activation de modems pour les fournisseurs uniquement s'ils en ont besoin, avec désactivation immédiate après utilisation. Vous pouvez implémenter cette exigence en désactivant la connexion root à distance, qu'un administrateur système pourra implémenter à la demande, puis désactiver lorsqu'elle n'est plus requise.

PowerSC Standard Edition réduit la gestion des configurations requise pour satisfaire les instructions définies par la version 2.0 et la version 3.0 du standard PCI-DSS. Cependant, le processus ne peut pas être automatisé dans son intégralité.

Par exemple, vous ne pouvez pas automatiser la restriction de l'accès aux données du titulaire de la carte en fonction de l'exigence d'affaires. Le système d'exploitation AIX met à disposition des technologies de sécurité puissantes telles que le contrôle d'accès basé sur les rôles (RBAC) ; toutefois, PowerSC Standard Edition ne peut pas automatiser cette configuration car il ne peut pas identifier les individus qui ont besoin d'un accès et ceux qui n'en ont pas besoin. IBM Compliance Expert peut automatiser la configuration d'autres paramètres de sécurité qui sont cohérents avec les exigences PCI.

Lorsque le profil PCI est appliqué à un environnement de base de données, plusieurs ports TCP et UDP qui sont utilisés par la pile de logiciels sont désactivés conformément aux restrictions. Vous devez activer ces ports et désactiver la fonction Trusted Execution afin d'exécuter l'application et la charge de travail. Exécutez les commandes suivantes pour supprimer les restrictions relatives aux ports et désactiver la fonction Trusted Execution :

```
trustchk -p TE=OFF
tcptr -delete 9091 65535
tcptr -delete 9090 9090
tcptr -delete 112 9089
tcptr -add 9091 65535 1024 1
```

Remarque : Tous les fichiers script personnalisés qui sont fournis pour gérer la conformité au standard PCI-DSS se trouvent dans le répertoire `/etc/security/pscexpert/bin`.

Le tableau ci-dessous montre comment PowerSC Standard Edition traite les exigences du standard PCI-DSS en utilisant les fonctions de l'utilitaire AIX Security Expert.

Tableau 7. Paramètres liés au standard PCI-DSS version 2.0 et version 3.0

Implémente ces standards PCI-DSS	Spécification d'implémentation	L'implémentation AIX Security Expert	Emplacement du script qui modifie la valeur
2.1	Changez systématiquement les valeurs par défaut définies par le fournisseur avant d'installer un système sur le réseau. Par exemple, incluez des mots de passe et des noms de communauté de protocole SNMP (Simple Network Management Protocol), et supprimez les comptes inutiles.	Définit le nombre minimal de semaines devant s'écouler avant que vous ne changiez un mot de passe à 0 en associant le paramètre **minage** à la valeur 0.	/etc/security/pscexpert/bin/chusrattr
PCI version 2 8.5.9 **PCI version 3** 8.2.4	Les mots de passe utilisateur doivent être changés tous les 90 jours au moins.	Définit le nombre maximal de semaines pendant lequel un mot de passe est valide à 13 en associant le paramètre **maxage** à la valeur 13.	/etc/security/pscexpert/bin/chusrattr
2.1	Changez systématiquement les valeurs par défaut définies par le fournisseur avant d'installer un système sur le réseau. Par exemple, incluez des mots de passe et des noms de communauté de protocole SNMP (Simple Network Management Protocol), et supprimez les comptes inutiles.	Définit le nombre de semaines pendant lequel un compte dont le mot de passe est arrivé à expiration est conservé sur le système à 8 en associant le paramètre **maxexpired** à la valeur 8.	/etc/security/pscexpert/bin/chusrattr
PCI version 2 8.5.10 **PCI version 3** 8.2.3	La longueur minimale d'un mot de passe est de 7 caractères.	Définit la longueur minimale d'un mot de passe à 7 caractères en associant le paramètre **minlen** à la valeur 7.	/etc/security/pscexpert/bin/chusrattr
PCI version 2 8.5.11 **PCI version 3** 8.2.3	Utilisez des mots de passe contenant des caractères numériques et des caractères alphabétiques.	Définit le nombre minimal de caractères alphabétiques requis dans un mot de passe à 1. Ce paramètre garantit que le mot de passe contient des caractères alphabétiques en associant le paramètre **minalpha** à la valeur 1.	/etc/security/pscexpert/bin/chusrattr
PCI version 2 8.5.11 **PCI version 3** 8.2.3	Utilisez des mots de passe contenant des caractères numériques et des caractères alphabétiques.	Définit le nombre minimal de caractères non-alphabétiques requis dans un mot de passe à 1. Ce paramètre garantit que le mot de passe contient des caractères non-alphabétiques en associant le paramètre **minother** à la valeur 1.	/etc/security/pscexpert/bin/chusrattr

Tableau 7. Paramètres liés au standard PCI-DSS version 2.0 et version 3.0 (suite)

Implémente ces standards PCI-DSS	Spécification d'implémentation	L'implémentation AIX Security Expert	Emplacement du script qui modifie la valeur
PCI version 2 2.1 **PCI version 3** 8.2.2	Changez systématiquement les valeurs par défaut définies par le fournisseur avant d'installer un système sur le réseau. Par exemple, incluez des mots de passe et des noms de communauté de protocole SNMP (Simple Network Management Protocol), et supprimez les comptes inutiles.	Définit le nombre maximal de fois qu'un caractère peut être répété dans un mot de passe à 8 en associant le paramètre **maxrepeats** à la valeur 8. Ce paramètre indique qu'un caractère dans un mot de passe peut être répété un nombre illimité de fois s'il respecte les autres limitations relatives aux mots de passe.	`/etc/security/pscexpert/bin/chusrattr`
PCI version 2 8.5.12 **PCI version 3** 8.2.5	Un individu ne doit pas pouvoir soumettre un nouveau mot de passe s'il est identique à l'un des quatre mots de passe précédents qu'il a utilisé.	Définit le nombre de semaines devant s'écouler avant qu'un mot de passe ne puisse être réutilisé à 52 en associant le paramètre **histexpire** à la valeur 52.	`/etc/security/pscexpert/bin/chusrattr`
PCI version 2 8.5.12 **PCI version 3** 8.2.5	Un individu ne doit pas pouvoir soumettre un nouveau mot de passe s'il est identique à l'un des quatre mots de passe précédents qu'il a utilisé.	Définit le nombre de mots de passe précédents que vous ne pouvez pas réutiliser à 4 en associant le paramètre **histsize** à la valeur 4.	`/etc/security/pscexpert/bin/chusrattr`
PCI version 2 8.5.13 **PCI version 3** 10.2.4	Les tentatives d'accès répétées doivent être limitées via le verrouillage de l'ID utilisateur après six échecs.	Définit le nombre d'échecs de tentative de connexion qui désactive un compte à 6 pour chaque compte non root en associant le paramètre **loginentries** à la valeur 6.	`/etc/security/pscexpert/bin/chusrattr`
PCI version 2 8.5.13 **PCI version 3** 10.2.4	Les tentatives d'accès répétées doivent être limitées via le verrouillage de l'ID utilisateur après six échecs.	Définit le nombre d'échecs de connexion consécutifs qui désactive un port à 6 en associant le paramètre **logindisable** à la valeur 6.	• `/etc/security/pscexpert/bin/chdefstanza` • `/etc/security/login.cfg`
PCI version 2 8.5.14 **PCI version 3** 10.2.4	La durée de verrouillage doit être de 30 minutes ou le verrouillage peut durer jusqu'à ce qu'un administrateur active l'ID utilisateur.	Définit la durée pendant laquelle un port est verrouillé après sa désactivation conformément à l'attribut *logindisable* à 30 minutes en associant le paramètre **loginreenable** à la valeur 30.	• `/etc/security/pscexpert/bin/chdefstanza` • `/etc/security/login.cfg`
12.3.9	Activation de technologies d'accès distant pour les fournisseurs et les partenaires commerciaux uniquement lorsque requis par les fournisseurs et les partenaires commerciaux, avec désactivation immédiate après utilisation.	Désactive la fonction de connexion root à distance en définissant la valeur false. L'administrateur système peut activer la fonction de connexion à distance selon les besoins, puis la désactiver une fois la tâche terminée.	• `/etc/security/pscexpert/bin/chuserstanza` • `/etc/security/user`
8.1	Affectez à tous les utilisateurs un ID unique avant de les autoriser à accéder à des composants système ou à des données de titulaire de carte.	Active la fonction qui garantit que tous les utilisateurs possèdent un nom d'utilisateur unique avant d'accéder à des composants système ou aux données d'un titulaire de carte en définissant la valeur true.	• `/etc/security/pscexpert/bin/chuserstanza` • `/etc/security/user`

Tableau 7. Paramètres liés au standard PCI-DSS version 2.0 et version 3.0 (suite)

Implémente ces standards PCI-DSS	Spécification d'implémentation	L'implémentation AIX Security Expert	Emplacement du script qui modifie la valeur
10.2	Activez la fonction d'audit sur le système.	Active la fonction d'audit des fichiers binaires sur le système.	/etc/security/pscexpert/bin/pciaudit
PCI version 2 1.1.5 2.2.2 **PCI version 3** 2.2.2	Désactivez les services inutiles et non sécurisés, notamment le démon lpd.	Arrête le démon lpd et met en commentaire l'entrée correspondante dans le fichier /etc/inittab qui démarre automatiquement le démon.	/etc/security/pscexpert/bin/comntrows
PCI version 2 1.1.5 2.2.2 **PCI version 3** 2.2.2	Désactivez les services inutiles et non sécurisés, notamment l'environnement CDE (Common Desktop Environment).	Désactive la fonction CDE lorsque LFT (Layer Four Traceroute) n'est pas configuré.	/etc/security/pscexpert/bin/comntrows
PCI version 2 1.1.5 2.2.2 **PCI version 3** 2.2.2	Désactivez les services inutiles et non sécurisés, notamment le démon timed.	Arrête le démon timed et met en commentaire l'entrée correspondante dans le fichier /etc/rc.tcpip qui démarre automatiquement le démon.	/etc/security/pscexpert/bin/rctcpip
PCI version 2 1.1.5 2.2.2 **PCI version 3** 2.2.2	Désactivez les services inutiles et non sécurisés, notamment le démon NTP.	Arrête le démon NTP et met en commentaire l'entrée correspondante dans le fichier /etc/rc.tcpip qui démarre automatiquement le démon.	/etc/security/pscexpert/bin/rctcpip
PCI version 2 1.1.5 2.2.2 **PCI version 3** 2.2.2	Désactivez les services inutiles et non sécurisés, notamment le démon rwhod.	Arrête le démon rwhod et met en commentaire l'entrée correspondante dans le fichier /etc/rc.tcpip qui démarre automatiquement le démon.	/etc/security/pscexpert/bin/rctcpip
PCI version 2 2.1 **PCI version 3** 2.1.1	Changez les valeurs par défaut définies par le fournisseur avant d'installer un système sur le réseau ; désactivez notamment le démon SNMP.	Arrête le démon SNMP et met en commentaire l'entrée correspondante dans le fichier /etc/rc.tcpip qui démarre automatiquement le démon.	/etc/security/pscexpert/bin/rctcpip
PCI version 2 2.1 **PCI version 3** 2.1.1	Changez les valeurs par défaut définies par le fournisseur avant d'installer un système sur le réseau ; désactivez notamment le démon SNMPMIBD.	Désactive le démon SNMPMIBD en mettant en commentaire l'entrée correspondante dans le fichier /etc/rc.tcpip qui démarre automatiquement le démon.	/etc/security/pscexpert/bin/rctcpip
2.1	Changez les valeurs par défaut définies par le fournisseur avant d'installer un système sur le réseau ; désactivez notamment le démon AIXMIBD.	Désactive le démon AIXMIBD en mettant en commentaire l'entrée correspondante dans le fichier /etc/rc.tcpip qui démarre automatiquement le démon.	/etc/security/pscexpert/bin/rctcpip

Tableau 7. Paramètres liés au standard PCI-DSS version 2.0 et version 3.0 (suite)

Implémente ces standards PCI-DSS	Spécification d'implémentation	L'implémentation AIX Security Expert	Emplacement du script qui modifie la valeur
2.1	Changez les valeurs par défaut définies par le fournisseur avant d'installer un système sur le réseau ; désactivez notamment le démon HOSTMIBD.	Désactive le démon HOSTMIBD en mettant en commentaire l'entrée correspondante dans le fichier /etc/rc.tcpip qui démarre automatiquement le démon.	/etc/security/pscexpert/bin/rctcpip
PCI version 2 1.1.5 2.2.2 **PCI version 3** 2.2.2	Désactivez les services inutiles et non sécurisés, notamment le démon DPID2.	Arrête le démon DPID2 et met en commentaire l'entrée correspondante dans le fichier /etc/rc.tcpip qui démarre automatiquement le démon.	/etc/security/pscexpert/bin/rctcpip
PCI version 2 2.1 **PCI version 3** 2.2.2	Changez les valeurs par défaut définies par le fournisseur avant d'installer un système sur le réseau ; arrêtez notamment le serveur DHCP.	Désactive le serveur DHCP.	/etc/security/pscexpert/bin/rctcpip
PCI version 2 1.1.5 2.2.2 **PCI version 3** 2.2.2	Désactivez les services inutiles et non sécurisés, notamment l'agent DHCP.	Arrête et désactive l'agent de relais DHCP et met en commentaire l'entrée correspondante dans le fichier /etc/rc.tcpip qui démarre automatiquement l'agent.	/etc/security/pscexpert/bin/rctcpip
PCI version 2 1.1.5 2.2.2 **PCI version 3** 2.2.2	Désactivez les services inutiles et non sécurisés, notamment le démon rshd.	Arrête et désactive toutes les instances du démon rshd ainsi que le service shell et met en commentaire les entrées correspondantes dans le fichier /etc/inetd.conf qui démarrent automatiquement les instances.	/etc/security/pscexpert/bin/cominetdconf
PCI version 2 1.1.5 2.2.2 **PCI version 3** 2.2.2	Désactivez les services inutiles et non sécurisés, notamment le démon rlogind.	Arrête et désactive toutes les instances du démon rlogind et du service rlogin. L'utilitaire AIX Security Expert met également en commentaire les entrées correspondantes dans le fichier /etc/inetd.conf qui démarrent automatiquement les instances.	/etc/security/pscexpert/bin/cominetdconf
PCI version 2 1.1.5 2.2.2 **PCI version 3** 2.2.2	Désactivez les services inutiles et non sécurisés, notamment le démon rexecd.	Arrête et désactive toutes les instances du démon rexecd. L'utilitaire AIX Security Expert met également en commentaire l'entrée correspondante dans le fichier /etc/inetd.conf qui démarre automatiquement le démon.	/etc/security/pscexpert/bin/cominetdconf
PCI version 2 1.1.5 2.2.2 **PCI version 3** 2.2.2	Désactivez les services inutiles et non sécurisés, notamment le démon comsat.	Arrête et désactive toutes les instances du démon comsat. L'utilitaire AIX Security Expert met également en commentaire l'entrée correspondante dans le fichier /etc/inetd.conf qui démarre automatiquement le démon.	/etc/security/pscexpert/bin/cominetdconf

Tableau 7. Paramètres liés au standard PCI-DSS version 2.0 et version 3.0 (suite)

Implémente ces standards PCI-DSS	Spécification d'implémentation	L'implémentation AIX Security Expert	Emplacement du script qui modifie la valeur
PCI version 2 1.1.5 2.2.2 **PCI version 3** 2.2.2	Désactivez les services inutiles et non sécurisés, notamment le démon `fingerd`.	Arrête et désactive toutes les instances du démon `fingerd`. L'utilitaire AIX Security Expert met également en commentaire l'entrée correspondante dans le fichier `/etc/inetd.conf` qui démarre automatiquement le démon.	`/etc/security/pscexpert/bin/cominetdconf`
PCI version 2 1.1.5 2.2.2 **PCI version 3** 2.2.2	Désactivez les services inutiles et non sécurisés, notamment le démon `systat`.	Arrête et désactive toutes les instances du démon `systat`. L'utilitaire AIX Security Expert met également en commentaire l'entrée correspondante dans le fichier `/etc/inetd.conf` qui démarre automatiquement le démon.	`/etc/security/pscexpert/bin/cominetdconf`
2.1	Changez les valeurs par défaut définies par le fournisseur avant d'installer un système sur le réseau ; désactivez notamment la commande `netstat`.	Désactive la commande `netstat` en mettant en commentaire l'entrée correspondante dans le fichier `/etc/inetd.conf`.	`/etc/security/pscexpert/bin/cominetdconf`
PCI version 2 1.1.5 2.2.2 **PCI version 3** 2.2.3	Désactivez les services inutiles et non sécurisés, notamment le démon `tftp`.	Arrête et désactive toutes les instances du démon `tftp`. L'utilitaire AIX Security Expert met également en commentaire l'entrée correspondante dans le fichier `/etc/inetd.conf` qui démarre automatiquement le démon.	`/etc/security/pscexpert/bin/cominetdconf`
PCI version 2 1.1.5 2.2.2 **PCI version 3** 2.2.2	Désactivez les services inutiles et non sécurisés, notamment le démon `talkd`.	Arrête et désactive toutes les instances du démon `talkd`. L'utilitaire AIX Security Expert met également en commentaire l'entrée correspondante dans le fichier `/etc/inetd.conf` qui démarre automatiquement le démon.	`/etc/security/pscexpert/bin/cominetdconf`
PCI version 2 1.1.5 2.2.2 **PCI version 3** 2.2.2	Désactivez les services inutiles et non sécurisés, notamment le démon `rquotad`.	Arrête et désactive toutes les instances du démon `rquotad`. L'utilitaire AIX Security Expert met également en commentaire l'entrée correspondante dans le fichier `/etc/inetd.conf` qui démarre automatiquement le démon.	`/etc/security/pscexpert/bin/cominetdconf`
PCI version 2 1.1.5 2.2.2 **PCI version 3** 2.2.2	Désactivez les services inutiles et non sécurisés, notamment le démon `rstatd`.	Arrête et désactive toutes les instances du démon `rstatd`. L'utilitaire AIX Security Expert met également en commentaire l'entrée correspondante dans le fichier `/etc/inetd.conf` qui démarre automatiquement le démon.	`/etc/security/pscexpert/bin/cominetdconf`

Tableau 7. Paramètres liés au standard PCI-DSS version 2.0 et version 3.0 (suite)

Implémente ces standards PCI-DSS	Spécification d'implémentation	L'implémentation AIX Security Expert	Emplacement du script qui modifie la valeur
PCI version 2 1.1.5 2.2.2 **PCI version 3** 2.2.2	Désactivez les services inutiles et non sécurisés, notamment le démon `rusersd`.	Arrête et désactive toutes les instances du démon `rusersd`. L'utilitaire AIX Security Expert met également en commentaire l'entrée correspondante dans le fichier `/etc/inetd.conf` qui démarre automatiquement le démon.	`/etc/security/pscexpert/bin/cominetdconf`
PCI version 2 1.1.5 2.2.2 **PCI version 3** 2.2.2	Désactivez les services inutiles et non sécurisés, notamment le démon `rwalld`.	Arrête et désactive toutes les instances du démon `rwalld`. L'utilitaire AIX Security Expert met également en commentaire l'entrée correspondante dans le fichier `/etc/inetd.conf` qui démarre automatiquement le démon.	`/etc/security/pscexpert/bin/cominetdconf`
PCI version 2 1.1.5 2.2.2 **PCI version 3** 2.2.2	Désactivez les services inutiles et non sécurisés, notamment le démon `sprayd`.	Arrête et désactive toutes les instances du démon `sprayd`. L'utilitaire AIX Security Expert met également en commentaire l'entrée correspondante dans le fichier `/etc/inetd.conf` qui démarre automatiquement le démon.	`/etc/security/pscexpert/bin/cominetdconf`
PCI version 2 1.1.5 2.2.2 **PCI version 3** 2.2.2	Désactivez les services inutiles et non sécurisés, notamment le démon `pcnfsd`.	Arrête et désactive toutes les instances du démon `pcnfsd`. L'utilitaire AIX Security Expert met également en commentaire l'entrée correspondante dans le fichier `/etc/inetd.conf` qui démarre automatiquement le démon.	`/etc/security/pscexpert/bin/cominetdconf`
PCI version 2 1.1.5 2.2.2 **PCI version 3** 2.2.2	Désactivez les services inutiles et non sécurisés, notamment le service `TCP echo`.	Arrête et désactive toutes les instances du service `echo(tcp)`. L'utilitaire AIX Security Expert met également en commentaire l'entrée correspondante dans le fichier `/etc/inetd.conf` qui démarre automatiquement le service.	`/etc/security/pscexpert/bin/cominetdconf`
PCI version 2 1.1.5 2.2.2 **PCI version 3** 2.2.2	Désactivez les services inutiles et non sécurisés, notamment le service `TCP discard`.	Arrête et désactive toutes les instances du service `discard(tcp)`. L'utilitaire AIX Security Expert met également en commentaire l'entrée correspondante dans le fichier `/etc/inetd.conf` qui démarre automatiquement le service.	`/etc/security/pscexpert/bin/cominetdconf`
PCI version 2 1.1.5 2.2.2 **PCI version 3** 2.2.2	Désactivez les services inutiles et non sécurisés, notamment le service `TCP chargen`.	Arrête et désactive toutes les instances du service `chargen(tcp)`. L'utilitaire AIX Security Expert met également en commentaire l'entrée correspondante dans le fichier `/etc/inetd.conf` qui démarre automatiquement le service.	`/etc/security/pscexpert/bin/cominetdconf`

Tableau 7. Paramètres liés au standard PCI-DSS version 2.0 et version 3.0 (suite)

Implémente ces standards PCI-DSS	Spécification d'implémentation	L'implémentation AIX Security Expert	Emplacement du script qui modifie la valeur
PCI version 2 1.1.5 2.2.2 **PCI version 3** 2.2.2	Désactivez les services inutiles et non sécurisés, notamment le service TCP `daytime`.	Arrête et désactive toutes les instances du service `daytime(tcp)`. L'utilitaire AIX Security Expert met également en commentaire l'entrée correspondante dans le fichier `/etc/inetd.conf` qui démarre automatiquement le service.	`/etc/security/pscexpert/bin/cominetdconf`
PCI version 2 1.1.5 2.2.2 **PCI version 3** 2.2.2	Désactivez les services inutiles et non sécurisés, notamment le service TCP `time`.	Arrête et désactive toutes les instances du service `timed(tcp)`. L'utilitaire AIX Security Expert met également en commentaire l'entrée correspondante dans le fichier `/etc/inetd.conf` qui démarre automatiquement le service.	`/etc/security/pscexpert/bin/cominetdconf`
PCI version 2 1.1.5 2.2.2 **PCI version 3** 2.2.2	Désactivez les services inutiles et non sécurisés, notamment le service UDP `echo`.	Arrête et désactive toutes les instances du service `echo(udp)`. L'utilitaire AIX Security Expert met également en commentaire l'entrée correspondante dans le fichier `/etc/inetd.conf` qui démarre automatiquement le service.	`/etc/security/pscexpert/bin/cominetdconf`
PCI version 2 1.1.5 2.2.2 **PCI version 3** 2.2.2	Désactivez les services inutiles et non sécurisés, notamment le service UDP `discard`.	Arrête et désactive toutes les instances du service `discard(udp)`. L'utilitaire AIX Security Expert met également en commentaire l'entrée correspondante dans le fichier `/etc/inetd.conf` qui démarre automatiquement le service.	`/etc/security/pscexpert/bin/cominetdconf`
PCI version 2 1.1.5 2.2.2 **PCI version 3** 2.2.2	Désactivez les services inutiles et non sécurisés, notamment le service UDP `chargen`.	Arrête et désactive toutes les instances du service `chargen(udp)`. L'utilitaire AIX Security Expert met également en commentaire l'entrée correspondante dans le fichier `/etc/inetd.conf` qui démarre automatiquement le service.	`/etc/security/pscexpert/bin/cominetdconf`
PCI version 2 1.1.5 2.2.2 **PCI version 3** 2.2.2	Désactivez les services inutiles et non sécurisés, notamment le service UDP `daytime`.	Arrête et désactive toutes les instances du service `daytime(udp)`. L'utilitaire AIX Security Expert met également en commentaire l'entrée correspondante dans le fichier `/etc/inetd.conf` qui démarre automatiquement le service.	`/etc/security/pscexpert/bin/cominetdconf`
PCI version 2 1.1.5 2.2.2 **PCI version 3** 2.2.2	Désactivez les services inutiles et non sécurisés, notamment le service UDP `time`.	Arrête et désactive toutes les instances du service `timed(udp)`. L'utilitaire AIX Security Expert met également en commentaire l'entrée correspondante dans le fichier `/etc/inetd.conf` qui démarre automatiquement le service.	`/etc/security/pscexpert/bin/cominetdconf`

Tableau 7. Paramètres liés au standard PCI-DSS version 2.0 et version 3.0 (suite)

Implémente ces standards PCI-DSS	Spécification d'implémentation	L'implémentation AIX Security Expert	Emplacement du script qui modifie la valeur
PCI version 2 1.1.5 2.2.2 **PCI version 3** 2.2.3	Désactivez les services inutiles et non sécurisés, notamment le service `FTP`.	Arrête et désactive toutes les instances du démon `ftpd`. L'utilitaire AIX Security Expert met également en commentaire l'entrée correspondante dans le fichier `/etc/inetd.conf` qui démarre automatiquement le démon.	`/etc/security/pscexpert/bin/cominetdconf`
PCI version 2 1.1.5 2.2.2 **PCI version 3** 2.2.3	Désactivez les services inutiles et non sécurisés, notamment le service `telnet`.	Arrête et désactive toutes les instances du démon `telnetd`. L'utilitaire AIX Security Expert met également en commentaire l'entrée correspondante dans le fichier `/etc/inetd.conf` qui démarre automatiquement le démon.	`/etc/security/pscexpert/bin/cominetdconf`
PCI version 2 1.1.5 2.2.2 **PCI version 3** 2.2.2	Désactivez les services inutiles et non sécurisés, notamment `dtspc`.	Arrête et désactive toutes les instances du démon `dtspc`. AIX Security Expert met également en commentaire l'entrée correspondante dans le fichier `/etc/inittab` qui démarre automatiquement le démon lorsque LFT n'est pas configuré et que l'environnement CDE est désactivé dans le fichier `/etc/inittab`.	`/etc/security/pscexpert/bin/cominetdconf`
PCI version 2 1.1.5 2.2.2 **PCI version 3** 2.2.2	Désactivez les services inutiles et non sécurisés, notamment le service `ttdbserver`.	Arrête et désactive toutes les instances du service `ttdbserver`. L'utilitaire AIX Security Expert met également en commentaire l'entrée correspondante dans le fichier `/etc/inetd.conf` qui démarre automatiquement le service.	`/etc/security/pscexpert/bin/cominetdconf`
PCI version 2 1.1.5 2.2.2 **PCI version 3** 2.2.2	Désactivez les services inutiles et non sécurisés, notamment le service `cmsd`.	Arrête et désactive toutes les instances du service `cmsd`. L'utilitaire AIX Security Expert met également en commentaire l'entrée correspondante dans le fichier `/etc/inetd.conf` qui démarre automatiquement le service.	`/etc/security/pscexpert/bin/cominetdconf`
PCI version 2 2.2.3 **PCI version 3** 2.2.4	Configurez les paramètres de sécurité du système pour empêcher toute mauvaise utilisation.	Supprime les commandes Set User ID (SUID) en mettant en commentaire l'entrée correspondante dans le fichier `/etc/inetd.conf` qui active automatiquement les commandes.	`/etc/security/pscexpert/bin/rmsuidfrmrcmds`
PCI version 2 2.2.3 **PCI version 3** 2.2.4	Configurez les paramètres de sécurité du système pour empêcher toute mauvaise utilisation.	Active le niveau de sécurité le plus bas pour le gestionnaire des droits d'accès aux fichiers.	`/etc/security/pscexpert/bin/filepermgr`

Tableau 7. Paramètres liés au standard PCI-DSS version 2.0 et version 3.0 (suite)

Implémente ces standards PCI-DSS	Spécification d'implémentation	L'implémentation AIX Security Expert	Emplacement du script qui modifie la valeur
PCI version 2 2.2.3 **PCI version 3** 2.2.4	Configurez les paramètres de sécurité du système pour empêcher toute mauvaise utilisation.	Modifie le protocole NFS (Network File System) avec des paramètres restreints conformes aux exigences de sécurité PCI. Ces paramètres restreints incluent la désactivation des droits d'accès de l'utilisateur root à distance ainsi que l'accès des ID utilisateur et des ID groupe anonyme.	`/etc/security/pscexpert/bin/nfsconfig`
PCI version 2 2.2.2 **PCI version 3** 2.2.3	Activez uniquement les services, les protocoles, les démons, etc., nécessaires et sécurisés, selon les besoins pour la fonction appropriée sur le système. Implémentez des fonctions de sécurité pour les services, protocoles ou démons requis considérés comme non sécurisés.	Désactive les démons `rlogind`, `rshd` et `tftpd`, qui ne sont pas sécurisés.	`/etc/security/pscexpert/bin/disrmtdmns`
PCI version 2 2.2.2 **PCI version 3** 2.2.3	Activez uniquement les services, les protocoles, les démons, etc., nécessaires et sécurisés, selon les besoins pour la fonction appropriée sur le système. Implémentez des fonctions de sécurité pour les services, protocoles ou démons requis considérés comme non sécurisés.	Désactive les démons `rlogind`, `rshd` et `tftpd`, qui ne sont pas sécurisés.	`/etc/security/pscexpert/bin/rmrhostsnetrc`
PCI version 2 2.2.2 **PCI version 3** 2.2.3	Activez uniquement les services, les protocoles, les démons, etc., nécessaires et sécurisés, selon les besoins pour la fonction appropriée sur le système. Implémentez des fonctions de sécurité pour les services, protocoles ou démons requis considérés comme non sécurisés.	Désactive les démons `logind`, `rshd` et `tftpdpci_rmetchostsequiv`, qui ne sont pas sécurisés.	`/etc/security/pscexpert/bin/rmetchostsequiv`
PCI version 2 1.3.6 **PCI version 3** 2.2.3	Implémentez l'inspection avec état ou le filtrage de paquets, où seules les connexions établies sont autorisées sur le réseau.	Active l'option de réseau **`clean_partial_conns`** en définissant la valeur 1.	`/etc/security/pscexpert/bin/ntwkopts`
PCI version 2 2.2.2 **PCI version 3** 2.2.3	Implémentez l'inspection avec état ou le filtrage de paquets, où seules les connexions établies sont autorisées sur le réseau.	Active la sécurité TCP en associant l'option de réseau **`tcp_tcpsecure`** à la valeur 7. Ce paramètre fournit une protection des données contre les attaques de type réinitialisation (RST) et demande de connexion TCP (SYN).	`/etc/security/pscexpert/bin/ntwkopts`

Tableau 7. Paramètres liés au standard PCI-DSS version 2.0 et version 3.0 (suite)

Implémente ces standards PCI-DSS	Spécification d'implémentation	L'implémentation AIX Security Expert	Emplacement du script qui modifie la valeur
1.2	Assurez la protection des accès non autorisés aux ports inutilisés.	Configure le système pour qu'il évite les hôtes pendant 5 minutes afin d'empêcher que d'autres systèmes accèdent à des ports inutilisés.	`/etc/security/pscexpert/bin/ipsecshunhosthls` **Remarque :** Vous pouvez entrer des règles de filtrage supplémentaires dans le fichier `/etc/security/aixpert/bin/filter.txt`. Ces règles sont intégrées par le script `ipsecshunhosthls.sh` lorsque vous appliquez le profil. Le format des entrées doit être le suivant : *numéro_port*:*adresse_ip*:*action* où les valeurs possibles pour *action* sont `Allow` et `Deny`.
1.2	Protégez l'hôte des analyses de port.	Configure le système pour qu'il évite les ports vulnérables pendant 5 minutes, ce qui empêche les analyses de port.	`/etc/security/pscexpert/bin/ipsecshunports` **Remarque :** Vous pouvez entrer des règles de filtrage supplémentaires dans le fichier `/etc/security/aixpert/bin/filter.txt`. Ces règles sont intégrées par le script `ipsecshunhosthls.sh` lorsque vous appliquez le profil. Le format des entrées doit être le suivant : *numéro_port*:*adresse_ip*:*action* où les valeurs possibles pour *action* sont `Allow` et `Deny`.
1.2	Limitez les droits de création d'objet.	Définit les droits de création d'objet par défaut 22 en associant le paramètre **umask** à la valeur 22.	`/etc/security/pscexpert/bin/chusrattr`
1.2	Limitez l'accès au système.	Assurez-vous que l'ID root est le seul répertorié dans le fichier `cron.allow` et supprimez le fichier `cron.deny` du système.	`/etc/security/pscexpert/bin/limitsysacc`
6.5.8	Supprimez les points du chemin racine.	Supprime les points de la variable d'environnement PATH dans les fichiers suivants, qui se trouvent dans le répertoire de base racine : • .cshrc • .kshrc • .login • .profile	`/etc/security/pscexpert/bin/rmdotfrmpathroot`
6.5.8	Supprimez les points du chemin non racine :	Supprimez les points de la variable d'environnement *PATH* dans les fichiers suivants qui se trouvent dans le répertoire de base de l'utilisateur : • .cshrc • .kshrc • .login • .profile	`/etc/security/pscexpert/bin/rmdotfrmpathnroot`
2.2.3	Limitez l'accès au système.	Ajoute la fonction utilisateur root et le nom d'utilisateur dans le fichier `/etc/ftpusers`.	`/etc/security/pscexpert/bin/chetcftpusers`

Tableau 7. Paramètres liés au standard PCI-DSS version 2.0 et version 3.0 (suite)

Implémente ces standards PCI-DSS	Spécification d'implémentation	L'implémentation AIX Security Expert	Emplacement du script qui modifie la valeur
2.1	Supprimez le compte invité.	Supprime le compte invité et ses fichiers.	`/etc/security/pscexpert/bin/execmds`
6.5.2	Empêchez le lancement de programmes dans l'espace de contenu.	Active la fonction SED (Stack Execution Disable).	`/etc/security/pscexpert/bin/sedconfig`
8.2	Vérifiez que le mot de passe pour root n'est pas faible.	Démarrez un contrôle d'intégrité du mot de passe root afin de garantir que le mot de passe root est fort.	`/etc/security/pscexpert/bin/chuserstanza`
PCI version 2 8.5.15 **PCI version 3** 8.1.8	Limitez l'accès au système en définissant le délai d'inactivité de session.	Définit le délai d'inactivité maximal à 15 minutes. Si la session est inactive pendant plus de 15 minutes, vous devez entrer à nouveau le mot de passe.	`/etc/security/pscexpert/bin/autologoff`
1.3.5	Limitez l'accès du trafic aux informations sur les titulaires de carte.	Définit la régulation de trafic TCP élevée, qui impose l'atténuation de refus de service sur les ports.	`/etc/security/pscexpert/bin/tcptr_pscexpert`
1.3.5	Gérez une connexion sécurisée lors de la migration des données.	Activez la création d'un tunnel IP Security (IPSec) automatisée entre les serveurs virtuels d'E-S au cours de la migration de partition active.	`/etc/security/pscexpert/bin/cfgsecmig`
1.3.5	Limitez les paquets provenant de sources inconnues.	Autorise les paquets provenant de la console HMC.	`/etc/security/pscexpert/bin/ipsecpermithostorport`
5.1.1	Gérez le logiciel antivirus.	Assure l'intégrité du système en assurant la protection contre les types connus de logiciels malveillants, en les détectant et en les supprimant.	`/etc/security/pscexpert/bin/manageITsecurity`
PCI version 2 Section 7 **PCI version 3** Section 7	Gérez l'accès en fonction des besoins.	Active le contrôle d'accès basé sur les rôles (RBAC) en créant des rôles opérateur système, administrateur système et responsable de la sécurité du système d'information avec les droits d'accès requis.	`/etc/security/pscexpert/bin/EnableRbac`
PCI version 2 Non inclus dans la version 2 du profil, ajouté dans la version 3. **PCI version 3** 2.3	Implémentez d'autres fonctions de sécurité pour les services, protocoles ou démons requis considérés comme non sécurisés.	Utilise des technologies de sécurité telles que Secure Shell (SSH), SSH File Transfer Protocol (S-FTP), Secure Sockets Layer (SSL) ou Internet Protocol Security Virtual Private Network (IPsec VPN) pour protéger des services non sécurisés, par exemple NetBIOS, le partage de fichiers, Telnet et FTP. Configure également le démon SSH pour qu'il n'utilise que le protocole SSHv2.	`/etc/security/pscexpert/bin/sshPCIconfig`

Tableau 7. Paramètres liés au standard PCI-DSS version 2.0 et version 3.0 (suite)

Implémente ces standards PCI-DSS	Spécification d'implémentation	L'implémentation AIX Security Expert	Emplacement du script qui modifie la valeur
PCI version 2 Non inclus dans la version 2 du profil, ajouté dans la version 3. **PCI version 3** 2.3	Le client SSH doit être configuré pour n'utiliser que le protocole SSHv2.	Configure le client SSH en vue de l'utilisation du protocole SSHv2.	`/etc/security/pscexpert/bin/sshPCIconfig`
PCI version 2 Non inclus dans la version 2 du profil, ajouté dans la version 3. **PCI version 3** 2.3	Le démon SSH doit être à l'écoute uniquement sur les adresses de réseau de gestion sauf s'il est autorisé pour des utilisations autres que la gestion.	Garantit que le démon SSH est configuré uniquement pour l'écoute.	`/etc/security/pscexpert/bin/sshPCIconfig`
PCI version 2 Non inclus dans la version 2 du profil, ajouté dans la version 3. **PCI version 3** 2.3	Le démon SSH doit être configuré pour n'utiliser que les chiffrements approuvés par la norme FIPS 140-2.	Garantit que le démon SSH utilise uniquement les chiffrements de la norme FIPS 140-2.	`/etc/security/pscexpert/bin/sshPCIconfig`
PCI version 2 Non inclus dans la version 2 du profil, ajouté dans la version 3. **PCI version 3** 2.3	Le démon SSH doit être configuré pour n'utiliser que les codes d'authentification de message qui emploient des algorithmes de hachage cryptographique approuvés par la norme FIPS 140-2.	Garantit que les codes d'authentification de message exécutent les algorithmes approuvés.	`/etc/security/pscexpert/bin/sshPCIconfig`
PCI version 2 Non inclus dans la version 2 du profil, ajouté dans la version 3. **PCI version 3** 2.3	Le démon SSH doit restreindre la possibilité de connexion à des utilisateurs ou des groupes spécifiques.	Restreint la connexion au système à des utilisateurs et des groupes spécifiques.	`/etc/security/pscexpert/bin/sshPCIconfig`

Tableau 7. Paramètres liés au standard PCI-DSS version 2.0 et version 3.0 (suite)

Implémente ces standards PCI-DSS	Spécification d'implémentation	L'implémentation AIX Security Expert	Emplacement du script qui modifie la valeur
PCI version 2 Non inclus dans la version 2 du profil, ajouté dans la version 3. **PCI version 3** 2.3	Le système doit afficher la date et l'heure de la dernière connexion au compte réussie lors de la connexion.	Gère les informations de la dernière connexion réussie et les affiche en cas de nouvelle connexion réussie.	`/etc/security/pscexpert/bin/sshPCIconfig`
PCI version 2 Non inclus dans la version 2 du profil, ajouté dans la version 3. **PCI version 3** 2.3	Le démon SSH doit effectuer une vérification en mode strict des fichiers de configuration qui se trouvent dans le répertoire de base.	Garantit que les fichiers de configuration qui se trouvent dans le répertoire de base sont associés aux modes appropriés.	`/etc/security/pscexpert/bin/sshPCIconfig`
PCI version 2 Non inclus dans la version 2 du profil, ajouté dans la version 3. **PCI version 3** 2.3	Le démon SSH doit utiliser la séparation des privilèges.	Garantit que le démon SSH utilise la séparation appropriée de ses privilèges.	`/etc/security/pscexpert/bin/sshPCIconfig`
PCI version 2 Non inclus dans la version 2 du profil, ajouté dans la version 3. **PCI version 3** 2.3	Le démon SSH ne doit pas autoriser rhosts à utiliser l'authentification RSA.	Désactive l'authentification RSA pour rhosts lorsque vous utilisez le démon SSH.	`/etc/security/pscexpert/bin/sshPCIconfig`
PCI version 2 Non inclus dans la version 2 du profil, ajouté dans la version 3. **PCI version 3** 2.3	Limitez le nombre maximal de sessions de connexion à 2 par utilisateur.	Définit le nombre maximal de sessions de connexion à 2 par utilisateur.	`/etc/security/pscexpert/bin/sshPCIconfig`
PCI version 2 1.1.5 2.2.2 **PCI version 3** 10.4	Examinez les normes et les processus de configuration afin de vérifier que la technologie de synchronisation de l'heure est implémentée et qu'elle reste à jour conformément aux exigences PCI-DSS 6.1 et 6.2.	Active le démon ntp.	`/etc/security/pscexpert/bin/rctcpip`

Tableau 7. Paramètres liés au standard PCI-DSS version 2.0 et version 3.0 (suite)

Implémente ces standards PCI-DSS	Spécification d'implémentation	L'implémentation AIX Security Expert	Emplacement du script qui modifie la valeur
PCI version 2 Non inclus dans la version 2 du profil, ajouté dans la version 3. **PCI version 3** 8.1.5	Désactivez un compte utilisateur s'il n'est pas utilisé.	Désactive les comptes utilisateur après 35 jours d'inactivité.	`/etc/security/pscexpert/bin/disableacctpci`
PCI version 2 Non inclus dans la version 2 du profil, ajouté dans la version 3. **PCI version 3** 8.2	Limitez le nombre maximal de sessions de connexion à 2 par utilisateur.	Définit le nombre maximal de sessions actives pour l'utilisateur à 2 en associant le paramètre **maxulogs** à la valeur 2.	`/etc/security/pscexpert/bin/chusrattr`

Loi Sarbanes-Oxley et conformité COBIT

La loi Sarbanes-Oxley (SOX) de 2002 établie par le 107ème congrès des Etats-Unis d'Amérique supervise l'audit des sociétés publiques soumises aux lois relatives à la sécurité, ainsi que les points afférents, afin de protéger les intérêts des investisseurs.

La section SOX 404 mandate l'évaluation de la gestion via des contrôles internes. Pour la plupart des organisations, les contrôles internes couvrent les systèmes de technologie de l'information qui traitent les données financières de la société et génèrent des rapports. La loi SOX fournit des détails spécifiques sur les technologies de l'information et la sécurité liée. La plupart des auditeurs SOX s'appuient sur des normes, telles que COBIT, comme moyen d'évaluer et d'effectuer un audit du contrôle et de la gouvernance informatique. L'option de configuration PowerSC Standard Edition SOX/COBIT XML fournit la configuration de sécurité d'AIX et du serveur d'E-S virtuel (systèmes VIOS requis pour satisfaire les instructions de conformité COBIT).

IBM Compliance Expert Express Edition s'exécute sur la version suivante du système d'exploitation AIX :

- AIX 6.1
- AIX 7.1
- AIX 7.2

L'administration système AIX est responsable de la conformité aux normes externes. IBM Compliance Expert Express Edition a été conçu pour simplifier la gestion des paramètres du système d'exploitation et des rapports qui sont requis pour la conformité aux normes.

Les profils de conformité préconfigurés distribués avec IBM Compliance Expert Express Edition réduisent la charge de travail administratif consistant à interpréter la documentation relative à la conformité et à implémenter ces normes sous forme de paramètres de configuration du système spécifiques.

Les fonctions d'IBM Compliance Expert Express Edition permettent aux clients de gérer efficacement la configuration système requise qui est associée à la conformité aux normes externes pouvant potentiellement réduire les coûts tout en améliorant la conformité. Toutes les normes de sécurité externes incluent des aspects autres que les paramètres de configuration du système. L'utilisation d'IBM Compliance Expert Express Edition ne garantit pas la conformité aux normes. Compliance Expert a été

conçu pour simplifier la gestion des paramètre de configuration des systèmes et permet aux administrateurs de se concentrer sur d'autres aspects de la conformité aux normes.

Information associée:

Conformité COBIT

La loi Health Insurance Portability and Accountability Act (HIPAA)

La loi Health Insurance Portability and Accountability Act (HIPAA) est un profil de sécurité qui assure la protection des informations de santé protégées électroniquement (EPHI).

La règle de sécurité HIPAA assure spécifiquement la protection des informations EPHI et seul un sous-ensemble des agences y sont soumises en fonction de leurs fonctions et de l'utilisation des informations EPHI.

Toutes les entités couvertes par la loi HIPAA, de même que certaines agences fédérales, doivent se conformer à la règle de sécurité HIPAA.

La règle de sécurité HIPAA assure la confidentialité, l'intégrité et la disponibilité des informations EPHI, comme défini dans la règle de sécurité.

Les informations EPHI qu'une entité couverte crée, reçoit, gère ou transmet doivent être protégées contre toute menace raisonnablement anticipée, tout danger et toute utilisation ou divulgation non autorisée.

Les exigences, normes et spécifications d'implémentation de la règle de sécurité HIPAA s'appliquent aux entités couvertes suivantes :

- Les prestataires de soins de santé
- Le système de soins médicaux
- Les clearinghouses des soins de santé
- Les ordonnances Medicare et les sponsors des cartes de paiement des médicaments

Le tableau ci-après détaille les différentes sections de la règle de sécurité HIPAA et chaque section inclut plusieurs normes et spécifications d'implémentation.

Remarque : Tous les fichiers script personnalisés qui sont fournis pour gérer la conformité à la loi HIPAA se trouvent dans le répertoire `/etc/security/pscexpert/bin`.

Tableau 8. Règles HIPAA et détails d'implémentation

Sections de la règle de sécurité HIPAA	Spécification d'implémentation	L'implémentation aixpert	Commandes et valeurs renvoyées
164.308 (a) (1) (ii) (D) 164.308 (a) (5) (ii) (C) 164.312 (b)	Implémente les procédures permettant de consulter régulièrement les enregistrements de l'activité du système d'information, comme les journaux d'audit, les rapports d'accès et les rapports sur les incidents de sécurité.	Détermine si la fonction d'audit est activée sur le système.	**Commande** : **#audit query**. **Valeur renvoyée** : si elle aboutit, cette commande renvoie la valeur 0. Si elle échoue, elle renvoie la valeur 1.

Tableau 8. Règles HIPAA et détails d'implémentation (suite)

Sections de la règle de sécurité HIPAA	Spécification d'implémentation	L'implémentation aixpert	Commandes et valeurs renvoyées
164.308 (a) (1) (ii) (D) 164.308 (a) (5) (ii) (C) 166.312 (b)	Implémente les procédures permettant de consulter régulièrement les enregistrements de l'activité du système d'information, comme les journaux d'audit, les rapports d'accès et les rapports sur les incidents de sécurité.	Active la fonction d'audit sur le système. De plus, configure les événements à capturer.	**Commande** : **# audit start >/dev/null 2>&1**. **Valeur renvoyée** : si elle aboutit, cette commande renvoie la valeur 0. Si elle échoue, elle renvoie la valeur 1. Les événements suivants sont audités : **FILE_Mknod, FILE_Open, FS_Mkdir, PROC_Execute, DEV_Create, FILE_Acl, FILE_Chpriv, FILE_Fchpriv, FILE_Mode, INIT_Start, PASSWORD_Change, PASSWORD_Check, PROC_Adjtime, PROC_Kill, PROC_Privilege, PROC_Setpgid, USER_SU, USER_Change, USER_Create, USER_Login, USER_Logout, USER_Reboot, USER_Remove, USER_SetEnv, USER_SU, FILE_Acl,FILE_Fchmod,FILE_Fchown**
164.312 (a) (2) (iV)	Chiffrement et déchiffrement (A) :Implémente un mécanisme de chiffrement et de déchiffrement des informations EPHI.	Détermine si le système de fichiers chiffrés (EFS) est activé sur le système.	**Commande** : **# efskeymgr -V >/dev/null 2>&1**. **Valeur renvoyée** : si le système de fichiers chiffrés est déjà activé, cette commande renvoie la valeur 0. S'il n'est pas activé, elle renvoie la valeur 1.
164.312 (a) (2) (iii)	Déconnexion automatique (A) : Implémente les procédures électroniques permettant de mettre fin à une session électronique après un délai d'inactivité prédéfini.	Configure le système pour qu'il se déconnecte des processus interactifs après 15 minutes d'inactivité.	**Commande** : **grep TMOUT= /etc/security /.profile > /dev/null 2>&1** **echo "TMOUT=900 ; TIMEOUT=900; export TMOUT TIMEOUT**. **Valeur renvoyée** : si la commande ne parvient pas à trouver la valeur **TMOUT=15**, le script renvoie la valeur 1. Sinon, la commande renvoie la valeur 0.
164.308 (a) (5) (ii) (D) 164.312 (a) (2) (i)	Gestion des mots de passe (A) :Implémente les procédures de création, de changement et de protection des mots de passe.	Garantit que tous les mots de passe contiennent 14 caractères au moins.	**Commande** : **chsec -f /etc/security/user -s user -a minlen=8**. **Valeur renvoyée** : s'il aboutit, ce script renvoie la valeur 0. S'il échoue, il renvoie le code d'erreur 1.
164.308 (a) (5) (ii) (D) 164.312 (a) (2) (i)	Gestion des mots de passe (A) :Implémente les procédures de création, de changement et de protection des mots de passe.	Garantit que tous les mots de passe incluent au moins deux caractères alphabétiques, dont l'un doit être en majuscule.	**Commande** : **chsec -f /etc/security/user -s user –a minalpha=4**. **Valeur renvoyée** : s'il aboutit, ce script renvoie la valeur 0. S'il échoue, il renvoie le code d'erreur 1.

Tableau 8. Règles HIPAA et détails d'implémentation (suite)

Sections de la règle de sécurité HIPAA	Spécification d'implémentation	L'implémentation aixpert	Commandes et valeurs renvoyées
164.308 (a) (5) (ii) (D) 164.312 (a) (2) (i)	Gestion des mots de passe (A) :Implémente les procédures de création, de changement et de protection des mots de passe.	Définit le nombre minimal de caractères non-alphabétiques dans un mot de passe à 2.	**Commande** : **#chsec –f /etc/security/user –s user –a minother=2**. **Valeur renvoyée** : s'il aboutit, ce script renvoie la valeur 0. S'il échoue, il renvoie le code d'erreur 1.
164.308 (a) (5) (ii) (D) 164.312 (a) (2) (i)	Gestion des mots de passe (A) :Implémente les procédures de création, de changement et de protection des mots de passe.	Garantit que les mots de passe ne contiennent pas de caractères répétés.	**Commande** : **#chsec –f /etc/security/user –s user –a maxrepeats=1**. **Valeur renvoyée** : s'il aboutit, ce script renvoie la valeur 0. S'il échoue, il renvoie le code d'erreur 1.
164.308 (a) (5) (ii) (D) 164.312 (a) (2) (i)	Gestion des mots de passe (A) :Implémente les procédures de création, de changement et de protection des mots de passe.	Garantit qu'un mot de passe n'est pas réutilisé dans le cadre des cinq derniers changements.	**Commande** : **#chsec –f /etc/security/user –s user –a histsize=5**. **Valeur renvoyée** : s'il aboutit, ce script renvoie la valeur 0. S'il échoue, il renvoie le code d'erreur 1.
164.308 (a) (5) (ii) (D) 164.312 (a) (2) (i)	Gestion des mots de passe (A) :Implémente les procédures de création, de changement et de protection des mots de passe.	Spécifie la valeur 13 pour le nombre maximal de semaines pendant lesquelles le mot de passe reste valide.	**Commande** : **#chsec –f /etc/security/user –s user –a maxage=8**. **Valeur renvoyée** : s'il aboutit, ce script renvoie la valeur 0. S'il échoue, il renvoie le code d'erreur 1.
164.308 (a) (5) (ii) (D) 164.312 (a) (2) (i)	Gestion des mots de passe (A) :Implémente les procédures de création, de changement et de protection des mots de passe.	Supprime toute exigence relative au nombre minimal de semaines au bout duquel un mot de passe peut être changé.	**Commande** : **#chsec –f /etc/security/user –s user –a minage=2**. **Valeur renvoyée** : s'il aboutit, ce script renvoie la valeur 0. S'il échoue, il renvoie le code d'erreur 1.
164.308 (a) (5) (ii) (D) 164.312 (a) (2) (i)	Gestion des mots de passe (A) :Implémente les procédures de création, de changement et de protection des mots de passe.	Spécifie la valeur 4 pour le nombre maximal de semaines pendant lesquelles vous pouvez changer un mot de passe arrivé à expiration, après l'expiration de la valeur du paramètre **maxage** définie par l'utilisateur.	**Commande** : **#chsec –f /etc/security/user –s user –a maxexpired=4**. **Valeur renvoyée** : s'il aboutit, ce script renvoie la valeur 0. S'il échoue, il renvoie le code d'erreur 1.
164.308 (a) (5) (ii) (D) 164.312 (a) (2) (i)	Gestion des mots de passe (A) :Implémente les procédures de création, de changement et de protection des mots de passe.	Spécifie la valeur 4 pour le nombre minimal de caractères ne pouvant pas être répétés et qui figurent dans l'ancien mot de passe.	**Commande** : **#chsec –f /etc/security/user –s user –a mindiff=4**. **Valeur renvoyée** : s'il aboutit, ce script renvoie la valeur 0. S'il échoue, il renvoie le code d'erreur 1.

Tableau 8. Règles HIPAA et détails d'implémentation (suite)

Sections de la règle de sécurité HIPAA	Spécification d'implémentation	L'implémentation aixpert	Commandes et valeurs renvoyées
164.308 (a) (5) (ii) (D) 164.312 (a) (2) (i)	Gestion des mots de passe (A) :Implémente les procédures de création, de changement et de protection des mots de passe.	Spécifie que le nombre de jours à attendre avant que le système n'émette un avertissement indiquant que le mot de passe doit être changé est 5.	**Commande** : **#chsec –f /etc/security/user –s user –a pwdwarntime = 5**. **Valeur renvoyée** : s'il aboutit, ce script renvoie la valeur 0. S'il échoue, il renvoie le code d'erreur 1.
164.308 (a) (5) (ii) (D) 164.312 (a) (2) (i)	Gestion des mots de passe (A) :Implémente les procédures de création, de changement et de protection des mots de passe.	Vérifie l'exactitude des définitions utilisateur et corrige les erreurs.	**Commande** : **/usr/bin/usrck -y ALL** **/usr/bin/usrck –n ALL**. **Valeur renvoyée** : la commande ne renvoie pas de valeur. Elle procède à une vérification et corrige les erreurs, le cas échéant.
164.308 (a) (5) (ii) (D) 164.312 (a) (2) (i)	Gestion des mots de passe (A) :Implémente les procédures de création, de changement et de protection des mots de passe.	Verrouille le compte après trois échecs de connexion consécutifs.	**Commande** : **#chsec –f /etc/security/user –s user –a loginretries=3**. **Valeur renvoyée** : s'il aboutit, ce script renvoie la valeur 0. S'il échoue, il renvoie le code d'erreur 1.
164.308 (a) (5) (ii) (D) 164.312 (a) (2) (i)	Gestion des mots de passe (A) :Implémente les procédures de création, de changement et de protection des mots de passe.	Spécifie la valeur de 5 secondes comme délai entre deux tentatives de connexion.	**Commande** : **chsec -f /etc/security/login.cfg -s default -a logindelay=5**. **Valeur renvoyée** : s'il aboutit, ce script renvoie la valeur 0. S'il échoue, il renvoie le code d'erreur 1.
164.308 (a) (5) (ii) (D) 164.312 (a) (2) (i)	Gestion des mots de passe (A) :Implémente les procédures de création, de changement et de protection des mots de passe.	Spécifie la valeur 10 pour le nombre d'échecs de connexion sur un port avant que le port ne soit verrouillé.	**Commande** : **chsec -f /etc/security/lastlog -s username -a \ unsuccessful_login_count=10**. **Valeur renvoyée** : s'il aboutit, ce script renvoie la valeur 0. S'il échoue, il renvoie le code d'erreur 1.
164.308 (a) (5) (ii) (D) 164.312 (a) (2) (i)	Gestion des mots de passe (A) :Implémente les procédures de création, de changement et de protection des mots de passe.	Spécifie la valeur de 60 secondes comme délai sur un port pour les échecs de connexion avant que le port ne soit désactivé.	**Commande** : **#chsec -f /etc/security/lastlog -s user –a time_last_unsuccessful_login=60**. **Valeur renvoyée** : s'il aboutit, ce script renvoie la valeur 0. S'il échoue, il renvoie le code d'erreur 1.
164.308 (a) (5) (ii) (D) 164.312 (a) (2) (i)	Gestion des mots de passe (A) :Implémente les procédures de création, de changement et de protection des mots de passe.	Spécifie la valeur de 30 minutes pour le délai au bout duquel un port est déverrouillé après sa désactivation.	**Commande** : **#chsec -f /etc/security/login.cfg -s default -a loginreenable = 30**. **Valeur renvoyée** : s'il aboutit, ce script renvoie la valeur 0. S'il échoue, il renvoie le code d'erreur 1.

Tableau 8. Règles HIPAA et détails d'implémentation (suite)

Sections de la règle de sécurité HIPAA	Spécification d'implémentation	L'implémentation aixpert	Commandes et valeurs renvoyées
164.308 (a) (5) (ii) (D) 164.312 (a) (2) (i)	Gestion des mots de passe (A) :Implémente les procédures de création, de changement et de protection des mots de passe.	Spécifie la valeur de 30 secondes pour le délai de saisie du mot de passe.	**Commande** : **chsec -f /etc/security/login.cfg -s usw -a logintimeout=30**. **Valeur renvoyée** : s'il aboutit, ce script renvoie la valeur 0. S'il échoue, il renvoie le code d'erreur 1.
164.308 (a) (5) (ii) (D) 164.312 (a) (2) (i)	Gestion des mots de passe (A) :Implémente les procédures de création, de changement et de protection des mots de passe.	Garantit que les comptes sont verrouillés après 35 jours d'inactivité.	**Commande** : **grep TMOUT= /etc/security /.profile > /dev/null 2>&1if TMOUT = (35x24x60x60){#chsec -f /etc/security/user -s user -aaccount_locked = true}**. **Valeur renvoyée** : si la commande ne parvient pas à associer **account_locked** à la valeur **true**, le script renvoie la valeur 1. Sinon, la commande renvoie la valeur 0.
164.312 (c) (1)	Implémente les règles et les procédures permettant de protéger les informations EPHI contre toute altération indésirable ou destruction.	Active les règles Trusted Execution (TE).	**Commande** : Turns on **CHKEXEC, CHKSHLIB, CHKSCRIPT, CHKKERNEXT, STOP_ON_CHKFAIL,TE=ON For example, trustchk –p TE=ON CHKEXEC = ON, CHKSHLIB,=ON, CHKSCRIPT=ON, CHKKERNEXT = ON**. **Valeur renvoyée** : en cas d'échec, le script renvoie la valeur 1.
164.312 (e) (1)	Implémente les mesures de sécurité techniques permettant d'empêcher tout accès non autorisé aux informations EPHI transmises sur un réseau de communication électronique.	Détermine si les ensembles de fichiers **ssh** sont installés. Si tel n'est pas le cas, affiche un message d'erreur.	**Commande** : **# lslpp –l | grep openssh > /dev/null 2>&1**. **Valeur renvoyée** : si le code retour pour cette commande est 0, le script renvoie la valeur 0. Si les ensembles de fichiers ssh ne sont pas installés, le script renvoie la valeur 1 et affiche le message d'erreur `Install ssh filesets for secure transmission`.

Le tableau ci-après détaille les différentes fonctions de la règle de sécurité HIPAA et chaque fonction inclut plusieurs normes et spécifications d'implémentation.

Tableau 9. Fonctions HIPAA et détails d'implémentation

Fonctions HIPAA	Spécification d'implémentation	L'implémentation aixpert	Commandes et valeurs renvoyées
Journalisation des erreurs	Consolide les erreurs provenant de différents journaux et envoie des courriers électroniques à l'administrateur.	Détermine si des erreurs matérielles existent. Détermine si des erreurs irrémédiables existent dans le fichier **trcfile** qui se trouve dans le répertoire `/var/adm/ras/trcfile`. Envoie les erreurs à **root@<nomhôte>**.	**Commande** : **errpt -d H**. **Valeur renvoyée** : si elle aboutit, cette commande renvoie la valeur 0. Si elle échoue, elle renvoie la valeur 1.

Tableau 9. Fonctions HIPAA et détails d'implémentation (suite)

Fonctions HIPAA	Spécification d'implémentation	L'implémentation aixpert	Commandes et valeurs renvoyées
Activation de FPM	Change les droits d'accès aux fichiers.	Change les droits d'accès aux fichiers à partir d'une liste de droits d'accès et de fichiers à l'aide de la commande **fpm**.	**Commande** : **# fpm -1 <niveau> -f <fichier_commandes>**. **Valeur renvoyée** : si elle aboutit, cette commande renvoie la valeur 0. Si elle échoue, elle renvoie la valeur 1.
Activation de RBAC	Crée les utilisateurs **isso**, **so** et **sa** et affecte les rôles appropriés aux utilisateurs.	Suggère de créer les utilisateurs **isso**, **so** et **sa**. Affecte les rôles appropriés aux utilisateurs.	**Commande** : **/etc/security/pscexpert/bin/RbacEnablement**.

Conformité à la norme North American Electric Reliability Corporation (NERC)

North American Electric Reliability Corporation (NERC) est une société sans but lucratif qui développe des normes pour l'industrie des réseaux électroniques. PowerSC Standard Edition contient un profil NERC préconfiguré qui fournit des normes de sécurité que vous pouvez utiliser pour protéger des réseaux électriques essentiels.

Le profil NERC respecte les normes CIP (Critical Infrastructure Protection).

Le profil NERC se trouve dans `/etc/security/aixpert/custom/NERC.xml`. Vous pouvez réinitialiser l'état par défaut des exigences CIP qui sont appliquées au profil NERC en appliquant le profil NERC_to_AIXDefault.xml qui se trouve dans le répertoire `/etc/security/aixpert/custom`. Ce processus n'est pas identique à l'opération d'annulation du profil NERC.

Le tableau ci-après fournit des informations sur les normes CIP qui sont appliques au système d'exploitation AIX et sur la façon dont PowerSC Standard Edition gère les normes CIP :

Tableau 10. Normes CIP pour PowerSC Standard Edition

Norme CIP	Implémentation AIX Security Expert	Emplacement du script qui modifie la valeur
CIP-003-3 R5.1	Configure les paramètres de sécurité du système afin d'éviter tout problème en supprimant les attributs set-user identification (SUID) et set-group identification (SGID) dans les fichiers binaires.	• `/etc/security/pscexpert/bin/filepermgr` • `/etc/security/pscexpert/bin/rmsuidfrmrcmds`
CIP-003-3 R5.1.1	Active le contrôle d'accès basé sur les rôles (RBAC) en créant des rôles opérateur système, administrateur système et responsable de la sécurité du système d'information avec les droits d'accès requis.	`/etc/security/pscexpert/bin/EnableRbac`
CIP-005-3a R2.1-R2.4	Active Secure Shell (SSH) pour l'accès de sécurité.	`/etc/security/pscexpert/bin/sshstart`
CIP-005-3a R2.5	Désactive les services inutiles et non sécurisés suivants : • Le démon **lpd** • L'environnement CDE (Common Desktop Environment)	`/etc/security/pscexpert/bin/comntrows`

Tableau 10. Normes CIP pour PowerSC Standard Edition (suite)

Norme CIP	Implémentation AIX Security Expert	Emplacement du script qui modifie la valeur
CIP-005-3a R2.5	Désactive les services inutiles et non sécurisés suivants : • Le démon **timed** • Le démon **NTP** • Le démon **rwhod** • Le démon **DPID2** • L'agent DHCP	`/etc/security/pscexpert/bin/rctcpip`
CIP-005-3a R2.5	Désactive les services inutiles et non sécurisés suivants : • Le démon **comsat** • Le démon **dtspcd** • Le démon **fingerd** • Le démon **ftpd** • Le démon **rshd** • Le démon **rlogind** • Le démon **rexecd** • Le démon **systat** • Le démon **tfptd** • Le démon **talkd** • Le démon **rquotad** • Le démon **rstatd** • Le démon **rusersd** • Le démon **rwalld** • Le démon **sprayd** • Le démon **pcnfsd** • Le démon **telnet** • Le service cmsd • Le service ttdbserver • Le service TCP echo • Le service TCP discard • Le service TCP chargen • Le service TCP daytime • Le service TCP time • Le service UDP echo • Le service UDP discard • Le service UDP chargen • Le service UDP daytime • Le service UDP time	`/etc/security/pscexpert/bin/cominetdconf`
CIP-005-3a R2.5	Impose l'atténuation du refus de demande de service sur les ports.	`/etc/security/pscexpert/bin/tcptr_aixpert`
CIP-005-3a R3 CIP-007-3a R5, R6.5	Active la fonction d'audit des fichiers binaires sur le système.	`/etc/security/pscexpert/bin/pciaudit`
CIP-005-3a R3	Met à jour le fichier de configuration d'audit avec de nouveaux utilisateurs, rôles et événements.	`/etc/security/pscexpert/bin/auditconfig`
CIP-007-3a R3	Affiche un message pour l'activation de Trusted Network Connect (TNC).	`/etc/security/pscexpert/bin/GeneralMsg`

Tableau 10. Normes CIP pour PowerSC Standard Edition (suite)

Norme CIP	Implémentation AIX Security Expert	Emplacement du script qui modifie la valeur
CIP-007-3a R4	Assure l'intégrité du système en assurant la protection contre les types connus de logiciels malveillants, en les détectant et en les supprimant.	`/etc/security/pscexpert/bin/manageITsecurity`
CIP-007-3a R5.2.1	Permet le changement du mot de passe à la première connexion pour tous les comptes utilisateur par défaut qui ne sont pas verrouillés.	`/etc/security/pscexpert/bin/pwdchg`
CIP-007-3a R5.2.2-R5.2.3	Verrouille tous les comptes utilisateur par défaut.	`/etc/security/pscexpert/dodv2/lockacc_rlogin`
CIP-007-3a R5.3.1	Spécifie que chaque mot de passe doit comporter 6 caractères au moins.	`/etc/security/pscexpert/bin/chusrattr`
CIP-007-3a R5.3.2	Spécifie que chaque mot de passe doit être une combinaison de caractères alphabétiques, numériques et spéciaux.	`/etc/security/pscexpert/bin/chusrattr`
CIP-007-3a R5.3.3	Change chaque mot de passe tous les ans.	`/etc/security/pscexpert/bin/chusrattr`
CIP-007-3a R7	Affiche un message pour l'activation du système de fichiers chiffrés (EFS).	`/etc/security/pscexpert/bin/GeneralMsg`
CIP-010-1	Affiche un message pour l'activation de Real Time Compliance (RTC).	`/etc/security/pscexpert/bin/GeneralMsg`

La liste ci-après affiche des informations sur les normes CIP qui sont appliquées au système d'exploitation AIX.

Standard CIP–003–3 — Cyber Security — Security Management Controls

R5. Access Control

The Responsible Entity documents and implements a program for managing access to protected Critical Cyber Asset (CCA) information.

- **R5.1:** The Responsible Entity maintains a list of designated personnel who are responsible for authorizing logical or physical access to protected information.
- **R5.1.1:** Personnel are identified by name, title, and the information for which they are responsible for authorizing access.

Standard CIP–005–3a — Cyber Security — Electronic Security Perimeters

R2. Electronic Access Controls

The Responsible Entity implements and documents the organizational processes and technical and procedural mechanisms for control of electronic access at all electronic access points to the Electronic Security Perimeters.

- **R2.1:** These processes and mechanisms use an access control model that denies access by default, such that explicit access permissions must be specified
- **R2.2:** At all access points to the Electronic Security Perimeter(s), the Responsible Entity enables only ports and services that are required for operations and for monitoring Cyber Assets within the Electronic Security Perimeter, and documents, individually or by specified grouping, the configuration of those ports and services.
- **R2.3:** The Responsible Entity implements and maintains a procedure for securing dial-up access to the Electronic Security Perimeters.
- **R2.4:** Where external interactive access into the Electronic Security Perimeter is enabled, the Responsible Entity implements strong procedural or technical controls at the access points to ensure authenticity of the accessing party, where technically feasible.
- **R2.5:** The required documentation, at a minimum, identify, and describe the following:
  - **R2.5.1:** The processes for access request and authorization.

- **R2.5.2:** The authentication methods.
- **R2.5.3:** The review process for authorization rights, in accordance with Standard CIP-004-3 Requirement R4.
- **R2.5.4:** The controls that are used to secure dial-up accessible connections.

R3. Monitoring Electronic Access

The Responsible Entity implements and documents an electronic or manual process for monitoring and logging access at access points to the Electronic Security Perimeters twenty-four hours a day, seven days a week.

- **R3.1:** For dial-up accessible Critical Cyber Assets that use non-routable protocols, the Responsible Entity implements and documents monitoring processes at each access point to the dial-up device, where technically feasible.
- **R3.2:** Where technically feasible, the security monitoring processes detect and alert for attempts at or actual unauthorized accesses. These alerts provide for appropriate notification to designated response personnel. Where alerting is not technically feasible, the Responsible Entity reviews or obtains access logs for attempts at or actual unauthorized accesses at least every 90 days.

Standard CIP–007–3a — Cyber Security — Systems Security Management

R2. Ports and Services

The Responsible Entity establishes, documents, and implements a process to ensure that only those ports and services that are required for normal and emergency operations are enabled.

- **R2.1:** The Responsible Entity enables only those ports and services that are required for normal and emergency operations.
- **R2.2:** The Responsible Entity disables other ports and services, including ports that are used for testing purposes, before production use of all Cyber Assets inside the Electronic Security Perimeters.
- **R2.3:** In the case where unused ports and services cannot be disabled due to technical limitations, the Responsible Entity documents the compensating measures that are applied to mitigate risk exposure.

R3. Security Patch Management

The Responsible Entity, either separately or as a component of the documented configuration management process that is specified in CIP-003-3 Requirement R6, establishes, documents, and implements a security patch management program for tracking, evaluating, testing, and installing applicable cyber security software patches for all Cyber Assets within the Electronic Security Perimeters.

- **R3.1:** The Responsible Entity documents the assessment of security patches and security upgrades for applicability within 30 days of availability of the patches or upgrades.
- **R3.2:** The Responsible Entity documents the implementation of security patches. In any case where the patch is not installed, the Responsible Entity documents the compensating measures that are applied to mitigate risk exposure.

R4. Malicious Software Prevention

The Responsible Entity uses anti-virus software and other malicious software (malware) prevention tools, where technically feasible, to detect, prevent, deter, and mitigate the introduction, exposure, and propagation of malware on all Cyber Assets within the Electronic Security Perimeters.

- **R4.1:** The Responsible Entity documents and implements anti-virus and malware prevention tools. In the case where anti-virus software and malware prevention tools are not installed, the Responsible Entity documents compensating measures that are applied to mitigate risk exposure.

- **R4.2:** The Responsible Entity documents and implements a process for the update of anti-virus and malware prevention signatures. The process must address testing and installing the signatures.

R5. Account Management

The Responsible Entity establishes, implements, and documents technical and procedural controls that enforce access authentication of, and accountability for, all user activity, and that minimize the risk of unauthorized system access.

- **R5.1:** The Responsible Entity verifies that individual and shared system accounts and authorized access permissions are consistent with the concept of `need to know` regarding work functions that are performed.
  - **R5.1.1:** The Responsible Entity reviews, at least annually, user accounts to verify that access privileges are in accordance with Standard CIP-003-3.
  - **R5.1.2:** The Responsible Entity establishes methods, processes, and procedures that generate logs of sufficient detail to create historical audit trails of individual user account access activity for a minimum of 90 days.
  - **R5.1.3:** The Responsible Entity reviews, at least annually, user accounts to verify that access privileges are in accordance with Standard CIP-003-3.
- **R5.2:** The Responsible Entity implements a policy to minimize and manage the scope and acceptable use of administrator, shared, and other generic account privileges that include factory default accounts.
  - **R5.2.1:** The policy includes the removal, disabling, or renaming of such accounts where possible. For such accounts that must remain enabled, passwords to be changed before putting any system into service.
  - **R5.2.2:** The Responsible Entity identifies those individuals with access to shared accounts.
  - **R5.2.3:** Where such accounts must be shared, the Responsible Entity has a policy for managing the use of such accounts that limits access to only users with authorization, an audit trail of the account use (automated or manual), and steps for securing the account if personnel changes (for example, change in assignment or termination).
- **R5.3:** At a minimum, the Responsible Entity is required to use passwords, subject to the following, as technically feasible:
  - **R5.3.1:** Each password must be a minimum of 6 characters.
  - **R5.3.2:** Each password must consist of a combination of alpha, numeric, and special characters.
  - **R5.3.3:** Each password must be changed at least annually, or more frequently based on risk.

R6. Security Status Monitoring

The Responsible Entity ensures that all Cyber Assets within the Electronic Security Perimeter, as technically feasible, implement automated tools or organizational process controls to monitor system events that are related to cyber security.

- **R6.1:** The Responsible Entity implements and documents the organizational processes and technical and procedural mechanisms for monitoring for security events on all Cyber Assets within the Electronic Security Perimeter.
- **R6.2:** The security monitoring controls issue automated or manual alerts for detected cyber security incidents.
- **R6.3:** The Responsible Entity maintains logs of system events that are related to cyber security, where technically feasible, to support incident response as required in Standard CIP-008-3.
- **R6.4:** The Responsible Entity retains all logs that are specified in Requirement R6 for 90 days.

- **R6.5:** The Responsible Entity reviews logs of system events that are related to cyber security and maintain records that document the review of the logs.

R7. Disposal or Redeployment

The Responsible Entity establishes and implements formal methods, processes, and procedures for disposal or redeployment of Cyber Assets within the Electronic Security Perimeter(s) as identified and documented in Standard CIP-005-3.

- **R7.1:** Before the disposal of such assets, the Responsible Entity destroys or erases the data storage media to prevent unauthorized retrieval of sensitive cyber security or reliability data.
- **R7.2:** Before redeployment of such assets, the Responsible Entity, at a minimum, erases the data storage media to prevent unauthorized retrieval of sensitive cyber security or reliability data.

CIP–010–1 — Cyber Security — Configuration Change Management and Vulnerability Assessments

R1: The Responsible Entity implements, in a manner that identifies, assesses, and corrects deficiencies, one or more documented processes that collectively include each of the applicable requirement parts.

Gestion de l'automatisation de la sécurité et de la conformité

Découvrez le processus de planification et de déploiement des profils d'automatisation de la sécurité et de la conformité de PowerSC sur un groupe de systèmes conformément aux procédures de conformité et de gouvernance informatique acceptées.

Dans le cadre de la conformité et de la gouvernance informatique, les systèmes exécutant des classes similaires de charge de travail et de sécurité des données similaires doivent être gérés et configurés de façon cohérente. Pour planifier et déployer la conformité sur les systèmes, procédez comme suit :

Identification des groupes de travail du système

Les instructions relatives à la conformité et la gouvernance informatique établissent que les systèmes exécutant des classes similaires de charge de travail et de sécurité des données doivent être gérés et configurés de façon cohérente. Par conséquent, vous devez identifier tous les systèmes dans un groupe de travail similaire.

Utilisation d'un système de test hors production pour la configuration initiale

Appliquez le profil de conformité PowerSC au système de test.

Prenons les exemples ci-après d'application des profils de conformité au système d'exploitation AIX.

Exemple 1 : Application de `DoD.xml`

```
% aixpert -f /etc/security/aixpert/custom/DoD.xml
Processedrules=38       Passedrules=38  Failedrules=0   Level=AllRules

Input file=/etc/security/aixpert/custom/DoD.xml
```

dans cet exemple, aucune règle n'est défaillante : `Failedrules=0`. Cela signifie que toutes les règles ont été appliquées et que la phase de test peut commencer. Si l'application de certaines règles a échoué, une sortie détaillée est générée.

Exemple 2 : Application de `PCI.xml` avec échec

```
# aixpert -f /etc/security/aixpert/custom/PCI.xml
do_action(): rule(pci_grpck) : failed.
Processedrules=85       Passedrules=84  Failedrules=1   Level=AllRules
```

```
Input file=/etc/security/aixpert/custom/PCI.xml
```

L'échec de la règle pci_grpck doit être résolu. Un échec peut survenir pour les raisons suivantes :

- La règle ne s'applique pas à l'environnement et doit être supprimée.
- Un problème lié au système doit être résolu.

Examen d'une règle ayant échoué

Dans la plupart des cas, l'application d'un profil de conformité et de sécurité PowerSC n'échoue pas. Toutefois, le système peut avoir des exigences relatives à l'installation qui n'ont pas été satisfaites ou peut présenter d'autres problèmes nécessitant l'attention de l'administrateur.

La cause de l'échec peut être identifiée avec l'exemple suivant :

Affichez le fichier /etc/security/aixpert/custom/PCI.xml et localisez la règle défaillante. Dans cet exemple, il s'agit de pci_grpck. Exécutez la commande **fgrep**, recherchez la règle défaillante pci_grpck et examinez la règle XML associée.

```
fgrep -p pci_grpck /etc/security/aixpert/custom/PCI.xml
<AIXPertEntry name="pci_grpck" function="grpck"
<AIXPertRuleType type="DLS"/
<AIXPertDescription&gt;Implements portions of PCI Section 8.2,
Check group definitions: Verifies the correctness of group definitions and fixes the errors
</AIXPertDescription
<AIXPertPrereqList&gt;bos.rte.security,bos.rte.date,bos.rte.ILS</AIXPertPrereqList
<AIXPertCommand
/etc/security/aixpert/bin/execmds</AIXPertCommand
<AIXPertArgs
"/usr/sbin/grpck -y ALL; /usr/sbin/grpck -n ALL"</AIXPertArgs
<AIXPertGroup
User Group System and Password Definitions</AIXPertGroup
</AIXPertEntry
```

La commande /usr/sbin/grpck peut être affichée depuis la règle pci_grpck.

Mise à jour de la règle ayant échoué

Lors de l'application d'un profil de conformité et de sécurité PowerSC, vous pouvez détecter des erreurs.

Le système peut avoir des exigences relatives à l'installation qui n'ont pas été satisfaites ou peut présenter d'autres problèmes nécessitant l'attention de l'administrateur. Après avoir déterminé la commande sous-jacente de la règle ayant échoué, examinez le système afin de comprendre quelle est la commande de configuration défaillante. Le système peut présenter un problème de sécurité. Il se peut également qu'une règle particulière ne soit pas applicable à l'environnement du système. Ensuite, vous devez créer un profil de sécurité personnalisé.

Création d'un profil de configuration de sécurité personnalisé

Si une règle n'est pas applicable à l'environnement spécifique du système, la plupart des organisations de conformité autorisent des exceptions documentées.

Pour supprimer une règle et créer une stratégie de sécurité personnalisée ainsi qu'un fichier de configuration, procédez comme suit :

1. Copiez le contenu des fichiers suivants dans un seul fichier nommé /etc/security/aixpert/custom/*<ma_stratégie_sécurité>*.xml :

   ```
   /etc/security/aixpert/custom/[PCI.xml|DoD.xml|SOX-COBIT.xml]
   ```

2. Editez le fichier *<ma_stratégie_sécurité>*.xml en supprimant la règle qui n'est pas applicable depuis la balise XML de début <AIXPertEntry name... jusqu'à la balise XML de fin </AIXPertEntry.

Vous pouvez insérer des règles de configuration supplémentaires pour la sécurité. Insérez les règles supplémentaires dans le schéma XML `AIXPertSecurityHardening`. Vous ne pouvez pas changer les profils PowerSC directement mais vous pouvez les personnaliser.

Pour la plupart des environnements, vous devez créer une stratégie XML personnalisée. Pour distribuer un profil client à d'autres systèmes, vous devez copier de façon sécurisée la stratégie XML personnalisée sur le système requérant la même configuration. Un protocole sécurisé, par exemple un protocole de transfert de fichier sécurisé (SFTP), est utilisé pour distribuer une stratégie XML personnalisée à d'autres systèmes, et le profil est stocké à l'emplacement sécurisé `/etc/security/aixpert/custom/<ma_stratégie_sécurité.xml>/etc/security/aixpert/custom/`

Connectez-vous au système sur lequel le profil personnalisé doit être créé et exécutez la commande suivante :

```
pscxpert –f :  /etc/security/aixpert/custom/<ma_stratégie_sécurité>.xml
```

Test des applications avec AIX Profile Manager

Les configurations de sécurité peuvent avoir un impact sur les applications ainsi que sur l'accès au système et sa gestion. Il est important de tester les applications et les méthodes de gestion du système prévues lors du déploiement du système dans un environnement de production.

Les normes de conformité aux réglementations imposent une configuration de sécurité plus stricte qu'une configuration prête à l'emploi. Pour tester le système, procédez comme suit :

1. Sélectionnez **Afficher et gérer les profils** dans le panneau de droite de la page de bienvenue d'AIX Profile Manager.
2. Sélectionnez le profil qui est utilisé par le modèle pour le déploiement sur les systèmes à surveiller.
3. Cliquez sur **Comparer**.
4. Sélectionnez le groupe géré ou sélectionnez des systèmes individuels dans le groupe et cliquez sur **Ajouter** pour les ajouter à la boîte sélectionnée.
5. Cliquez sur **OK**.

L'opération de comparaison démarre.

Surveillance des systèmes pour une conformité continue avec AIX Profile Manager

Les configurations de sécurité peuvent avoir un impact sur les applications ainsi que sur l'accès au système et sa gestion. Il est important de surveiller les applications et les méthodes de gestion du système prévues lors du déploiement du système dans un environnement de production.

Pour utiliser AIX Profile Manager afin de surveiller un système AIX, procédez comme suit :

1. Sélectionnez **Afficher et gérer les profils** dans le panneau de droite de la page de bienvenue d'AIX Profile Manager.
2. Sélectionnez le profil qui est utilisé par le modèle pour le déploiement sur les systèmes à surveiller.
3. Cliquez sur **Comparer**.
4. Sélectionnez le groupe géré ou sélectionnez des systèmes individuels dans le groupe et ajoutez-les à la boîte sélectionnée.
5. Cliquez sur **OK**.

L'opération de comparaison démarre.

Configuration de l'automatisation de la sécurité et de la conformité de PowerSC

Apprenez à configurer PowerSC pour l'automatisation de la sécurité et de la conformité depuis la ligne de commande et avec AIX Profile Manager.

Configuration des paramètres des options de conformité PowerSC

Familiarisez-vous avec les notions de base de la fonction d'automatisation de la sécurité et de la conformité de PowerSC, testez la configuration sur des systèmes de test hors production, et planifiez et déployez les paramètres. Lorsque vous appliquez une configuration de conformité, les paramètres changent de nombreux paramètres de configuration sur le système d'exploitation.

Remarque : Certains profils et certaines normes de conformité désactivent Telnet car ce dernier utilise des mots de passe en clair. Par conséquent, Open SSH doit être installé, configuré et opérationnel. Vous pouvez utiliser tout autre moyen de communication sécurisé avec le système en cours de configuration. Ces normes de conformité requièrent la désactivation de la connexion `root`. Configurez un ou plusieurs utilisateurs autres que root avant d'appliquer les changements de configuration. Cette configuration ne désactive pas root et vous pouvez vous connecter en tant qu'utilisateur non root et exécutez la commande **su** pour passer à root. Vérifiez que vous pouvez établir la connexion SSH au système, connectez-vous en tant qu'utilisateur non root et exécutez la commande pour passer à `root`.

Pour accéder aux profils de configuration DoD, PCI, SOX ou COBIT, utilisez le répertoire suivant :

- Les profils sur le système d'exploitation AIX sont placés dans le répertoire `/etc/security/aixpert/custom`.
- Les profils sur le serveur d'E-S virtuel (VIOS) sont placés dans le répertoire `/etc/security/aixpert/core`.

Configuration de la conformité PowerSC depuis la ligne de commande

Implémentez ou vérifiez le profil de conformité avec la commande **pscxpert** sur le système AIX et la commande **viosecure** sur le serveur d'E-S virtuel (VIOS).

Pour appliquer les profils de conformité PowerSC sur un système AIX, entrez l'une des commandes ci-après, qui dépend du niveau de conformité de la sécurité que vous voulez appliquer.

Tableau 11. Commandes PowerSC pour AIX

Commande	Norme de conformité
% pscxpert -f /etc/security/aixpert/custom/DoD.xml	*Guide STIG du département de la défense des Etats-Unis (Department of Defense Security Technical Implementation Guide) pour UNIX*
% pscxpert -f /etc/security/aixpert/custom/Hipaa.xml	*Loi Heath Insurance Portability and Accountability Act (HIPAA)*
% pscxpert -f /etc/security/aixpert/custom/PCI.xml	*Standard PCI-DSS (Payment Card Industry Data Security Standard)*
% pscxpert -f /etc/security/aixpert/custom/SOX-COBIT.xml	*Loi Sarbanes-Oxley de 2002 – Gouvernance informatique COBIT*

Pour appliquer les profils de conformité PowerSC sur un système VIOS, entrez l'une des commandes ci-après pour le niveau de conformité de la sécurité que vous voulez appliquer.

Tableau 12. Commandes PowerSC pour le serveur d'E-S virtuel

Commande	Norme de conformité
% viosecure -file /etc/security/aixpert/custom/DoD.xml	*Guide STIG du département de la défense des Etats-Unis (Department of Defense Security Technical Implementation Guide) pour UNIX*
% viosecure -file /etc/security/aixpert/custom/Hipaa.xml	*Loi Heath Insurance Portability and Accountability Act (HIPAA)*
% viosecure -file /etc/security/aixpert/custom/PCI.xml	*Standard PCI-DSS (Payment Card Industry Data Security Standard)*
% viosecure -file /etc/security/aixpert/custom/SOX-COBIT.xml	*Loi Sarbanes-Oxley de 2002 – Gouvernance informatique COBIT*

La commande **pscxpert** sur le système AIX et la commande **viosecure** sur le VIOS peuvent prendre du temps car elles vérifient ou définissent le système entier et modifient la configuration liée à la sécurité. La sortie est similaire à l'exemple suivant :

```
Processedrules=38       Passedrules=38  Failedrules=0   Level=AllRules
```

Toutefois, certaines règles échouent en fonction de l'environnement AIX, de l'ensemble d'installation et de la configuration précédente.

Par exemple, une règle prérequise peut échouer car le système ne comporte pas l'ensemble de fichiers d'installation requis. Il est essentiel de comprendre chaque échec et de le résoudre avant de déployer les profils de conformité dans le centre de données.

Concepts associés:

«Gestion de l'automatisation de la sécurité et de la conformité», à la page 111
Découvrez le processus de planification et de déploiement des profils d'automatisation de la sécurité et de la conformité de PowerSC sur un groupe de systèmes conformément aux procédures de conformité et de gouvernance informatique acceptées.

Configuration de la conformité à PowerSC avec AIX Profile Manager

Apprenez à configurer des profils de conformité et de sécurité PowerSC ainsi qu'à déployer la configuration sur un système géré AIX à l'aide d'AIX Profile Manager.

Pour configurer des profils de conformité et de sécurité PowerSC à l'aide d'AIX Profile Manager, procédez comme suit :

1. Connectez-vous à IBM Systems Director et sélectionnez AIX Profile Manager.
2. Créez un modèle qui repose sur l'un des profils de conformité et de sécurité PowerSC comme suit :
   a. Cliquez sur l'option d'**affichage et de gestion des modèles** dans le panneau de droite de la page de bienvenue d'AIX Profile Manager.
   b. Cliquez sur **Créer**.
   c. Cliquez sur **Système d'exploitation** dans la liste **Type de modèle**.
   d. Indiquez un nom pour le modèle dans la zone **Nom du modèle de configuration**.
   e. Cliquez sur **Continuer** > **Sauvegarder**.
3. Sélectionnez le profil à utiliser avec le modèle en cliquant sur **Parcourir** sous l'option de **sélection du profil à utiliser pour ce modèle**. Les profils affichent les éléments suivants :
   - `ice_DLS.xml` est le niveau de sécurité par défaut du système d'exploitation AIX.
   - `ice_DoD.xml` est le guide STIG du département de la défense des Etats-Unis (Department of Defense Security Technical Implementation Guide) pour les paramètres UNIX.
   - `ice_HLS.xml` est une sécurité de niveau élevé générique pour les paramètres AIX.
   - `ice_LLS.xml` est la sécurité de niveau faible pour les paramètres AIX.
   - `ice_MLS.xml` est la sécurité de niveau intermédiaire pour les paramètres AIX.
   - `ice_PCI.xml` est le paramètre PCI (Payment Card Industry) pour le système d'exploitation AIX.
   - `ice_SOX.xml` est le paramètre SOX ou COBIT pour le système d'exploitation AIX.

4. Supprimez tout profil de la boîte sélectionnée.
5. Sélectionnez **Ajouter** pour déplacer le profil requis dans la boîte sélectionnée.
6. Cliquez sur **Sauvegarder**.

Pour déployer la configuration sur un système géré AIX, procédez comme suit :

1. Sélectionnez l'option d'**affichage et de gestion des modèles** dans le panneau de droite de la page de bienvenue d'AIX Profile Manager.
2. Sélectionnez le modèle requis à déployer.
3. Cliquez sur **Déployer**.
4. Sélectionnez les systèmes pour le déploiement du profil et cliquez sur **Ajouter** pour déplacer le profil requis dans la boîte sélectionnée.
5. Cliquez sur **OK** pour déployer le modèle de configuration. Le système est configuré conformément au modèle sélectionné du profil.

Pour que le déploiement aboutisse pour DoD, PCI ou SOX, PowerSC Standard Edition doit être installé sur le point d'extrémité du système AIX. Si PowerSC n'est pas installé sur le système en cours de déploiement, le déploiement échoue. IBM Systems Director déploie le modèle de configuration sur les noeuds d'extrémité du système AIX sélectionnés et configure les noeuds d'extrémité conformément aux exigences de conformité.

Information associée:

AIX Profile Manager

IBM Systems Director

PowerSC Real Time Compliance

La fonction PowerSC Real Time Compliance surveille en permanence les systèmes AIX gérés pour vérifier qu'ils sont configurés de façon cohérente et sécurisée.

La fonction PowerSC Real Time Compliance utilise les règles PowerSC Compliance Automation et AIX Security Expert pour envoyer une notification en cas de violation de conformité ou lorsqu'un fichier surveillé est modifié. Lorsque la règle de configuration d'un système n'est pas respectée, la fonction PowerSC Real Time Compliance envoie un courrier électronique ou un message texte à l'administrateur système pour l'avertir.

La fonction PowerSC Real Time Compliance est une fonction de sécurité passive qui prend en charge des profils de conformité prédéfinis ou modifiés, notamment le guide STIG du département de la défense des Etats-Unis (Department of Defense Security Technical Implementation Guide), le standard PCI-DSS (Payment Card Industry Data Security Standard), la loi Sarbanes-Oxley et la conformité COBIT. Elle fournit une liste par défaut de fichiers dont la modification doit être surveillée ; cependant, vous pouvez ajouter des fichiers à cette liste.

installation de PowerSC Real Time Compliance

La fonction PowerSC Real Time Compliance est installée avec PowerSC Standard Edition version 1.1.4 ou ultérieure et ne fait pas partie du système d'exploitation AIX de base.

Pour installer PowerSC Real Time Compliance, procédez comme suit :

1. Assurez-vous d'exécuter l'un des systèmes d'exploitation AIX suivants sur le système sur lequel vous installez la fonction PowerSC Real Time Compliance :
   - IBM AIX 6 avec niveau de technologie 7 ou version ultérieure, avec AIX Event Infrastructure for AIX and AIX Clusters (bos.ahafs 6.1.7.0) ou version ultérieure
   - IBM AIX 7 avec niveau de technologie 1 ou version ultérieure, avec AIX Event Infrastructure for AIX and AIX Clusters (bos.ahafs 7.1.1.0) ou version ultérieure
   - AIX version 7.2 ou version ultérieure, avec AIX Event Infrastructure for AIX and AIX Clusters (bos.ahafs 7.2.0.0) ou version ultérieure
2. Pour mettre à jour ou installer l'ensemble de fichiers de la fonction PowerSC Real Time Compliance, installez l'ensemble de fichiers `powerscStd.rtc` du module d'installation pour PowerSC Standard Edition version 1.1.4 ou ultérieure.

Configuration de PowerSC Real Time Compliance

Vous pouvez configurer PowerSC Real Time Compliance afin d'envoyer des alertes lorsqu'un profil de conformité n'est pas respecté ou lorsqu'un fichier surveillé est modifié. Les profils peuvent être les suivants : le guide STIG du département de la défense des Etats-Unis (Department of Defense Security Technical Implementation Guide), le standard PCI-DSS (Payment Card Industry Data Security Standard), la loi Sarbanes-Oxley et COBIT.

Vous pouvez configurer PowerSC Real Time Compliance en appliquant l'une des méthodes suivantes :

- Entrez la commande **mkrtc**.
- Exécutez l'outil SMIT en entrant la commande suivante :

  ```
  smit RTC
  ```

Identification des fichiers surveillés par la fonction PowerSC Real Time Compliance

La fonction PowerSC Real Time Compliance surveille une liste par défaut de fichiers répertoriés dans les paramètres de sécurité de niveau élevé, pour déterminer si ces fichiers sont modifiés, que vous pouvez personnaliser en ajoutant ou en supprimant des fichiers dans le fichier `/etc/security/rtc/rtcd_policy.conf`.

Il existe deux méthodes d'identification du modèle de conformité appliqué à un système. La première méthode consiste à utiliser la commande **pscxpert** ; la deuxième méthode consiste à utiliser AIX Profile Manager avec IBM Systems Director.

Une fois le profil de conformité identifié, vous pouvez ajouter des fichiers supplémentaires à la liste de fichiers à surveiller en incluant les fichiers supplémentaires dans le fichier `/etc/security/rtc/rtcd_policy.conf`. Une fois le fichier sauvegardé, la nouvelle liste est utilisée immédiatement comme référence et surveillée afin d'identifier les modifications sans qu'il ne soit nécessaire de redémarrer le système.

Définition d'alertes pour PowerSC Real Time Compliance

Vous devez configurer la notification de la fonction PowerSC Real Time Compliance en indiquant les types d'alerte et les destinataires des alertes.

Le démon rtcd, qui constitue le composant principal de la fonction PowerSC Real Time Compliance, obtient ses informations sur les types d'alerte et les destinataires depuis le fichier de configuration `/etc/security/rtc/rtcd.conf`. Vous pouvez éditer ce fichier afin de mettre à jour les informations dans un éditeur de texte.

Information associée:

Format du fichier /etc/security/rtc/rtcd.conf pour la fonction Real-Time Compliance

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 123
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 d'audit, 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 123
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 1.1.4», à la page 7
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 13. 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.
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.

Tableau 13. Traitement des incidents détectés lors de l'utilisation de certains scénarios courants (suite)

Motif de l'échec	Causes possibles	Résolution recommandée
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 120
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 119
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 la figure 1, à la page 128, 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.

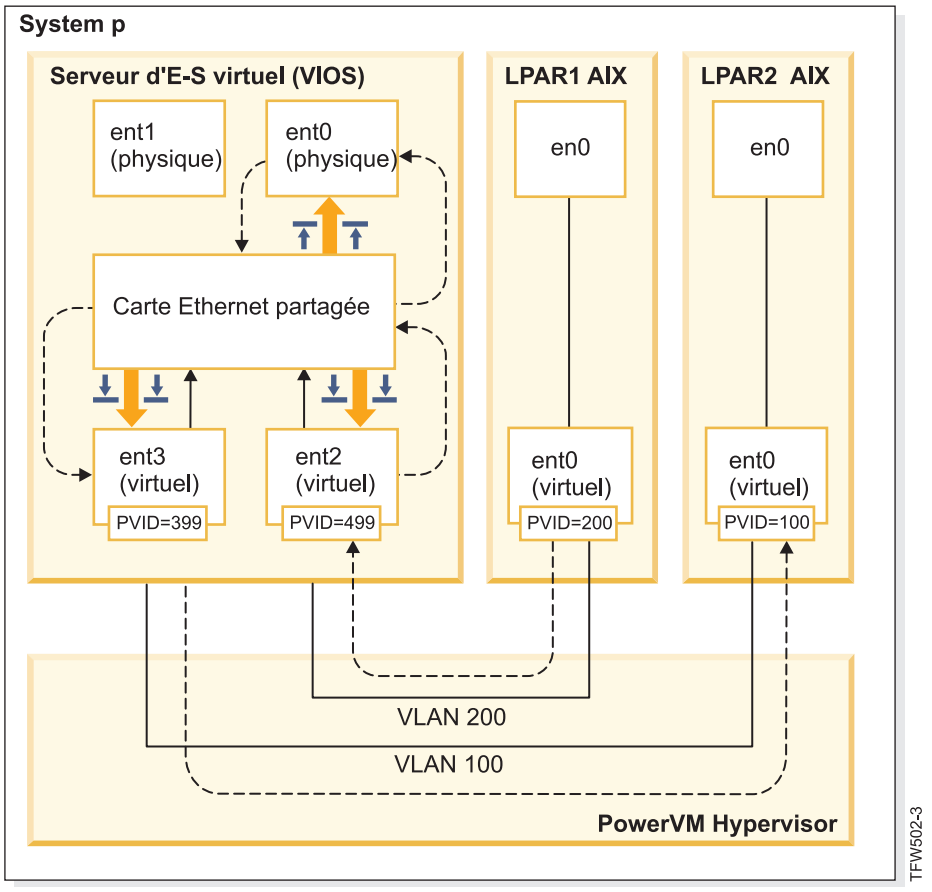

Figure 1. Exemple de transfert d'informations entre réseaux locaux virtuels sans la fonction Trusted Firewall

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 la figure 2, à la page 129.

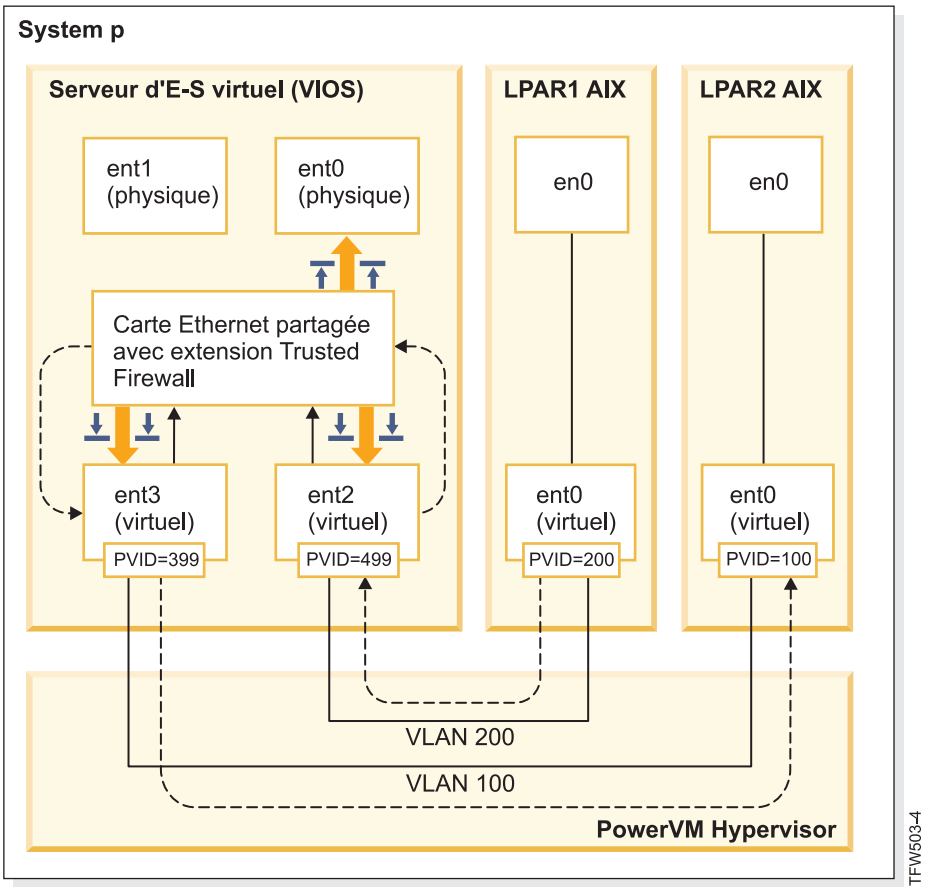

Figure 2. Exemple de transfert d'informations entre réseaux locaux virtuels avec la fonction Trusted Firewall

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 1.1.4», à la page 7
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 sur le système à partir de différentes partitions logiques afin de fournir des informations 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 depuis différents réseaux locaux virtuels se trouvant 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 en interne permet une meilleure efficacité, la fonction de journalisation de Trusted Firewall gère une liste de chemins dans le fichier `svm.log`. La taille du fichier `svm.log` ne peut pas dépasser 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`.

Remarque : Vous ne pouvez exécuter les commandes de démarrage et d'arrêt de la fonction de journalisation de Trusted Firewall que si vous vous êtes authentifié en tant qu'utilisateur root.

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, à la page 132 illustre un environnement dans lequel plusieurs cartes Ethernet partagées sont utilisées.

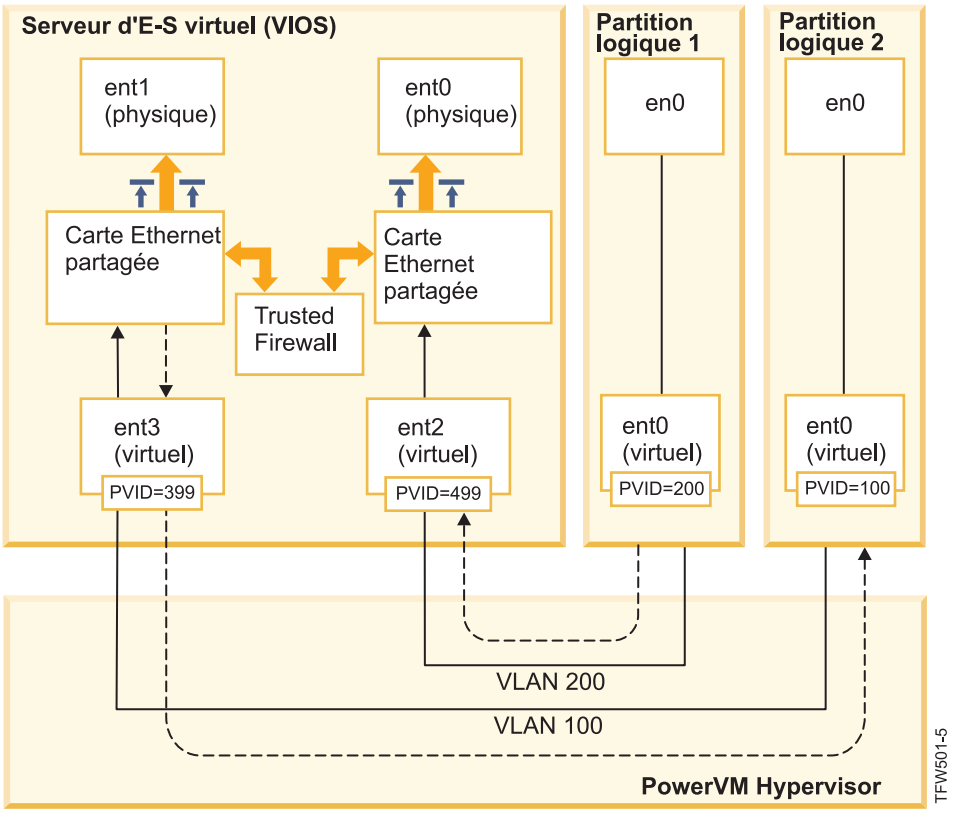

Figure 3. Configuration avec plusieurs cartes Ethernet partagées sur un VIOS

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 154

«Commande mkvfilt», à la page 156

«Commande vlantfw», à la page 172

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 133
Vous pouvez activer des règles pour autoriser le routage Trusted Firewall entre des réseaux locaux virtuels.

Référence associée:

«Commande lsvfilt», à la page 156

«Commande rmvfilt», à la page 171

Trusted Logging

La fonction PowerVM Trusted Logging permet aux partitions logiques AIX d'écrire dans des fichiers journaux qui sont stockés 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 du 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 du VIOS doit lui affecter un nom, composé comme suit :

- Nom du client
- Nom du journal

L'administrateur du 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 (LPAR) donnée (par exemple, le nom d'hôte de la partition logique (LPAR)). 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 1.1.4», à la page 7
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 138.

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 138.

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 161

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 148.
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 161

Information associée:

«Installation de PowerSC Standard Edition 1.1.4», à la page 7
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 161

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 161

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 161

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 161

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 161

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 161

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 161

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 161

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 161

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 161

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 157

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 161

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 161

Traitement des incidents liés à Trusted Network Connect and Patch management

Découvrez les causes possibles de défaillance, ainsi que les étapes permettant de traiter des 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 14. 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.

Tableau 14. Traitement des incidents liés aux paramètres de configuration pour les systèmes TNC and Patch management (suite)

Problème	Solution
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

-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 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 156

«Commande vlantfw», à la page 172

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 134
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 154

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* | nomhôte **:** *port*

pmconf rmtncpm

pmconf start

pmconf stop

pmconf init -i <*intervalle_téléchargement*> **-l** <*liste_TL*> **-A** [**-P** <*chemin_téléchargement*>] [**-x** <*intervalle_ifix*>] [**-K** <*ifix clé*>]

pmconf add -l *liste_TL*

pmconf add -p <*liste_SP*> [**-U** <*chemin_SP_défini_par_utilisateur*>]

pmconf add -p <*SP*> **-e** <*fichier_ifix*>

pmconf add -y <*fichier_recommandation*> **-v** <*fichier_signature*> **-e** <*fichier_tar_ifix*>

pmconf delete -l *liste_TL*

pmconf delete -p <*liste_SP*>

pmconf delete -p <*SP*>**-e** *fichier_ifix*

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 *nom_fichier_cert* **-k** *nom_fichier_clés*

pmconf export -f *nom_fichier*

pmconf modify -i <*intervalle_téléchargement*>

pmconf modify -P <*chemin_téléchargement*>

pmconf modify -g <*yes ou no pour accepter toutes les licences*>

pmconf modify -t <*liste_types_APAR*>

pmconf modify -x <*intervalle_ifix*>

pmconf modify -K <*clé_ifix*>

pmconf delete -l <*liste_TL*>

pmconf restart

pmconf status

pmconf log loglevel = info | error | none

pmconf chtncpm attribute = *valeur*

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 <fichier_recommandation>	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 <fichier_ifix>	Permet de spécifier les correctifs temporaires qui sont ajoutés au serveur TNCPM.
-i *intervalle_téléchargement*	Permet de spécifier la fréquence à laquelle TNCPM vérifie la présence d'un nouveau Service Pack pour les niveaux technologiques enregistrés. L'intervalle est une valeur de type entier qui représente des minutes ou dont le format est le suivant : **d** (nb de jours): **h** (heures): **m** (minutes). La plage prise en charge pour *intervalle_téléchargement* va de 30 à 525600 minutes.
-K <clé_ifix>	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 *liste_SP*	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 *liste_types_APAR*	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. liste_types_APAR est une liste séparée par des virgules contenant les types suivants : HIPER, FileNet Process Engine, Enhancement.
-P *chemin_référentiel_fichiers*	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**.
-U *référentiel_correctifs_défini_par_utilisateur*	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 *nom_fichier*	Permet de spécifier le nom du fichier certificat.
-k *nom_fichier_clés*	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: attribut1: attribut2: ...`
	`policy: valeur1: valeur2: ...`

-v *<signature file>*	Permet de spécifier le fichier de signature relatif à la recommandation de vulnérabilité IBM AIX.
-y *<fichier_recommandation>*	Permet de spécifier le fichier de recommandation de vulnérabilité IBM AIX.
-q	Permet de supprimer les informations d'en-tête.
-x *<intervalle_ifix>*	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. La plage prise en charge pour *intervalle_ifix* va de 30 à 525600 minutes.

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=**<*hôte*:*port*> [tsserver=<hôte>] [
| **recheck_interval=**<*durée_en_minutes*> | **d** (days) : **h** (hours) : **m** (minutes)] [**dbpath** =
| <*répertoire_défini_par_utilisateur*>] [**default_policy=**<*yes* | *no* >] [**clientData_interval=**<*durée_en_minutes* >
| | **d** (days) : **h** (hours) : **m** (minutes)] [**clientDataPath=**<*chemin_complet* >]

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

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

psconf chserver attribute = *valeur*

| **psconf clientData -i** *hôte* **[-l | -g]**

psconf add -F <*nom_règle_FS*> -r <*info_génération*> **[apargrp= [±]**<*groupe_apar1, groupe_apar2.. >*] [*groupe_ifix*=[+|-]<*groupe_ifix1,groupe_ifix2...>*]

psconf add { **-G** <*nom_groupe_ip*> **ip=[±]**<*hôte1, hôte2...*> | {**-A**<*groupe_apar*> **[aparlist**=[**±**]*apar1, apar2...* | {-**V** <*groupe_ifix*> [*ifixlist*=[+|-]*ifix1,ifix2...*]}

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

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

psconf add -I ip= [±]<*hôte1, hôte2...*>

psconf delete { **-F** <*nom_règle_FS*> | **-G** <*nom_groupe_ip*> | **-P** <*nom_règle*> | **-A** <*groupe_apar*> | **-V** <*groupe_ifix*>}

psconf delete -H -i <*hôte* | **ALL**> **-D** <*aaaa-mm-jj*>

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

psconf certdel -i <*hôte*>

psconf verify -i <*hôte*> | **-G** <*groupe_ip*>

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

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

psconf import -C -i <*hôte*> **-f** <*nom_fichier*> | **–d** <*nom_fichier_base_de_données_import*>

psconf { **import -k** <*nom_fichier_clés*> | **export**} **-S -f** <*nom_fichier*>

psconf list { **-S** | **-G** < *nom_groupe_ip* | **ALL** > | **-F** < *nom_règle_FS* | **ALL** > | **-P** < *nom_règle* | **ALL** > | **-r** < *info_génération* | **ALL** > | **-I -i** < *ip* | **ALL** > | **-A** < *groupe_apar* | **ALL** > | **-V** <*groupe_ifix*>} **[-c] [-q]**

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

psconf export -d <*chemin_rép_export*>

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

psconf report -A <nom_recommandation>

psconf report -P <nom_règle|ALL> -o <TEXT|CSV>

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

psconf report -B <info_génération|ALL> -o <TEXT|CSV>

Opérations client TNC :

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

psconf mkclient tncport=<*port*> -T

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

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

psconf chclient attribute = *valeur*

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

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

psconf import { **-S** | **-C -k** <*nom_fichier_clés*> } **-f** <*nom_fichier*>

Opérations IPRef TNC :

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

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

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

psconf chipref attribute =*valeur*

psconf { **import -k** <*nom_fichier_clés*> | **export** } **-R -f** <*nom_fichier*>

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 attribute=valeur 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 attribute=valeur 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 attribute=valeur 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**.
clientData	Permet de créer une image instantanée des informations (niveau de système d'exploitation et ensembles de fichiers installés) relatives au client TNC. Le chemin *clientDataPath* identifie l'emplacement des informations de collecte d'images instantanées. L'emplacement par défaut est le répertoire `/var/tnc/clientData/` sur le serveur TNC. Vous pouvez changer le chemin *clientDataPath* ou le définir à l'aide de la sous-commande **chserver** ou **mkserver**. Vous pouvez lancer la collecte d'images instantanées du client TNC depuis la ligne de commande en exécutant la sous-commande **clientData** depuis le serveur TNC. La sous-commande **clientData** qui est exécutée depuis la ligne de commande ne dépend pas de l'intervalle **clientData_interval**.
clientData_interval	Vous pouvez utiliser la sous-commande **chserver** ou **mkserver** pour configurer la collecte d'images instantanées de sorte qu'elle ait lieu à intervalles réguliers en spécifiant une valeur pour l'intervalle **clientData_interval**. La collecte d'images instantanées démarre automatiquement lorsque l'intervalle **clientData_interval** est associé à une valeur autre que 0 (zéro). Par défaut, la collecte d'images instantanées est désactivée par le planificateur. Pour activer le planificateur, spécifiez une valeur **clientData_interval** supérieure ou égale à 30. Pour désactiver le planificateur, associez le paramètre **clientData_interval** à la valeur 0 (zéro). La plage prise en charge pour l'intervalle **clientData_interval** va de 30 à 525600 minutes.
dbpath	Permet de spécifier l'emplacement de la base de données TNC. La valeur par défaut est `/var/tnc`.
default_policy	Permet d'activer ou de désactiver la vérification automatique des clients TNC permettant d'identifier le correctif temporaire (ifix) et les APAR dont le niveau est le même que celui du client. Spécifiez *yes* pour activer la vérification automatique. Spécifiez *no* pour désactiver la vérification automatique. Pour plus d'informations sur la sous-commande **default_policy**, voir le tableau relatif à la commande default_policy.
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.

Elément	Description
ipgroup	Permet de spécifier un groupe IP (Internet Protocol) contenant plusieurs adresses IP client ou noms d'hôte.
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. La plage prise en charge pour l'intervalle **recheck_interval** va de 30 à 525600 minutes. **Important :** La valeur **recheck_interval=0** signifie que le planificateur ne lance pas la vérification des clients à intervalles réguliers et que les clients enregistrés sont vérifiés automatiquement lorsqu'ils démarrent. 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 vérification manuelle des clients.

Le tableau suivant affiche les résultats de la configuration de la sous-commande **default_policy** lorsqu'elle est associée à la valeur *yes* ou à la valeur *no* :

Tableau 15. Résultats de la sous-commande default_policy

FSpolicy (règle d'ensemble de fichiers)	**default policy=***yes*	**default policy=***no*
Le client TNC appartient à une règle d'ensemble de fichiers pour laquelle un correctif temporaire (iFix) et des groupes d'APAR sont définis	La règle par défaut est remplacée par le correctif temporaire (iFix) et les APAR fournis dans la règle d'ensemble de fichiers.	La règle par défaut n'est pas utilisée. Le correctif temporaire et les APAR fournis dans la règle d'ensemble de fichiers sont pris en compte lors du processus de vérification pour le client TNC.
Le client TNC appartient à une règle d'ensemble de fichiers pour laquelle aucun correctif temporaire ou groupe d'APAR n'est défini	La règle par défaut est utilisée avec le correctif temporaire (iFix) et les APAR au cours du processus de vérification pour le client TNC. Seul le correctif temporaire et les APAR correspondant au niveau du client TNC sont utilisés au cours du processus de vérification.	La règle par défaut n'est pas utilisée.

Options

Elément	Description
-A <nom_recommandation>	Permet de spécifier le nom de recommandation pour le rapport.
-B <info_génération>	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: attribut1: attribut2: ...`
	`policy: valeur1: valeur2: ...`

-C	Permet de spécifier que l'opération concerne un composant client.
-d *emplacement_fichier_base_de_données/chemin_rép_base_de_données*	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 *aaaa-mm-jj*	Permet de spécifier la date d'une entrée client donnée dans l'historique de journalisation, où *aaaa* indique l'année, *mm* le mois et *jj* le jour.
-e *id_email* **ipgroup=[±]***g1, g2...*	Permet de spécifier l'ID de messagerie électronique suivi d'une liste de noms de groupe IP séparés par une virgule.
-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 *nom_fichier*	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.
-F *fspolicy info_génération*	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	Permet d'exécuter la sous-commande **clientData** sur le client TNC spécifié. Cet indicateur n'est disponible qu'avec la sous-commande **clientData**.
-G *nom_groupe_ip* **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 *hôte*	Permet de spécifier l'adresse IP ou le nom d'hôte.
-I ip=[±]*ip1, ip2...* | [±] hôte1,hôte2...	Permet de spécifier l'adresse IP/le nom d'hôte qui doit être ignoré lors d'une vérification.
-k *nom_fichier*	Permet de spécifier le fichier à partir duquel la clé de certificat doit être lue dans le cas d'une importation.
-l	Permet de répertorier les détails des images instantanées sur le serveur TNC pour le client TNC spécifié. Cet indicateur n'est disponible qu'avec la sous-commande **clientData**.
-p	Permet de prévisualiser la mise à jour client TNC.
-P <nom_règle>	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 *info_génération*	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.

Elément	Description
-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 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 <hôte>	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
    ```
18. Pour afficher les informations sur les images instantanées qui ont été collectées avec la sous-commande **clientData**, entrez la commande suivante :
    ```
    psconf clientData -l [ip|host]
    ```
19. Pour afficher l'historique du client TNC, entrez la commande suivante :
    ```
    psconf list –H –i [ip|ALL]
    ```

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 pscxpert

Objectif

Aide l'administrateur système à définir la configuration des paramètres de sécurité.

Syntaxe

pscxpert -l {high|medium|low|default|sox-cobit} **[-p]**

pscxpert -l {h|m|l|d|s} **[-p]**

pscxpert -f Profil **[-p]**

pscxpert -u [-p]

pscxpert -c [-p] [-r|-R] [-P Profil**] [-l** Niveau**]**

pscxpert -t

pscxpert -l <Niveau> [**-p**] <**-a** *Fichier1* | **-n** *Fichier2* | **-a** *Fichier3* **-n** *Fichier4*>

pscxpert -f Profil **-a** Fichier [**-p**]

pscxpert -d

Description

La commande **pscxpert** définit divers paramètres de configuration du système pour activer le niveau de sécurité spécifié.

L'exécution de la commande **pscxpert** avec l'indicateur **-l** seulement implémente les paramètres de sécurité rapidement sans que l'utilisateur ne puisse configurer les paramètres. Par exemple, l'exécution de la commande **pscxpert -l high** applique tous les paramètres de sécurité de niveau élevé au système automatiquement. Cependant, l'exécution de la commande **pscxpert -l** avec les indicateurs **-n** et **-a** sauvegarde les paramètres de sécurité dans un fichier spécifié par le paramètre *Fichier*. L'indicateur **-f** applique ensuite les nouvelles configurations.

Après la sélection initiale, un menu affiche toutes les options de configuration de la sécurité qui sont associées au niveau de sécurité sélectionné. Vous pouvez accepter l'ensemble des options ou les activer ou les désactiver individuellement. En cas de changement secondaire, la commande **pscxpert** continue d'appliquer les paramètres de sécurité au système informatique.

Exécutez la commande **pscxpert** en tant qu'utilisateur root du serveur virtuel d'E-S cible. Si vous n'êtes pas connecté en tant qu'utilisateur root du serveur virtuel d'E-S cible, exécutez d'abord la commande **oem_setup_env**.

Si vous exécutez la commande **pscxpert** alors qu'une autre instance de la commande **pscxpert** est déjà en cours, la commande **pscxpert** s'arrête avec un message d'erreur.

Remarque : Exécutez à nouveau la commande **pscxpert** après tout changement majeur apporté aux systèmes, comme l'installation ou la mise à jour de logiciels. Si un élément de configuration de la sécurité particulier n'est pas sélectionné lorsque la commande **pscxpert** est réexécutée, il est ignoré.

Indicateurs

Elément	Description
-a	Les paramètres avec les options de niveau de sécurité associées sont écrits dans le fichier spécifié dans un format abrégé.
-c	Vérifie les paramètres de sécurité par rapport à l'ensemble de règles précédemment appliqué. Si la vérification d'une règle échoue, les versions précédentes de la règle sont également vérifiées. Ce processus continue jusqu'à ce que la vérification aboutisse ou jusqu'à ce que toutes les instances de la règle défaillante dans le fichier `/etc/security/aixpert/core/appliedaixpert.xml` soient vérifiées. Vous pouvez exécuter cette vérification pour tout profil par défaut ou personnalisé.
-d	Affiche la définition de type de document (DTD).

Elément	Description
-f	Applique les paramètres de sécurité qui sont fournis dans le fichier *Profil* spécifié. Les profils se trouvent dans le répertoire `/etc/security/aixpert/custom`. Les profils disponibles incluent les profils standard suivants : **DataBase.xml** Ce fichier contient les exigences pour les paramètres de base de données par défaut. **DoD.xml** Ce fichier contient les exigences pour les paramètres du guide STIG du département de la défense des Etats-Unis (Department of Defense Security Technical Implementation Guide). **DoD_to_AIXDefault.xml** Ce fichier remplace les paramètres par les paramètres AIX par défaut. **DoDv2.xml** Ce fichier contient les exigences pour la version 2 des paramètres du guide STIG du département de la défense des Etats-Unis (Department of Defense Security Technical Implementation Guide). **DoDv2_to_AIXDefault.xml** Ce fichier remplace les paramètres par les paramètres AIX par défaut. **Hipaa.xml** Ce fichier contient les exigences pour les paramètres de la loi Health Insurance Portability and Accountability Act (HIPAA). **NERC.xml** Ce fichier contient les exigences pour la norme NERC (North American Electric Reliability Corporation). **NERC_to_AIXDefault.xml** Ce fichier remplace les paramètres NERC par les paramètres AIX par défaut. **PCI.xml** Ce fichier contient les exigences pour les paramètres du standard PCI-DSS (Payment Card Industry Data Security Standard). **PCIv3.xml** Ce fichier contient les exigences pour les paramètres de la version 3 du standard PCI-DSS (Payment Card Industry Data Security Standard). **PCI_to_AIXDefault.xml** Ce fichier remplace les paramètres par les paramètres AIX par défaut. **PCIv3_to_AIXDefault.xml** Ce fichier remplace les paramètres par les paramètres AIX par défaut. **SOX-COBIT.xml** Ce fichier contient les exigences pour les paramètres de la loi Sarbanes-Oxley et de COBIT. Vous pouvez aussi créer des profils personnalisés dans le même répertoire et les appliquer à vos paramètres en renommant et en modifiant les fichiers XML existants. Par exemple, la commande suivante applique le profil HIPAA à votre système : `pscxpert -f /etc/security/aixpert/custom/Hipaa.xml` Lorsque vous spécifiez l'indicateur **-f**, les paramètres de sécurité sont appliqués de façon cohérente d'un système à l'autre par le biais du transfert et de l'application sécurisés d'un fichier **appliedaixpert.xml**. Toutes les règles appliquées sont écrites dans le fichier `/etc/security/aixpert/core/appliedaixpert.xml` et les règles d'action `undo` correspondantes sont écrites dans le fichier `/etc/security/aixpert/core/undo.xml`.

Elément	Description
-l	Définit les paramètres de sécurité du système en fonction du niveau spécifié. Cet indicateur propose les options suivantes : **h | high** Spécifie les options de sécurité de niveau élevé. **m | medium** Spécifie les options de sécurité de niveau intermédiaire. **l | low** Spécifie les options de sécurité de niveau faible. **d | default** Spécifie les options de sécurité AIX de niveau standard. **s | sox-cobit** Spécifie les options de sécurité de la loi Sarbanes-Oxley et de COBIT. Si vous spécifiez les indicateurs **-l** et **-n**, les paramètres de sécurité ne sont pas implémentés sur le système ; toutefois, ils sont écrits dans le fichier spécifié. Toutes les règles appliquées sont écrites dans le fichier `/etc/security/aixpert/core/appliedaixpert.xml` et les règles d'action d'annulation correspondantes sont écrites dans le fichier `/etc/security/aixpert/core/undo.xml`. **Avertissement :** Lorsque vous utilisez l'indicateur **d | default**, il peut remplacer les paramètres de sécurité configurés que vous avez définis précédemment avec la commande **pscxpert** ou indépendamment, et restaure la configuration ouverte traditionnelle du système.
-n	Ecrit les paramètres avec les options de niveau de sécurité associées dans le fichier spécifié.
-p	Spécifie que la sortie des règles de sécurité est affichée en mode prolixe. L'indicateur **-p** journalise les règles qui sont traitées dans le sous-système d'audit si l'option **auditing** est activée. Vous pouvez utiliser cette option avec les indicateurs **-l**, **-u**, **-c** et **-f**.
-P	Accepte le nom de profil comme entrée. Cette option est utilisée avec l'indicateur **-c**. Les indicateurs **-c** et **-P** sont utilisés pour vérifier la compatibilité du système avec le profil transmis.
-r	Ecrit les paramètres existants du système dans le fichier `/etc/security/aixpert/check_report.txt`. Vous pouvez utiliser la sortie dans les rapports d'audit de conformité ou de sécurité. Le rapport décrit chaque paramètre, son éventuelle relation avec une exigence de conformité réglementaire, et indique si la vérification a abouti ou échoué.
-R	Génère la même sortie que l'indicateur **-r**, mais ajoute une description de chaque script ou programme utilisé pour implémenter le paramètre de configuration.
-t	Affiche le type de profil qui est appliqué sur le système.
-u	Annule les paramètres de sécurité qui sont appliqués. **Remarque :** Vous ne pouvez pas utiliser l'indicateur **-u** pour inverser l'application des profils DoD, DoDv2, NERC, PCI et PCIv3. Pour supprimer ces profils après qu'ils ont été ajoutés, appliquez le profil qui se termine par `_AIXDefault.xml`. Par exemple, pour supprimer le profil NERC.xml, vous devez appliquer le profil NERC_to_AIXDefault.xml.

Paramètres

Elément	Description
Fichier	Fichier de sortie dans lequel sont stockés les paramètres de sécurité. Le droit root est requis pour l'accès à ce fichier.
Niveau	Niveau personnalisé à vérifier par rapport aux paramètres appliqués précédemment.
Profil	Nom de fichier du profil qui fournit les règles de conformité pour le système. Le droit root est requis pour l'accès à ce fichier.

Sécurité

La commande **pscxpert** peut être exécutée par root seulement.

Exemples

1. Pour écrire toutes les options de sécurité de niveau élevé dans un fichier de sortie, entrez la commande suivante :

```
pscxpert -l high -n /etc/security/pscexpert/plugin/myPreferredSettings.xml
```

Une fois cette commande exécutée, vous pouvez éditer le fichier de sortie et mettre en commentaire des rôles de sécurité spécifiques en les plaçant dans la chaîne de commentaire XML standard (<-- ouvre le commentaire et -\> le ferme).

2. Pour appliquer les paramètres de sécurité figurant dans le fichier de configuration du guide STIG du département de la défense des Etats-Unis (Department of Defense Security Technical Implementation Guide), entrez la commande suivante :

   ```
   pscxpert -f /etc/security/aixpert/custom/DoD.xml
   ```

3. Pour appliquer les paramètres de sécurité figurant dans le fichier de configuration HIPAA, entrez la commande suivante :

   ```
   pscxpert -f /etc/security/aixpert/custom/Hipaa.xml
   ```

4. Pour vérifier les paramètres de sécurité du système et pour journaliser les règles qui ont échoué dans le sous-système d'audit, entrez la commande suivante :

   ```
   pscxpert -c -p
   ```

5. Pour vérifier le niveau personnalisé des paramètres de sécurité pour le profil NERC sur le système et pour journaliser les règles qui ont échoué dans le sous-système d'audit, entrez la commande suivante :

   ```
   pscxpert -c -p -l NERC
   ```

6. Pour générer des rapports et les écrire dans le fichier /etc/security/aixpert/check_report.txt, entrez la commande suivante :

   ```
   pscxpert -c -r
   ```

Emplacement

Elément	Description
/usr/sbin/pscxpert	Contient la commande **pscxpert**.

Fichiers

Elément	Description
/etc/security/aixpert/log/aixpert.log	Contient un journal de trace des paramètres de sécurité appliqués. Ce fichier n'utilise pas le fichier standard syslog. La commande **pscxpert** écrit les données directement dans le fichier, dispose des droits d'accès de lecture/écriture, et requiert la sécurité root.
/etc/security/aixpert/log/firstboot.log	Contient un journal de trace des paramètres de sécurité qui ont été appliqués lors du premier amorçage d'une installation SbD (Secure by Default).
/etc/security/aixpert/core/undo.xml	Contient une liste XML des paramètres de sécurité qui peuvent être annulés.

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 134
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 154

Remarques

Le présent document peut contenir des informations ou des références concernant certains produits, logiciels ou services du fabricant non annoncés dans ce pays.

Pour plus de détails, référez-vous aux documents d'annonce disponibles dans votre pays, ou adressez-vous à votre partenaire commercial IBM. 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, MD-NC119
Armonk, NY 10504-1785
United States of America

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 peuvent être obtenues par écrit à l'adresse suivante :

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

Le paragraphe suivant ne s'applique ni au Royaume-Uni, ni dans aucun pays dans lequel il serait contraire aux lois locales : CE DOCUMENT EST LIVRE EN L'ETAT SANS AUCUNE GARANTIE EXPLICITE OU IMPLICITE. IBM DECLINE NOTAMMENT TOUTE RESPONSABILITE RELATIVE A CES INFORMATIONS EN CAS DE CONTREFAÇON AINSI QU'EN CAS DE DEFAUT D'APTITUDE A L'EXECUTION D'UN TRAVAIL DONNE. 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.

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.

La société 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
USA

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 exemples de programmes 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 :

Des segments de ce code sont dérivés des Programmes exemples d'IBM Corp.

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 et 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 147
affichage des résultats de la vérification 149
affichage des unités de journal virtuel 138
attestation d'un système 122

C

client TNC 142
commande chvfilt 153
commande genvfilt 154
commande lsvfilt 156
commande mkvfilt 156
commande pmconf 157
commande psconf 161
commande pscxpert 167
commande rmvfilt 171
commande vlantfw 172
commandes
  chvfilt 153
  genvfilt 154
  lsvfilt 156
  mkvfilt 156
  rmvfilt 171
  vlantfw 172
communication sécurisée 142
composants 141
concepts 141
concepts Trusted Boot 119
concepts Trusted Firewall 127
configuration 144
configuration d'un serveur de gestion de correctifs 145
configuration de l'automatisation de la sécurité et de la conformité de PowerSC 114
configuration de la journalisation sécurisée 139
configuration de serveur 144
configuration de Trusted Boot 122
configuration du client 145
configuration matérielle et logicielle 5
configuration prérequise 120
conformité au guide STIG du département de la défense des Etats-Unis (Department of Defense Security Technical Implementation Guide) 10
considérations relatives à la migration 121

E

écriture de données sur des unités de journal virtuel 140
examen d'une règle ayant échoué 112

F

fichier syslog AIX 139
fonction
  PowerSC Real Time Compliance 117

G

gestion de correctifs 141
gestion de l'automatisation de la sécurité et de la conformité 111, 112, 113
gestion de TNC and Patch management 147
gestion de Trusted Boot 123
gestion des règles 150

I

importation de certificats 142, 150
inscription d'un système 122
installation 7, 143
installation de PowerSC Standard Edition 7
installation de Trusted Boot 121
installation du collecteur 121
installation du vérificateur 121
interprétation des résultats d'attestation 123

J

journaux virtuels 137

M

mise à jour d'une règle ayant échoué 112
mise à jour de la règle ayant échoué 112
mise à jour du client TNC 149
modules IMC et IMV 143

N

notification par courrier électronique 146

O

outil de génération de rapports et de gestion pour TNC, SUMA
  utilisation de la commande psconf 161
outil de génération de rapports et de gestion pour TNCPM
  utilisation de la commande pmconf 157

P

planification 120
PowerSC 10, 100, 111, 114
  Real-Time Compliance 117
  Trusted Firewall
    configuration 130
    configuration avec plusieurs cartes Ethernet partagées 131
    création de règles 133
    désactivation de règles 134
    installation 130
    retrait de cartes Ethernet partagées 133
  Trusted Logging
    installation 138
PowerSC Standard Edition 5, 7

préparation aux actions de résolution 120
présentation 5, 141
protocole 142

R

Real-Time Compliance 117
référenceur IP 142
référenceur IP sur VIOS 147
règles client 148

S

sécurité
  PowerSC
    Real-Time Compliance 117
serveur 141
serveur Trusted Network Connect 146, 147
sous-système de contrôle AIX 139
SOX et COBIT 100
SUMA 141
suppression de systèmes 123
surveillance des systèmes pour une conformité continue 113

T

test des applications 113
TNC 151
traitement des incidents 123
traitement des incidents liés à TNC and Patch management 151
Trusted Boot 119, 120, 121, 122, 123
Trusted Firewall 127
  configuration 130
    plusieurs cartes Ethernet partagées 131
  création de règles 133
  désactivation de règles 134
  installation 130
  retrait
    cartes Ethernet partagées 133
Trusted Logging 137, 138, 140
  installation 138
Trusted Logging, présentation 137
Trusted Network Connect 141, 142, 143, 144, 145, 147, 148, 149, 150
Trusted Network Connect and Patch management 141

V

vérification du client 149