IBM PowerSC

Standard Edition

Versió 1.1.6

PowerSC Standard Edition

IBM PowerSC

Standard Edition

Versió 1.1.6

PowerSC Standard Edition

Nota

Abans d'utilitzar aquesta informació i el producte al qual fa referència, llegiu la informació de l'apartat "Avisos" a la pàgina 197.

Aquesta edició s'aplica a la versió 1.1.6 de l'IBM PowerSC Standard Edition i a totes les versions i modificacions posteriors fins que no s'indiqui el contrari en edicions noves.

Contingut

Quant a aquest document

Aquest document proporciona als administradors del sistema informació completa sobre la seguretat de fitxers, del sistema i de la xarxa.

Ressaltat

En aquest document s'utilitzen els convenis tipogràfics següents:

Negreta	Identifica ordres, subrutines, paraules clau, fitxers, estructures, directoris i altres elements els noms dels quals estan predefinits pel sistema. També identifica objectes gràfics com ara botons, etiquetes i icones que selecciona l'usuari.
Cursiva	Identifica els paràmetres els noms o valors reals dels quals subministrarà l'usuari.
`Monoespai`	Identifica exemples de valors de dades concrets, exemples de text que s'assemblen a la informació que es veurà a la pantalla, exemples de codi de programa que s'assemblen als que un programador pot desenvolupar, missatges del sistema o bé informació que en realitat ha d'escriure l'usuari.

Sensibilitat a les majúscules i minúscules a l'AIX

Tot és sensible a les majúscules i minúscules al sistema operatiu AIX, el que significa que es fa distinció entre lletres majúscules i minúscules. Per exemple, podeu utilitzar l'ordre **ls** per llistar fitxers. Però si escriviu `LS`, el sistema mostrarà el missatge `no s'ha trobat`. De la mateixa manera, `FILEA`, `FiLea` i `filea` són tres noms de fitxer diferents, encara que siguin al mateix directori. Per evitar que es produeixin accions no desitjades, assegureu-vos que utilitzeu sempre les majúscules o minúscules adequades.

ISO 9000

Els sistemes de qualitat registrats ISO 9000 es van utilitzar en el desenvolupament i fabricació d'aquest producte.

Novetats sobre el PowerSC Standard Edition

Llegiu la informació nova o que ha canviat de forma significativa a la col•lecció de temes segons la versió del PowerSC Standard Edition.

En aquest arxiu PDF, es poden trobar marques de revisió (|) en el marge esquerre que identifica la informació nova o canviada.

Setembre de 2017

S'han afegit les característiques següents a la GUI del PowerSC:

- S'ha afegit un panell d'eines de màxim nivell de seguretat i conformitat que proporciona un resum a cop d'ull de tota la informació de l'estat d'integritat de fitxers en temps real i de conformitat.
- S'ha afegit integració amb els gestors de virtualització com, per exemple, PowerVC a través de la integració Open Stack proporcionant un descobriment de punts finals automatitzat i segur. A més, la integració admet un entorn de núvol amb visibilitat de la seguretat des del primer moment de la creació de la màquina virtual.
- S'han afegit prestacions de creació d'informes per donar suport a les auditories. Ara disposeu d'informes sobre la integritat de fitxers i de conformitat de caire general o detallats en format HTML i com a fitxer CSV. Aquests informes es poden planificar perquè es distribueixin immediatament o cada dia.
- L'Enhanced Profile Editor millora la possibilitat de personalitzar les regles i els perfils de conformitat. Les regles es poden combinar ara des de diversos orígens i es poden editar mitjançant la GUI.
- S'ha afegit integració amb els gestors d'informació d'esdeveniments de seguretat com, per exemple, QRadar. Gràcies a les entrades Syslog per tal d'oferir esdeveniments d'integritat de fitxers i de conformitat significatius es proporciona una integració fàcil.
- Les prestacions UNDO millorades ajuden de forma significativa la tasca complexa de desfer un perfil aplicat. PowerSC 1.1.6 emprèn passos importants cap a la prestació UNDO integrada amb el perfil PCI.
- S'ha millorat l'escalabilitat de la GUI quant a la conformitat. El servidor de la GUI és escalable en horitzontal i cada instància pot admetre fins a 1.000 punts finals o més.

S'han afegit les següents funcions al Trusted Network Connect Patch Management (TNCPM):

- S'ha introduït un servidor intermediari que proporciona una capa addicional de seguretat que permet que el TNCPM estigui aïllat de la Internet.
- La integració de les correccions provisionals (iFixes) al TNCPM s'ha automatitzat completament. El TNCPM pot supervisar i posar pedaços a les vulnerabilitats que s'apliquen al sistema operatiu sense que calgui la intervenció de l'usuari.
- La baixada de paquets de l'Open Source s'ha integrat ara al TNCPM, racionalitzant el flux de treball de l'Open Source.

S'ha afegit la funció següent per millorar les prestacions de conformitat:

- S'ha afegit una opció d'informe que proporciona detalls sobre les regles incloses en un perfil quan aquest s'aplica.

Fitxers en format PDF del PowerSC Standard Edition

Podeu veure la documentació del PowerSC Standard Edition com a fitxers en format PDF.

- PowerSC Standard Edititon
- Notes del lliurament del PowerSC Standard Edition

Conceptes del PowerSC Standard Edition

Aquesta visió general del PowerSC Standard Edition explica les funcions, els components i el suport de maquinari relacionats amb la funció del PowerSC Standard Edition.

El PowerSC Standard Edition proporciona seguretat i control del sistema operatiu en un núvol o en centres de dades virtualitzats i proporciona una visió d'empresa i prestacions de gestió. PowerSC Standard Edition és un conjunt de funcions que inclou l'Automatització de seguretat i de conformitat, l'Engegada fiable, el Tallafoc fiable, el Registre fiable i la gestió de pedaços i de Trusted Network Connect. La tecnologia de seguretat que s'ha inclòs a la capa de virtualització proporciona una seguretat addicional als sistemes autònoms.

A la taula següent es proporcionen detalls sobre les edicions, les funcions incloses en les edicions, els components i el maquinari basat en el processador en el que està disponible cada component.

Taula 1. Components, descripció, suport del sistema operatiu i suport del maquinari del PowerSC Standard Edition

Components	Descripció	Sistema operatiu suportat	Maquinari suportat
Automatització de seguretat i de conformitat	Automatitza el valor, la supervisió i l'auditoria de la configuració de la seguretat i de la conformitat per als estàndards següents: • Normativa de seguretat de la informació en la indústria de mitjans de pagament (PCI DSS) • Conformitat amb la llei Sarbanes-Oxley i el COBIT (SOX/COBIT) • STIG del departament de defensa (DoD) dels Estats Units • Llei de responsabilitat i portabilitat de l'assegurança mèdica (HIPAA)	• AIX 5.3 • AIX 6.1 • AIX 7.1 • AIX 7.2	• POWER5 • POWER6 • POWER7 • POWER8
Engegada fiable	Mesura la imatge d'engegada, el sistema operatiu i les aplicacions, i en testifica la fiabilitat utilitzant la tecnologia del mòdul de plataforma fiable (TPM) virtual.	• AIX 6 amb 6100-07 o posterior • AIX 7 amb 7100-01 o posterior	Microprogramari de POWER7 eFW7.4 o posterior
Tallafoc fiable	Desa l'hora i els recursos habilitant l'encaminament directe a través de les LAN virtuals (VLAN) especificades que es controlen mitjançant el mateix servidor d'E/S virtual.	• AIX 6.1 • AIX 7.1 • AIX 7.2 • VIOS, versió 2.2.1.4 o posterior	• POWER6 • POWER7 • POWER8 • servidor d'E/S virtual, versió 6.1S o posterior
Registre fiable	El registres de l'AIX es troben centralitzats al servidor d'E/S virtual (VIOS) en temps real. Aquesta funció proporciona registres segurs i la funció de còpia de seguretat i gestió de registres convenient.	• AIX 5.3 • AIX 6.1 • AIX 7.1 • AIX 7.2	• POWER5 • POWER6 • POWER7 • POWER8

Taula 1. Components, descripció, suport del sistema operatiu i suport del maquinari del PowerSC Standard Edition (continuació)

Components	Descripció	Sistema operatiu suportat	Maquinari suportat
Trusted Network Connect i gestió de pedaços	Verifica que tots els sistemes AIX de l'entorn virtual tinguin el nivell de programari especificat i els pedaços especificats i proporciona les eines de gestió per garantir que tots els sistemes AIX tinguin el nivell de programari especificat. Proporciona alertes si s'afegeix a la xarxa un sistema virtual de baix nivell o si s'activa un pedaç de seguretat que afecti els sistemes.	• AIX 5.3 • AIX 6.1 • AIX 7.1 • AIX 7.2	• POWER5 • POWER6 • POWER7 • POWER8
Client de Trusted Network Connect	El client de Trusted Network Connect requereix un dels components llistats amb el sistema operatiu.	• AIX 6.1 amb 6100-06 o posterior • AIX, versió 7.1, amb el sistema de consola SUMA (Service Update Management Assistant) en un entorn SUMA per a la gestió de pedaços • AIX, versió 7.2.1, amb el sistema de consola SUMA (Service Update Management Assistant) en un entorn SUMA per a la gestió de pedaços	

Instal•lació del PowerSC Standard Edition

Heu d'instal•lar un conjunt de fitxers per a cada funció específica del PowerSC Standard Edition.

Hi ha disponibles els següents conjunts de fitxers per al PowerSC Standard Edition i la Interfície gràfica d'usuari (GUI) del PowerSC:

- `powerscStd.ice`: instal•lat als sistemes AIX que requereixen la funció Automatització de la seguretat i de la conformitat del PowerSC Standard Edition. El programa de conformitat requereix de 5 MB, com a mínim, d'espai de disc disponible al sistema de fitxers "/".
- `powerscStd.vtpm`: instal•lat als sistemes AIX que requereixen la funció Engegada fiable del PowerSC Standard Edition. Podeu obtenir el conjunt de fiters powerscStd.vtpm dels suports d'emmagatzematge bàsics de l'AIX o des de https://www-01.ibm.com/marketing/iwm/iwm/web/preLogin.do?source=aixbp&S_PKG=vtpm.
- `powerscStd.vlog`: instal•lat als sistemes AIX que requereixen la funció Engegada fiable del PowerSC Standard Edition.
- `powerscStd.tnc_pm`: instal•lat al AIX versió 7.1 TL4 o posterior, amb el sistema de consola SUMA (Service Update Management Assistant) en un entorn SUMA per a la gestió de pedaços amb la versió 7.2.1.0. Cal tenir instal•lat el producte Curl 7.52.1-1 al TNC Patch Manager per efectuar una transmissió segura de fitxers de correcció des del lloc de seguretat d'IBM.
- `powerscStd.svm`: instal•lat als sistemes AIX que es poden beneficiar de la funció d'encaminament del PowerSC Standard Edition.
- `powerscStd.rtc`: instal•lat als sistemes AIX que requereixen la funció Real Time Compliance del PowerSC Standard Edition.
- `powerscStd.uiAgent.rte`: instal•lat als sistemes AIX que es gestionaran utilitzant la Interfície gràfica d'usuari (GUI) del PowerSC. Per instal•lar powerscStd.uiAgent.rte 116 cal el conjunt de fitxers powerscStd.ice 115 o posterior.
- `powerscStd.uiServer.rte`: instal•lat als sistemes AIX configurats específicament per executar el servidor de la Interfície gràfica d'usuari (GUI) del PowerSC.

Podeu instal•lar el PowerSC Standard Edition i la Interfície gràfica d'usuari (GUI) del PowerSC utilitzant una de les interfícies següents:

- L'ordre **installp** de la interfície de línia d'ordres (CLI)
- La interfície SMIT

Per instal•lar el PowerSC Standard Edition utilitzant la interfície SMIT, seguiu aquests passos:

1. Executeu l'ordre següent:
   ```
   % smitty installp
   ```
2. Seleccioneu l'opció **Instal•la programari**.
3. Seleccioneu el dispositiu d'entrada o el directori del programari per tal d'especificar la ubicació i el fitxer d'instal•lació de la imatge d'instal•lació de l'IBM Compliance Expert. Per exemple, si la imatge d'instal•lació té el camí d'accés de directori i el nom de fitxer `/usr/sys/inst.images/powerscStd.vtpm`, heu d'especificar el camí d'accés del fitxer al camp **INPUT**.
4. Visualitzeu i accepteu l'acord de llicència. Accepteu l'acord de llicència utilitzant la fletxa cap avall per seleccionar **ACCEPTAR nous acords de llicència** i premeu la tecla de tabulació per canviar el valor a **Sí**.
5. Premeu **Intro** per iniciar la instal•lació.
6. Verifiqueu que l'estat de l'ordre sigui **D'acord** una vegada acabada la instal•lació.

Consulteu l'apartat "Instal•lació del GUI del PowerSC" a la pàgina 151 si us cal més informació sobre com instal•lar la Interfície gràfica d'usuari (GUI) del PowerSC

Visualització de la llicència de programari

La llicència de programari es pot visualitzar a la CLI utilitzant l'ordre següent:

```
% installp –lE –d camí d'accés/nom de fitxer
```

En què *camí d'accés/nom de fitxer* especifica la imatge d'instal•lació del PowerSC Standard Edition.

Per exemple, podeu escriure l'ordre següent utilitzant la CLI per especificar la informació de llicència relacionada amb el PowerSC Standard Edition:

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

Conceptes relacionats:

"Conceptes del PowerSC Standard Edition" a la pàgina 5
Aquesta visió general del PowerSC Standard Edition explica les funcions, els components i el suport de maquinari relacionats amb la funció del PowerSC Standard Edition.

"Instal•lació de l'engegada fiable" a la pàgina 117
Hi ha certes configuracions de maquinari i programari necessàries per instal•lar l'engegada fiable.

Tasques relacionades:

"Instal•lació del tallafoc fiable" a la pàgina 125
La instal•lació del tallafoc fiable del PowerSC és similar a instal•lar altres funcions del PowerSC.

"Instal•lació del registre fiable" a la pàgina 132
Podeu instal•lar la funció Registre fiable del PowerSC utilitzant la interfície de línia d'ordres o l'eina SMIT.

"Configuració dels components de TNC" a la pàgina 138
Cadascun dels components de Trusted Network Connect (TNC) requereixen certa configuració per poder-lo executar al vostre entorn.

Automatització de seguretat i de conformitat

L'AIX Profile Manager gestiona perfils predefinits respecte a la seguretat i la conformitat. El PowerSC Real Time Compliance supervisa constantment els sistemes AIX habilitats per garantir que s'hagin configurat de forma coherent i segura.

Els perfils XML automatitzen la configuració del sistema AIX recomanada d'IBM perquè sigui coherent amb la Payment Card Data Security Standard (normativa de seguretat de la informació de mitjans de pagament), la llei Sarbanes-Oxley o la U.S. Department of Defense UNIX Security Technical Implementation Guide (guia per a la implementació tècnica de seguretat del departament de defensa dels Estats Units) i la Health Insurance Portability and Accountability Act (HIPAA) (llei de responsabilitat i portabilitat de l'assegurança mèdica (HIPAA)). Les organitzacions que compleixen la normativa de seguretat han d'utilitzar els paràmetres de seguretat del sistema predefinits.

L'AIX Profile Manager funciona com un connector de l'IBM® Systems Director que simplifica l'aplicació dels paràmetres de seguretat, la supervisió dels paràmetres de seguretat i l'elaboració d'auditories dels paràmetres de seguretat tant per al sistema operatiu AIX com per al servidor d'E/S virtual (VIOS). Si voleu fer servir la funció de conformitat de seguretat, cal tenir instal•lada l'aplicació del PowerSC als sistemes gestionats per l'AIX que formen els estàndards de conformitat. La funció Automatització de seguretat i de conformitat s'inclou al PowerSC Standard Edition.

El paquet d'instal•lació del PowerSC Standard Edition, 5765-PSE, ha d'estar instal•lat als sistemes gestionats per l'AIX. El paquet d'instal•lació instal•la el conjunt de fitxers `powerscStd.ice` que es pot implementar al sistema utilitzant l'AIX Profile Manager o l'ordre **pscxpert**. S'ha habilitat la conformitat del PowerSC amb l'IBM Compliance Expert Express (ICEE) per gestionar i millorar els perfils XML. Els perfils XML es gestionen mitjançant l'AIX Profile Manager.

Nota: Instal•leu totes les aplicacions al sistema abans d'aplicar un perfil de seguretat.

Conceptes de l'automatització de seguretat i de conformitat

La funció de seguretat i de conformitat del PowerSC és un mètode automatitzat per configurar i elaborar una auditoria dels sistemes AIX juntament amb la U.S. Department of Defense (DoD) Security Technical Implementation Guide (STIG - guia per a la implementació tècnica de seguretat del departament de defensa dels Estats Units), la Payment Card Industry (PCI) data security standard (DSS - normativa de seguretat de la informació en la indústria de mitjans de pagament), la llei Sarbanes-Oxley, el COBIT (SOX/COBIT) i la Health Insurance Portability and Accountability Act (HIPAA - llei de responsabilitat i portabilitat de l'assegurança mèdica).

El PowerSC ajuda a automatitzar la configuració i la supervisió de sistemes que han de ser compatibles amb la versió 1.2, 2.0 o 3.0 del Payment Card Industry (PCI) data security standard (DSS) (normativa de seguretat de la informació en la indústria de mitjans de pagament). Per tant, la funció de seguretat i de conformitat del PowerSC és un mètode precís i complet d'automatització de la configuració de la seguretat que s'utilitza per complir els requisits de conformitat de TI del DoD UNIX STIG, la PCI DSS, la llei Sarbanes-Oxley, la conformitat COBIT (SOX/COBIT) i la Health Insurance Portability and Accountability Act (HIPAA) - llei de responsabilitat i portabilitat de l'assegurança mèdica.

Nota: La seguretat i la conformitat del PowerSC actualitzen els perfils XML existents que utilitza l'edició de l'IBM Compliance Expert express (ICEE). Podeu utilitzar els perfils XML PowerSC Standard Edition amb l'ordre **pscxpert**, de manera similar que l'ICEE.

Els perfils de conformitat preconfigurats que se subministren amb PowerSC Standard Edition redueixen la càrrega de treball administrativa de la interpretació de la documentació de conformitat i la

implementació dels estàndards com a paràmetres de configuració específics del sistema. Aquesta tecnologia redueix el cost de la configuració de conformitat i l'elaboració d'auditories automatitzant-ne els processos. L'IBMPowerSC Standard Edition s'ha dissenyat per ajudar de forma eficaç a gestionar els requeriments del sistema associats al compliment d'estàndards externs el que pot donar com a resultat una possible reducció de costos i una millora del rendiment.

Conformitat amb la STIG del departament de defensa

El departament de defensa (DoD) dels Estats Units requereix sistemes informàtics altament segurs. Aquest nivell de seguretat i qualitat definit pel departament de defensa s'adiu amb el grau de qualitat i personalització del servidor de l'AIX on Power Systems.

Un sistema operatiu segur com, per exemple, l'AIX, s'ha de configurar amb molt de compte per aconseguir la finalitat de la seguretat especificada. El departament de defensa ha reconegut la necessitat de les configuracions de seguretat de tots els sistemes operatius en lla directiva 8500.1. Aquesta directiva establia la política i la responsabilitat assignada a l'agència de seguretat d'informació de defensa (DISA - Defense Information Security Agency) dels Estats Units perquè proporcionés instruccions sobre la configuració de la seguretat.

DISA va desenvolupar els principis i les instruccions a la Security Technical Implementation Guide (STIG - guia per a la implementació tècnica de seguretat) de l'UNIX que proporciona un entorn que compleix o supera els requeriments de seguretat dels sistemes del departament de defensa que estan operatius al nivell d'informació confidencial de TI de MAC (Mission Assurance Category), que conté sistema. El departament de defensa dels Estats Units té uns requeriments de seguretat de la TI molt estrictes i tot una sèrie de detalls dels paràmetres de configuració necessaris per garantir que el sistema funcioni d'una manera segura. Podeu aprofitar les instruccions expertes necessàries. El PowerSC Standard Edition ajuda a automatitzar el procés de configuració dels paràmetres segons el que ha definit el departament de defensa.

Nota: Tots els fitxers script personalitzats que es proporcionen per mantenir la conformitat del departament de defensa es troben al directori `/etc/security/pscexpert/dodv2`.

El PowerSC Standard Edition dóna suport als requeriments de la versió 1 release 2 de la guia per a la implementació tècnica de seguretat de l'AIX del departament de defensa. A les taules següents es proporcionen els requeriments i s'explica com garantir la conformitat.

Taula 2. Requeriments generals del departament de defensa

ID de punt de comprovació de la guia per a la implementació tècnica de seguretat del departament de defensa	**Categoria de la regla STIG**	**Descripció**	**Ubicació de l'script on es defineix l'acció i els resultats de l'acció que permeten la conformitat**
AIX00020	2	Cal implementar el programari de base informàtica fiable de l'AIX.	**Ubicació** `/etc/security/pscexpert/dodv2/trust` **Acció de conformitat** Garanteix que el sistema compleix els requeriments especificats.
AIX00040	2	S'ha d'utilitzar l'ordre **securetcpip**.	**Ubicació** `/etc/security/pscexpert/dodv2/dodsecuretcpip` **Acció de conformitat** Garanteix que el sistema compleix els requeriments especificats.

Taula 2. Requeriments generals del departament de defensa (continuació)

ID de punt de comprovació de la guia per a la implementació tècnica de seguretat del departament de defensa	Categoria de la regla STIG	Descripció	Ubicació de l'script on es defineix l'acció i els resultats de l'acció que permeten la conformitat
AIX00060	2	Cal comprovar setmanalment el sistema perquè no hi hagi fitxers `setuid` no autoritzats ni cap modificació de no autorització a fitxers `setuid` autoritzats.	**Ubicació** `/etc/security/pscexpert/dodv2/trust` **Acció de conformitat** Comprova setmanalment que s'identifiquin els canvis als fitxers especificats.
AIX00080	1	L'atribut `SYSTEM` no s'ha de definir a *none* per a cap compte.	**Ubicació** `/etc/security/pscexpert/dodv2/SYSattr` **Acció de conformitat** Garanteix que l'atribut especificat s'hagi definit en un valor diferent de *cap*. **Nota:** Aquest paràmetre no es canvia automàticament quan es restableix la política per defecte de l'AIX mitjançant el fitxer `DoDv2_to_ AIXDefault.xml`. Heu de canviar manualment aquest paràmetre.
AIX00200	2	El sistema no ha de permetre que les difusions dirigides traspassin la passarel•la.	**Ubicació** `/etc/security/pscexpert/dodv2/ntwkoptsdod` **Acció de conformitat** Estableix el valor de l'opció de xarxa `direct_broadcast` a *0*.
AIX00210	2	El sistema ha de proporcionar protecció contra atacs ICMP (Internet Control Message Protocol) a les connexions TCP.	**Ubicació** `/etc/security/pscexpert/dodv2/ntwkoptsdod` **Acció de conformitat** Estableix el valor de l'opció de xarxa `tcp_icmpsecure` a *1*.
AIX00220	2	El sistema ha de proporcionar protecció de la pila de TCP contra els atacs de restabliment de connexió, sincronització (SYN) i injecció de dades.	**Ubicació** `/etc/security/pscexpert/dodv2/ntwkoptsdod` **Acció de conformitat** Garanteix que el valor de l'opció de xarxa `tcp_tcpsecure` s'hagi establert a *7*.
AIX00230	2	El sistema ha de proporcionar protecció contra atacs de fragmentació d'IP.	**Ubicació** `/etc/security/pscexpert/dodv2/ntwkoptsdod` **Acció de conformitat** Estableix el valor de l'opció de xarxa `ip_nfrag` a *200*.
AIX00300	1,2,3	El sistema no ha de tenir actiu el servei `bootp`.	**Ubicació** `/etc/security/pscexpert/dodv2/inetdservices` **Acció de conformitat** Inhabilita el servei especificat.
AIX00310	2	Han d'existir els fitxers `/etc/ftpaccess.ctl`.	**Ubicació** `/etc/security/pscexpert/dodv2/dodv2loginherald` **Acció de conformitat** Garanteix que existeixi el fitxer.

Taula 2. Requeriments generals del departament de defensa (continuació)

ID de punt de comprovació de la guia per a la implementació tècnica de seguretat del departament de defensa	Categoria de la regla STIG	Descripció	Ubicació de l'script on es defineix l'acció i els resultats de l'acció que permeten la conformitat
GEN000020	2	El sistema ha de requerir autenticació quan s'inicia en mode d'usuari únic.	**Ubicació** `/etc/security/pscexpert/dodv2/rootpasswd_home` **Acció de conformitat** Garanteix que el compte arrel per a particions engegables tingui una contrasenya al fitxer `/etc/security/passwd`. **Nota:** Aquest paràmetre no es canvia automàticament quan es restableix la política per defecte de l'AIX mitjançant el fitxer `DoDv2_to_ AIXDefault.xml`. Heu de canviar manualment aquest paràmetre.
GEN000100	1	El sistema operatiu ha de ser d'una versió admesa.	**Ubicació** `/etc/security/pscexpert/dodv2/dodv2cat1` **Acció de conformitat** Mostra els resultats de les proves de regles especificades.

GEN000120	2	S'han d'instal•lar les actualitzacions i els pedaços de seguretat del sistema més recents.	**Ubicació**
			`/usr/sbin/instfix -i`
			`/etc/security/pscexpert/dodv2/dodv2cat1`
			Acció de conformitat
			Configureu aquest valor utilitzant la funció Trusted Network Connect.

GEN000140	2	Cal comprovar setmanalment el sistema perquè no hi hagi fitxers `setuid` no autoritzats ni cap modificació de no autorització a fitxers `setuid` autoritzats.	**Ubicació** `/etc/security/pscexpert/dodv2/trust` **Acció de conformitat** Comprova setmanalment que s'identifiquin els canvis als fitxers especificats.
GEN000220	2	Cal comprovar setmanalment el sistema perquè no hi hagi fitxers `setuid` no autoritzats ni cap modificació de no autorització a fitxers `setuid` autoritzats.	**Ubicació** `/etc/security/pscexpert/dodv2/trust` **Acció de conformitat** Comprova setmanalment que s'identifiquin els canvis als fitxers especificats.
GEN000240	2	El rellotge del sistema ha d'estar sincronitzat amb una font horària del departament de defensa (DoD).	**Ubicació** `/etc/security/pscexpert/dodv2/dodv2cmntrows` **Acció de conformitat** Garanteix que el rellotge del sistema sigui compatible.
GEN000241	2	El rellotge del sistema ha de sincronitzar-se constantment o, si més no, cada dia.	**Ubicació** `/etc/security/pscexpert/dodv2/dodv2cmntrows` **Acció de conformitat** Garanteix que el rellotge del sistema sigui compatible.

Taula 2. Requeriments generals del departament de defensa (continuació)

ID de punt de comprovació de la guia per a la implementació tècnica de seguretat del departament de defensa	Categoria de la regla STIG	Descripció	Ubicació de l'script on es defineix l'acció i els resultats de l'acció que permeten la conformitat
GEN000242	2	El sistema ha d'utilitzar com a mínim dues fonts per a la sincronització del rellotge.	**Ubicació** `/etc/security/pscexpert/dodv2/dodv2netrules` **Acció de conformitat** Garanteix que s'utilitza més d'una font horària per a la sincronització del rellotge.
GEN000280	2	No s'han de permetre els inicis de sessió dirigits als següents tipus de comptes: • aplicació • per defecte • compartit • utilitat	**Ubicació** `/etc/security/pscexpert/dodv2/lockacc_rlogin` **Acció de conformitat** Evita inicis de sessió dirigits als comptes especificats.
GEN000290	2	El sistema no ha de tenir comptes innecessaris.	**Ubicació** `/etc/security/pscexpert/dodv2/lockacc_rlogin` **Acció de conformitat** Garanteix que no hi hagi comptes no utilitzats.
GEN000300 (relacionat amb GEN000320, GEN000380, GEN000880)	2	Tots els comptes del sistema han de tenir noms d'usuaris o de comptes exclusius i contrasenyes d'usuaris o de comptes exclusives.	**Ubicació** `/etc/security/pscexpert/dodv2/grpusrpass_chk` **Acció de conformitat** Garanteix que tots els comptes compleixin els requeriments especificats. **Nota:** Aquest paràmetre no es canvia automàticament quan es restableix la política per defecte de l'AIX mitjançant el fitxer `DoDv2_to_ AIXDefault.xml`. Heu de canviar manualment aquest paràmetre.
GEN000320 (relacionat amb GEN000300, GEN000380, GEN000880)	2	Tots els comptes del sistema han de tenir noms d'usuaris o de comptes exclusius i contrasenyes d'usuaris o de comptes exclusives.	**Ubicació** `/etc/security/pscexpert/dodv2/grpusrpass_chk` **Acció de conformitat** Garanteix que tots els comptes compleixin els requeriments especificats. **Nota:** Aquest paràmetre no es canvia automàticament quan es restableix la política per defecte de l'AIX mitjançant el fitxer `DoDv2_to_ AIXDefault.xml`. Heu de canviar manualment aquest paràmetre.
GEN000340	2	Els ID d'usuari (UID) i els ID de grups (GID) que es reserven per a comptes del sistema no s'han d'assignar a comptes o a grups que no siguin del sistema.	**Ubicació** `/etc/security/pscexpert/dodv2/account` **Acció de conformitat** Aquest paràmetre s'habilita automàticament per aplicar aquesta regla.
GEN000360	2	Els UID i els GID que es reserven per a comptes del sistema no s'han d'assignar a comptes o a grups que no siguin del sistema.	**Ubicació** `/etc/security/pscexpert/dodv2/account` **Acció de conformitat** Aquest paràmetre s'habilita automàticament per aplicar aquesta regla.

Taula 2. Requeriments generals del departament de defensa (continuació)

ID de punt de comprovació de la guia per a la implementació tècnica de seguretat del departament de defensa	Categoria de la regla STIG	Descripció	Ubicació de l'script on es defineix l'acció i els resultats de l'acció que permeten la conformitat
GEN000380 (relacionat amb GEN000300, GEN000320, GEN000880)	2	Tots els comptes del sistema han de tenir noms d'usuaris o de comptes exclusius i contrasenyes d'usuaris o de comptes exclusives.	**Ubicació** `/etc/security/pscexpert/dodv2/grpusrpass_chk` **Acció de conformitat** Garanteix que tots els comptes compleixin els requeriments especificats.
GEN000400	2	El bàner d'inici de sessió del departament de defensa (DoD) ha d'aparèixer immediatament abans, o com a part, de les sol•licituds d'inici de sessió de la consola.	**Ubicació** `/etc/security/pscexpert/dodv2/dodv2loginherald` **Acció de conformitat** Mostra el bàner necessari.
GEN000402	2	El bàner d'inici de sessió del departament de defensa ha d'aparèixer immediatament abans, o com a part, de les sol•licituds d'inici de sessió de l'entorn gràfic de l'escriptori.	**Ubicació** `/etc/security/pscexpert/dodv2/dodv2loginherald` **Acció de conformitat** El bàner d'inici de sessió s'estableix al bàner del departament de defensa.
GEN000410	2	El servei FTPS (File Transfer Protocol over SSL - protocol de transferència de fitxers a través d'SSL) o FTP (File Transfer Protocol) del sistema s'ha d'haver configurat amb el bàner d'inici de sessió del departament de defensa.	**Ubicació** `/etc/security/pscexpert/dodv2/dodv2loginherald` **Acció de conformitat** Mostra el bàner quan utilitzeu el servei FTP.
GEN000440	2	Els intents satisfactoris i no satisfactoris en iniciar i finalitzar sessió s'ha d'enregistrar.	**Ubicació** `/etc/security/pscexpert/dodv2/loginout` **Acció de conformitat** Habilita el registre necessari.
GEN000452	2	El sistema ha de mostrar la data i l'hora del darrer inici de sessió satisfactori del compte a l'hora en què s'ha produït cada inici de sessió.	**Ubicació** `/etc/security/pscexpert/dodv2/sshDoDconfig` **Acció de conformitat** Mostra la informació necessària.
GEN000460	2	Aquesta regla inhabilita un compte després de 3 intents consecutius fallits d'inici de sessió.	**Ubicació** `/etc/security/pscexpert/dodv2/chusrattrdod` **Acció de conformitat** Estableix els limit d'intents d'inici de sessió en el valor especificat.

Taula 2. Requeriments generals del departament de defensa (continuació)

ID de punt de comprovació de la guia per a la implementació tècnica de seguretat del departament de defensa	Categoria de la regla STIG	Descripció	Ubicació de l'script on es defineix l'acció i els resultats de l'acció que permeten la conformitat
GEN000480	2	Aquesta regla estableix el temps de retard d'inici de sessió a 4 segons.	**Ubicació** `/etc/security/pscexpert/dodv2/chdefstanzadod` **Acció de conformitat** Estableix el temps de retard d'inici de sessió en el valor necessari.
GEN000540	2	Aquesta regla garanteix que els fitxers de configuració de contrasenya global del sistema es configurin segons els requisits de contrasenya.	**Ubicació** `/etc/security/pscexpert/dodv2/chusrattrdod` **Acció de conformitat** Estableix els paràmetres de contrasenya necessaris.
GEN000560	1	Tots els comptes del sistema han de tenir contrasenyes vàlides.	**Ubicació** `/etc/security/pscexpert/dodv2/grpusrpass_chk` **Acció de conformitat** Garanteix que tots els comptes tinguin contrasenyes.
GEN000580	2	Aquesta regla garanteix que totes les contrasenyes continguin, com a mínim 14 caràcters.	**Ubicació** `/etc/security/pscexpert/dodv2/chusrattrdod` **Acció de conformitat** Estableix la longitud mínima de contrasenya a 14 caràcters.
GEN000585	2	El sistema ha d'utilitzar un algoritme de hash criptogràfic aprovat per la normativa 140-2 del FIPS (Federal Information Processing Standards) per a generar hash de contrasenyes de comptes.	**Ubicació** `/etc/security/pscexpert/dodv2/fipspasswd` **Acció de conformitat** Garanteix que els hash de contrasenyes utilitzin un algoritme de hash aprovat.
GEN000590	2	El sistema ha d'utilitzar un algoritme de hash criptogràfic aprovat per la normativa 140-2 del FIPS per a generar hash de contrasenyes de comptes.	**Ubicació** `/etc/security/pscexpert/dodv2/fipspasswd` **Acció de conformitat** Garanteix que els hash de contrasenyes utilitzin un algoritme de hash aprovat.
GEN000595	2	Utilitza un algoritme de hash criptogràfic aprovat per la normativa 140-2 del FIPS a l'hora de generar els hash de contrasenyes que s'emmagatzemen al sistema.	**Ubicació** `/etc/security/pscexpert/dodv2/fipspasswd` **Acció de conformitat** Garanteix que els hash de contrasenyes utilitzin un algoritme de hash aprovat.

Taula 2. Requeriments generals del departament de defensa (continuació)

ID de punt de comprovació de la guia per a la implementació tècnica de seguretat del departament de defensa	Categoria de la regla STIG	Descripció	Ubicació de l'script on es defineix l'acció i els resultats de l'acció que permeten la conformitat
GEN000640	2	Aquesta regla requereix que la contrasenya tingui com a mínim un caràcter no alfabètic.	**Ubicació** `/etc/security/pscexpert/dodv2/chusrattrdod` **Acció de conformitat** Estableix en 1 el número mínim de caràcters no alfabètics en una contrasenya.
GEN000680	2	Aquesta regla garanteix que les contrasenyes no continguin més de tres caràcters repetits consecutius.	**Ubicació** `/etc/security/pscexpert/dodv2/chusrattrdod` **Acció de conformitat** Estableix en 3 el número màxim de caràcters repetits en una contrasenya.
GEN000700	2	Aquesta regla garanteix que els fitxers de configuració de contrasenya global del sistema es configurin segons els requisits de contrasenya.	**Ubicació** `/etc/security/pscexpert/dodv2/chusrattrdod` **Acció de conformitat** Garanteix que els fitxers de configuració de contrasenyes compleixen el requeriments.

GEN000740	2	Cal bloquejar totes les contrasenyes de comptes de procés automatitzat i no interactiu (GEN000280). No s'han de permetre els inicis de sessió directes a comptes compartits, per defecte, d'aplicació o d'utilitat. (GEN002640) Cal inhabilitar o eliminar els comptes del sistema per defecte.	**Ubicació**
			`/etc/security/pscexpert/dodv2/loginout`
			`/etc/security/pscexpert/dodv2/lockacc_rlogin`
			Acció de conformitat
			Aquest paràmetre està habilitat automàticament.

GEN000740	2	Cal canviar o bloquejar al menys una vegada l'any totes les contrasenyes de comptes de procés automatitzat i no interactiu.	**Ubicació** `/etc/security/pscexpert/dodv2/lockacc_rlogin` **Acció de conformitat** Garanteix que les contrasenyes especificades es canviïn anualment o es bloquegin.
GEN000750	2	Aquesta regla requereix que les contrasenyes noves continguin com a mínim 4 caràcters que no estiguin a la contrasenya antiga.	**Ubicació** `/etc/security/pscexpert/dodv2/chusrattrdod` **Acció de conformitat** Estableix en 4 el número mínim de caràcters nous que són necessaris en una contrasenya nova.

Taula 2. Requeriments generals del departament de defensa (continuació)

ID de punt de comprovació de la guia per a la implementació tècnica de seguretat del departament de defensa	Categoria de la regla STIG	Descripció	Ubicació de l'script on es defineix l'acció i els resultats de l'acció que permeten la conformitat
GEN000760	2	Cal bloquejar els comptes després de 35 dies d'inactivitat.	**Ubicació** `/etc/security/pscexpert/dodv2/disableacctdod` **Acció de conformitat** Bloqueja els comptes després de 35 dies d'inactivitat.
GEN000790	2	El sistema ha d'impedir l'ús de paraules de diccionari per contrasenyes.	**Ubicació** `/etc/security/pscexpert/dodv2/chuserstanzadod` **Acció de conformitat** Garanteix que la contrasenya per defecte que s'està definint no sigui dèbil.
GEN000800	2	Aquesta regla garanteix que no es tornen a utilitzar les últimes cinc contrasenyes.	**Ubicació** `/etc/security/pscexpert/dodv2/chusrattrdod` **Acció de conformitat** Garanteix que la contrasenya nova no és la mateixa que cap de les últimes 5 contrasenyes.
GEN000880 (relacionat amb GEN000300, GEN000320, GEN000380)	2	Tots els comptes del sistema han de tenir noms d'usuaris o de comptes exclusius i contrasenyes d'usuaris o de comptes exclusives.	**Ubicació** `/etc/security/pscexpert/dodv2/grpusrpass_chk` **Acció de conformitat** Garanteix que tots els comptes compleixin els requeriments especificats.
GEN000900	3	El directori inicial de l'usuari root no ha de ser el directori arrel (/).	**Ubicació** `/etc/security/pscexpert/dodv2/rootpasswd_home` **Acció de conformitat** Garanteix que el sistema compleix el requeriment especificat. **Nota:** Aquest paràmetre no es canvia automàticament quan es restableix la política per defecte de l'AIX mitjançant el fitxer `DoDv2_to_ AIXDefault.xml`. Heu de canviar manualment aquest paràmetre.
GEN000940	2	El camí de cerca executable del compte arrel ha de ser el valor per defecte del proveïdor i ha de contenir només camins d'accés absoluts.	**Ubicació** `/etc/security/pscexpert/dodv2/fixpathvars` **Acció de conformitat** Garanteix que el sistema compleix els requeriments especificats. **Nota:** Aquest paràmetre no es canvia automàticament quan es restableix la política per defecte de l'AIX mitjançant el fitxer `DoDv2_to_ AIXDefault.xml`. Heu de canviar manualment aquest paràmetre.

Taula 2. Requeriments generals del departament de defensa (continuació)

ID de punt de comprovació de la guia per a la implementació tècnica de seguretat del departament de defensa	Categoria de la regla STIG	Descripció	Ubicació de l'script on es defineix l'acció i els resultats de l'acció que permeten la conformitat
GEN000945	2	El camí de cerca de la biblioteca del compte arrel ha de ser el valor per defecte del sistema i ha de contenir només camins d'accés absoluts.	**Ubicació** `/etc/security/pscexpert/dodv2/fixpathvars` **Acció de conformitat** Garanteix que el sistema compleix els requeriments especificats. **Nota:** Aquest paràmetre no es canvia automàticament quan es restableix la política per defecte de l'AIX mitjançant el fitxer `DoDv2_to_ AIXDefault.xml`. Heu de canviar manualment aquest paràmetre.
GEN000950	2	La llista de comptes arrel de les biblioteques precarregades ha d'estar buit.	**Ubicació** `/etc/security/pscexpert/dodv2/fixpathvars` **Acció de conformitat** Garanteix que el sistema compleix els requeriments especificats. **Nota:** Aquest paràmetre no es canvia automàticament quan es restableix la política per defecte de l'AIX mitjançant el fitxer `DoDv2_to_ AIXDefault.xml`. Heu de canviar manualment aquest paràmetre.
GEN000960 (relacionat amb GEN003000, GEN003020, GEN003160, GEN003360, GEN003380)	2	El compte arrel no ha de tenir directoris amb permís d'escriptura global al camí de cerca executable.	**Ubicació** `/etc/security/pscexpert/dodv2/rmwwpaths` **Acció de conformitat** Garanteix que el sistema compleix els requeriments especificats. **Nota:** Aquest paràmetre no es canvia automàticament quan es restableix la política per defecte de l'AIX mitjançant el fitxer `DoDv2_to_ AIXDefault.xml`. Heu de canviar manualment aquest paràmetre.
GEN000980	2	El sistema ha d'evitar que el compte arrel realitzi un inici de sessió directament, excepte si és des de la consola del sistema.	**Ubicació** `/etc/security/pscexpert/dodv2/chuserstanzadod` **Acció de conformitat** Garanteix que el sistema compleix els requeriments especificats.
GEN001000	2	Les consoles remotes han d'estar inhabilitades o protegides de l'accés no autoritzat.	**Ubicació** `/etc/security/pscexpert/dodv2/remoteconsole` **Acció de conformitat** Garanteix que les consoles especificades estiguin inhabilitades.
GEN001020	2	el compte arrel no s'ha d'utilitzar per a l'inici de sessió directe.	**Ubicació** `/etc/security/pscexpert/dodv2/sshDoDconfig` **Acció de conformitat** Inhabilita el compte arrel de l'inici de sessió directament.

Taula 2. Requeriments generals del departament de defensa (continuació)

ID de punt de comprovació de la guia per a la implementació tècnica de seguretat del departament de defensa	Categoria de la regla STIG	Descripció	Ubicació de l'script on es defineix l'acció i els resultats de l'acció que permeten la conformitat
GEN001060	2	El sistema ha registrar els intents correctes i no correctes d'accedir al compte arrel.	**Ubicació** `/etc/security/pscexpert/dodv2/loginout` **Acció de conformitat** Garanteix que el sistema compleix els requeriments especificats.
GEN001100	1	Les contrasenyes de root mai han de traspassar a una xarxa en format de text.	**Ubicació** `/etc/security/pscexpert/dodv2/chuserstanzadod` **Acció de conformitat** Garanteix que el sistema compleix els requeriments especificats.
GEN001120	2	El sistema no ha de permetre l'inici de sessió com a root utilitzant el protocol `SSH`.	**Ubicació** `/etc/security/pscexpert/dodv2/sshDoDconfig` **Acció de conformitat** Inhabilita l'inici de sessió com a root per a `SSH`.
GEN001440	3	Tots els usuaris interactius han de tenir assignat un directori inicial al fitxer `/etc/passwd`.	**Ubicació** `/etc/security/pscexpert/dodv2/grpusrpass_chk` **Acció de conformitat** Garanteix que tots els usuaris interactius tinguin el directori especificat.
GEN001475	2	El fitxer `/etc/group` no ha de contenir cap hash de contrasenya de grup.	**Ubicació** `/etc/security/pscexpert/dodv2/passwdhash` **Acció de conformitat** Garanteix que no hi hagi cap has de contrasenya de grup al fitxer especificat. **Nota:** Aquest paràmetre no es canvia automàticament quan es restableix la política per defecte de l'AIX mitjançant el fitxer `DoDv2_to_ AIXDefault.xml`. Heu de canviar manualment aquest paràmetre.
GEN001600	2	Els camins de cerca d'executables dels scripts de control d'executables han de contenir només camins d'accés absoluts.	**Ubicació** `/etc/security/pscexpert/dodv2/fixpathvars` **Acció de conformitat** Garanteix que el sistema compleix els requeriments especificats. **Nota:** Aquest paràmetre no es canvia automàticament quan es restableix la política per defecte de l'AIX mitjançant el fitxer `DoDv2_to_ AIXDefault.xml`. Heu de canviar manualment aquest paràmetre.
GEN001605	2	Els camins de cerca de biblioteques dels scripts de control d'executables han de contenir només camins d'accés absoluts.	**Ubicació** `/etc/security/pscexpert/dodv2/fixpathvars` **Acció de conformitat** Garanteix que el sistema compleix els requeriments especificats. **Nota:** Aquest paràmetre no es canvia automàticament quan es restableix la política per defecte de l'AIX mitjançant el fitxer `DoDv2_to_ AIXDefault.xml`. Heu de canviar manualment aquest paràmetre.

Taula 2. Requeriments generals del departament de defensa (continuació)

ID de punt de comprovació de la guia per a la implementació tècnica de seguretat del departament de defensa	Categoria de la regla STIG	Descripció	Ubicació de l'script on es defineix l'acció i els resultats de l'acció que permeten la conformitat
GEN001610	2	Les llistes de biblioteques precarregades d'scripts de control d'executables han de contenir només camins d'accés absoluts.	**Ubicació** `/etc/security/pscexpert/dodv2/fixpathvars` **Acció de conformitat** Garanteix que el sistema compleix els requeriments especificats. **Nota:** Aquest paràmetre no es canvia automàticament quan es restableix la política per defecte de l'AIX mitjançant el fitxer `DoDv2_to_ AIXDefault.xml`. Heu de canviar manualment aquest paràmetre.
GEN001840	2	Tots els camins de cerca d'executables dels fitxers d'inicialització global han de contenir només camins d'accés absoluts.	**Ubicació** `/etc/security/pscexpert/dodv2/fixpathvars` **Acció de conformitat** Garanteix que el sistema compleix els requeriments especificats. **Nota:** Aquest paràmetre no es canvia automàticament quan es restableix la política per defecte de l'AIX mitjançant el fitxer `DoDv2_to_ AIXDefault.xml`. Heu de canviar manualment aquest paràmetre.
GEN001845	2	Tots els camins de cerca de biblioteques executables dels fitxers d'inicialització global han de contenir només camins d'accés absoluts.	**Ubicació** `/etc/security/pscexpert/dodv2/fixpathvars` **Acció de conformitat** Garanteix que el sistema compleix els requeriments especificats. **Nota:** Aquest paràmetre no es canvia automàticament quan es restableix la política per defecte de l'AIX mitjançant el fitxer `DoDv2_to_ AIXDefault.xml`. Heu de canviar manualment aquest paràmetre.
GEN001850	2	Totes les llistes de biblioteques precarregades de fitxers d'inicialització globals han de contenir només camins d'accés absoluts.	**Ubicació** `/etc/security/pscexpert/dodv2/fixpathvars` **Acció de conformitat** Garanteix que el sistema compleix els requeriments especificats. **Nota:** Aquest paràmetre no es canvia automàticament quan es restableix la política per defecte de l'AIX mitjançant el fitxer `DoDv2_to_ AIXDefault.xml`. Heu de canviar manualment aquest paràmetre.
GEN001900	2	Tots els camins de cerca d'executables dels fitxers d'inicialització locals han de contenir només camins d'accés absoluts.	**Ubicació** `/etc/security/pscexpert/dodv2/fixpathvars` **Acció de conformitat** Garanteix que el sistema compleix els requeriments especificats. **Nota:** Aquest paràmetre no es canvia automàticament quan es restableix la política per defecte de l'AIX mitjançant el fitxer `DoDv2_to_ AIXDefault.xml`. Heu de canviar manualment aquest paràmetre.

Taula 2. Requeriments generals del departament de defensa (continuació)

ID de punt de comprovació de la guia per a la implementació tècnica de seguretat del departament de defensa	Categoria de la regla STIG	Descripció	Ubicació de l'script on es defineix l'acció i els resultats de l'acció que permeten la conformitat
GEN001901	2	Tots els camins de cerca de biblioteques dels fitxers d'inicialització locals han de contenir només camins d'accés absoluts.	**Ubicació** `/etc/security/pscexpert/dodv2/fixpathvars` **Acció de conformitat** Garanteix que el sistema compleix els requeriments especificats. **Nota:** Aquest paràmetre no es canvia automàticament quan es restableix la política per defecte de l'AIX mitjançant el fitxer `DoDv2_to_ AIXDefault.xml`. Heu de canviar manualment aquest paràmetre.
GEN001902	2	Totes les llistes de biblioteques precarregades de fitxers d'inicialització locals han de contenir només camins d'accés absoluts.	**Ubicació** `/etc/security/pscexpert/dodv2/fixpathvars` **Acció de conformitat** Garanteix que el sistema compleix els requeriments especificats. **Nota:** Aquest paràmetre no es canvia automàticament quan es restableix la política per defecte de l'AIX mitjançant el fitxer `DoDv2_to_ AIXDefault.xml`. Heu de canviar manualment aquest paràmetre.
GEN001940	2	Els fitxers d'inicialització d'usuaris no ha d'executar programes amb permís d'escriptura global.	**Ubicació** `/etc/security/pscexpert/dodv2/rmwwpaths` **Acció de conformitat** Garanteix que el sistema compleix els requeriments especificats.
GEN001980	2	Els fitxers `.rhosts`, `.shosts`, `hosts.equiv`, `shosts.equiv`, `/etc/passwd`, `/etc/shadow` o `/etc/group` no han de contenir cap signe més (+) sense definir les entrades pels grups de xarxa NIS+.	**Ubicació** `/etc/security/pscexpert/dodv2/dodv2netrules` **Acció de conformitat** Garanteix que els fitxers especificats compleixen els requeriments especificats.
GEN002000	2	No hi ha d'haver cap fitxer `.netrc` al sistema.	**Ubicació** `/etc/security/pscexpert/dodv2/dodv2netrules` **Acció de conformitat** Garanteix que no hi hagi cap dels fitxers especificats al sistema. **Nota:** Aquest paràmetre no es canvia automàticament quan es restableix la política per defecte de l'AIX mitjançant el fitxer `DoDv2_to_ AIXDefault.xml`. Heu de canviar manualment aquest paràmetre.
GEN002020	2	Tots els fitxers `.rhosts`, `.shosts` o `hosts.equiv` han de contenir només parells amfitrió-usuari fiables.	**Ubicació** `/etc/security/pscexpert/dodv2/dodv2netrules` **Acció de conformitat** Garanteix que els fitxers especificats compleixen aquest requeriment.

Taula 2. Requeriments generals del departament de defensa (continuació)

ID de punt de comprovació de la guia per a la implementació tècnica de seguretat del departament de defensa	Categoria de la regla STIG	Descripció	Ubicació de l'script on es defineix l'acció i els resultats de l'acció que permeten la conformitat
GEN002040	1	Aquesta regla inhabilita els fitxers `.rhosts`, `.shosts` i `hosts.equiv` o els fitxers `shosts.equiv`.	**Ubicació** `/etc/security/pscexpert/dodv2/mvhostsfilesdod` **Acció de conformitat** Inhabilita els fitxers especificats.
GEN002120	1,2	Aquesta regla comprova i configura els intèrprets d'ordres d'usuaris.	**Ubicació** `/etc/security/pscexpert/dodv2/usershells` **Acció de conformitat** Crea els intèrprets d'ordres necessaris. **Nota:** Aquest paràmetre no es canvia automàticament quan es restableix la política per defecte de l'AIX mitjançant el fitxer `DoDv2_to_ AIXDefault.xml`. Heu de canviar manualment aquest paràmetre.
GEN002140	1,2	Tots els intèrprets d'ordres als que es fa referència a la llista de `/etc/passwd` han d'aparèixer en forma de llista al fitxer `/etc/shells`, excepte els intèrprets d'ordres que s'hagin especificat per evitar inicis de sessió.	**Ubicació** `/etc/security/pscexpert/dodv2/usershells` **Acció de conformitat** Garanteix que els intèrprets d'ordres es llistin als fitxers correctes. **Nota:** Aquest paràmetre no es canvia automàticament quan es restableix la política per defecte de l'AIX mitjançant el fitxer `DoDv2_to_ AIXDefault.xml`. Heu de canviar manualment aquest paràmetre.
GEN002280	2	Els fitxers de dispositius i els directoris han de tenir permís d'escriptura només per a usuaris amb un compte de sistema o en el cas que el sistema l'hagi configurat el proveïdor.	**Ubicació** `/etc/security/pscexpert/dodv2/wwdevfiles` **Acció de conformitat** Mostra els fitxers i els directoris del dispositiu amb permís d'escriptura global així com altres fitxers del sistema de que estiguin en directoris no públics.
GEN002300	2	Els fitxers de dispositius que s'utilitzen per a realitzar la còpia de seguretat els ha de poder llegir, escriure, o ambdues accions, l'usuari root o l'usuari de suport.	**Ubicació** `/etc/security/pscexpert/dodv2/wwdevfiles` **Acció de conformitat** Mostra els fitxers i els directoris del dispositiu amb permís d'escriptura global així com altres fitxers del sistema de que estiguin en directoris no públics.
GEN002400	2	Cal comprovar setmanalment el sistema perquè no hi hagi fitxers `setuid` no autoritzats ni cap modificació de no autorització a fitxers `setuid` autoritzats.	**Ubicació** `/etc/security/pscexpert/dodv2/trust` **Acció de conformitat** Comprova setmanalment que s'identifiquin els canvis als fitxers especificats. **Nota:** Compara els dos registres setmanals més nous que s'han creat al directori `/var/security/pscexpert` per tal de verificar que no hi hagi activitat no autoritzada.

Taula 2. Requeriments generals del departament de defensa (continuació)

ID de punt de comprovació de la guia per a la implementació tècnica de seguretat del departament de defensa	Categoria de la regla STIG	Descripció	Ubicació de l'script on es defineix l'acció i els resultats de l'acció que permeten la conformitat
GEN002420	2	Els suports d'emmagatzematge extraïbles, els sistemes de fitxers remots i qualsevol sistema de fitxers que no contingui fitxers `setuid` aprovats s'hauran de muntat mitjançant l'opció *nosuid*.	**Ubicació** `/etc/security/pscexpert/dodv2/fsmntoptions` **Acció de conformitat** Garanteix que els sistemes de fitxers muntats de forma remota tinguin les opcions especificades. **Nota:** Aquest paràmetre no es canvia automàticament quan es restableix la política per defecte de l'AIX mitjançant el fitxer `DoDv2_to_ AIXDefault.xml`. Heu de canviar manualment aquest paràmetre.
GEN002430	2	Els suports d'emmagatzematge extraïbles, els sistemes de fitxers remots i qualsevol sistema de fitxers que no contingui fitxers aprovats s'hauran de muntat mitjançant l'opció *nodev*.	**Ubicació** `/etc/security/pscexpert/dodv2/fsmntoptions` **Acció de conformitat** Garanteix que els sistemes de fitxers muntats de forma remota tinguin les opcions especificades. **Nota:** Aquest paràmetre no es canvia automàticament quan es restableix la política per defecte de l'AIX mitjançant el fitxer `DoDv2_to_ AIXDefault.xml`. Heu de canviar manualment aquest paràmetre.

GEN002480	2	Els directoris públics han de ser els únics directoris amb permís d'escriptura global i els fitxers amb permís d'escriptura global han d'estar ubicats només en directoris públics.	**Ubicació**
			`/etc/security/pscexpert/dodv2/wwdevfiles`
			`/etc/security/pscexpert/dodv2/fpmdodfiles`
			Acció de conformitat
			Informa quan els fitxers amb permís d'escriptura global no es troben en directoris públics.

GEN002640	2	Cal inhabilitar o eliminar els comptes del sistema per defecte.	**Ubicació**
			`/etc/security/pscexpert/dodv2/lockacc_rlogin`
			`/etc/security/pscexpert/dodv2/loginout`
			Acció de conformitat
			Inhabilita els comptes del sistema per defecte.

GEN002660	2	S'han d'haver habilitat l'auditoria.	**Ubicació** `/etc/security/pscexpert/dodv2/dodaudit` **Acció de conformitat** Habilita l'ordre `dodaudit`, que habilita l'auditoria.
GEN002720	2	El sistema d'auditoria s'ha d'haver configurat per fer auditoria dels intents fallits per accedir a fitxers i a programes.	**Ubicació** `/etc/security/pscexpert/dodv2/dodaudit` **Acció de conformitat** S'habilita automàticament l'auditoria especificada.
GEN002740	2	El sistema d'auditoria s'ha d'haver configurat per fer auditoria de les supressions de fitxers.	**Ubicació** `/etc/security/pscexpert/dodv2/dodaudit` **Acció de conformitat** S'habilita automàticament l'auditoria especificada.

Taula 2. Requeriments generals del departament de defensa (continuació)

ID de punt de comprovació de la guia per a la implementació tècnica de seguretat del departament de defensa	Categoria de la regla STIG	Descripció	Ubicació de l'script on es defineix l'acció i els resultats de l'acció que permeten la conformitat
GEN002750	3	El sistema d'auditoria s'ha d'haver configurat per fer auditoria de la creació de comptes.	**Ubicació** `/etc/security/pscexpert/dodv2/dodaudit` **Acció de conformitat** S'habilita automàticament l'auditoria especificada.
GEN002751	3	El sistema d'auditoria s'ha d'haver configurat per fer auditoria de la modificació de comptes.	**Ubicació** `/etc/security/pscexpert/dodv2/dodaudit` **Acció de conformitat** S'habilita automàticament l'auditoria especificada.
GEN002752	3	El sistema d'auditoria s'ha d'haver configurat per fer auditoria dels comptes que s'han inhabilitat.	**Ubicació** `/etc/security/pscexpert/dodv2/dodaudit` **Acció de conformitat** S'habilita automàticament l'auditoria especificada.
GEN002753	3	El sistema d'auditoria s'ha d'haver configurat per fer auditoria de la finalització de comptes.	**Ubicació** `/etc/security/pscexpert/dodv2/dodaudit` **Acció de conformitat** S'habilita automàticament l'auditoria especificada.
GEN002760	2	El sistema d'auditoria s'ha d'haver configurat per fer auditoria de totes les accions administratives, amb privilegis i de seguretat.	**Ubicació** `/etc/security/pscexpert/dodv2/dodaudit` **Acció de conformitat** S'habilita automàticament l'auditoria especificada.
GEN002800	2	El sistema d'auditoria s'ha d'haver configurat per fer auditoria de l'inici de sessió, fi de sessió i iniciacions de sessions.	**Ubicació** `/etc/security/pscexpert/dodv2/dodaudit` **Acció de conformitat** S'habilita automàticament l'auditoria especificada.
GEN002820	2	El sistema d'auditoria s'ha d'haver configurat per fer auditoria de totes les modificacions de permisos de control d'accés discrecionals.	**Ubicació** `/etc/security/pscexpert/dodv2/dodaudit` **Acció de conformitat** S'habilita automàticament l'auditoria especificada.
GEN002825	2	El sistema d'auditoria s'ha d'haver configurat per fer auditoria de la càrrega i descàrrega dels mòduls de kernel dinàmic.	**Ubicació** `/etc/security/pscexpert/dodv2/dodaudit` **Acció de conformitat** S'habilita automàticament l'auditoria especificada.
GEN002860	2	Els registres d'auditoria s'han de rotar diàriament.	**Ubicació** `/etc/security/pscexpert/dodv2/rotateauditdod` **Acció de conformitat** Garanteix que els registres d'auditoria es rotin.

Taula 2. Requeriments generals del departament de defensa (continuació)

ID de punt de comprovació de la guia per a la implementació tècnica de seguretat del departament de defensa	Categoria de la regla STIG	Descripció	Ubicació de l'script on es defineix l'acció i els resultats de l'acció que permeten la conformitat
GEN002960	2	L'accés a la utilitat de `cron` s'ha de controlar mitjançant el fitxer `cron.allow` o el fitxer `cron.deny`, o tots dos.	**Ubicació** `/etc/security/pscexpert/dodv2/limitsysacc` **Acció de conformitat** Garanteix que estiguin habilitats els límits compatibles.
GEN003000 (relacionat amb GEN000960, GEN003020, GEN003160, GEN003360, GEN003380)	2	La tasca `cron` no s'ha d'executar en programes amb permís d'escriptura per a grups o global.	**Ubicació** `/etc/security/pscexpert/dodv2/rmwwpaths` **Acció de conformitat** Garanteix que estiguin habilitats els límits compatibles. **Nota:** Aquest paràmetre no es canvia automàticament quan es restableix la política per defecte de l'AIX mitjançant el fitxer `DoDv2_to_ AIXDefault.xml`. Heu de canviar manualment aquest paràmetre.
GEN003020 (relacionat amb GEN000960, GEN003000, GEN003160, GEN003360, GEN003380)	2	La tasca `cron` no s'ha d'executar en programes de directoris amb permís d'escriptura global ni programes subordinats a aquest tipus de directoris.	**Ubicació** `/etc/security/pscexpert/dodv2/rmwwpaths` **Acció de conformitat** Elimina el permís d'escriptura global dels directoris de programes `cron`. **Nota:** Aquest paràmetre no es canvia automàticament quan es restableix la política per defecte de l'AIX mitjançant el fitxer `DoDv2_to_ AIXDefault.xml`. Heu de canviar manualment aquest paràmetre.
GEN003060	2	Els comptes del sistema per defecte (excepte els root) no s'han de llistar al fitxer `cron.allow` o no s'han d'incloure al fitxer `cron.deny` si no existeix el fitxer `cron.allow`.	**Ubicació** `cron.allow` o `cron.deny` **Acció de conformitat** Garanteix que el sistema compleix els requeriments especificats.
GEN003160 (relacionat amb GEN000960, GEN003000, GEN003020, GEN003360, GEN003380)	2	El registre de `cron` ha d'estar en execució.	**Ubicació** `/etc/security/pscexpert/dodv2/rmwwpaths` **Acció de conformitat** Garanteix que el sistema compleix els requeriments especificats.
GEN003280	2	L'accés a la utilitat `at` s'ha de controlar mitjançant els fitxers `at.allow` i `at.deny`.	**Ubicació** `/etc/security/pscexpert/dodv2/chcronfilesdod` **Acció de conformitat** Garanteix que el sistema compleix els requeriments especificats.
GEN003300	2	El fitxer `at.deny` no ha d'estar buit, si existeix.	**Ubicació** `/etc/security/pscexpert/dodv2/chcronfilesdod` **Acció de conformitat** Garanteix que el sistema compleix els requeriments especificats.

Taula 2. Requeriments generals del departament de defensa (continuació)

ID de punt de comprovació de la guia per a la implementació tècnica de seguretat del departament de defensa	Categoria de la regla STIG	Descripció	Ubicació de l'script on es defineix l'acció i els resultats de l'acció que permeten la conformitat
GEN003320	2	Els comptes del sistema per defecte que no són root no s'han de llistar al fitxer `at.allow` o s'han d'incloure al fitxer `at.deny` si no existeix el fitxer `at.allow`.	**Ubicació** `/etc/security/pscexpert/dodv2/chcronfilesdod` **Acció de conformitat** Garanteix que el sistema compleix els requeriments especificats.
GEN003360 (relacionat amb GEN000960, GEN003000, GEN003020, GEN003160, GEN003380)	2	El daemon `at` no ha d'executar programes amb permís d'escriptura per a grups o global.	**Ubicació** `/etc/security/pscexpert/dodv2/rmwwpaths` **Acció de conformitat** Garanteix que el sistema compleix els requeriments especificats. **Nota:** Aquest paràmetre no es canvia automàticament quan es restableix la política per defecte de l'AIX mitjançant el fitxer `DoDv2_to_ AIXDefault.xml`. Heu de canviar manualment aquest paràmetre.
GEN003380 (relacionat amb GEN000960, GEN003000, GEN003020, GEN003160, GEN003360)	2	El daemon `at` no ha d'executar programes en directoris amb permís d'escriptura global o que hi estiguin subordinats.	**Ubicació** `/etc/security/pscexpert/dodv2/rmwwpaths` **Acció de conformitat** Garanteix que el sistema compleix els requeriments especificats. **Nota:** Aquest paràmetre no es canvia automàticament quan es restableix la política per defecte de l'AIX mitjançant el fitxer `DoDv2_to_ AIXDefault.xml`. Heu de canviar manualment aquest paràmetre.
GEN003510	2	Els abocaments de memòria de nucli de kernel s'han d'inhabilitar a menys que siguin necessaris.	**Ubicació** `/etc/security/pscexpert/dodv2/coredumpdev` **Acció de conformitat** Inhabilita els abocaments de memòria de nucli de kernel.
GEN003540	2	El sistema ha d'utilitzar piles de programes no executables.	**Ubicació** `/etc/security/pscexpert/dodv2/sedconfigdod` **Acció de conformitat** Obliga a utilitzar piles de programes no executables.
GEN003600	2	El sistema no ha de remetre paquets amb direccionament d'origen IPv4.	**Ubicació** `/etc/security/pscexpert/dodv2/ntwkoptsdod` **Acció de conformitat** Estableix el valor de l'opció de xarxa `ipsrcforward` a *0*.
GEN003601	2	Les mides de cua d'endarreriment de TCP s'han de definir correctament.	**Ubicació** `/etc/security/pscexpert/dodv2/ntwkoptsdod` **Acció de conformitat** Estableix el valor de l'opció de xarxa `clean_partial_ conns` en *1*.

Taula 2. Requeriments generals del departament de defensa (continuació)

ID de punt de comprovació de la guia per a la implementació tècnica de seguretat del departament de defensa	Categoria de la regla STIG	Descripció	Ubicació de l'script on es defineix l'acció i els resultats de l'acció que permeten la conformitat
GEN003603	2	El sistema no ha de respondre als ecos de la versió 4 de l'Internet Control Message Protocol (ICMPv4) que s'envien a una adreça de difusió.	**Ubicació** `/etc/security/pscexpert/dodv2/ntwkoptsdod` **Acció de conformitat** Estableix el valor de l'opció de xarxa `bcastping` a *0*.
GEN003604	2	El sistema no ha de respondre a les sol•licituds de marca horària de l'ICMP que s'envien a una adreça de difusió.	**Ubicació** `/etc/security/pscexpert/dodv2/ntwkoptsdod` **Acció de conformitat** Estableix el valor de l'opció de xarxa `bcastping` a *0*.
GEN003605	2	El sistema no ha d'aplicar l'encaminament d'origen invers a les respostes de TCP.	**Ubicació** `/etc/security/pscexpert/dodv2/ntwkoptsdod` **Acció de conformitat** Estableix el valor de l'opció de xarxa `nonlocsrcroute` a *0*.
GEN003606	2	El sistema ha d'impedir que les aplicacions locals generin paquets amb direccionament d'origen.	**Ubicació** `/etc/security/pscexpert/dodv2/ntwkoptsdod` **Acció de conformitat** Estableix el valor de l'opció de xarxa `ipsrcroutesend` a *0*.
GEN003607	2	El sistema no ha d'acceptar paquets d'IPv4 amb direccionament d'origen.	**Ubicació** `/etc/security/pscexpert/dodv2/ntwkoptsdod` **Acció de conformitat** Inhabilita la possibilitat d'acceptar paquets d'IPv4 amb direccionament d'origen.
GEN003609	2	El sistema ha d'ignorar els missatges de redirecció d'ICMP d'IPv4.	**Ubicació** `/etc/security/pscexpert/dodv2/ntwkoptsdod` **Acció de conformitat** Estableix el valor de l'opció de xarxa `ipignoreredirects` a *1*.
GEN003610	2	El sistema no ha d'enviar els missatges de redirecció d'ICMP d'IPv4.	**Ubicació** `/etc/security/pscexpert/dodv2/ntwkoptsdod` **Acció de conformitat** Estableix el valor de l'opció de xarxa `ipsendredirects` a *0*.
GEN003612	2	El sistema s'ha de configurar perquè utilitzi galetes de sincronització de TCP quan es produeix un augment del valor SYN de TCP.	**Ubicació** `/etc/security/pscexpert/dodv2/ntwkoptsdod` **Acció de conformitat** Estableix el valor de l'opció de xarxa `clean_partial_conns` en *1*.

Taula 2. Requeriments generals del departament de defensa (continuació)

ID de punt de comprovació de la guia per a la implementació tècnica de seguretat del departament de defensa	Categoria de la regla STIG	Descripció	Ubicació de l'script on es defineix l'acció i els resultats de l'acció que permeten la conformitat
GEN003640	2	El sistema de fitxers root ha d'utilitzar el registre de diari o qualsevol altre mètode de garantir la coherència del sistema de fitxers.	**Ubicació** `/etc/security/pscexpert/dodv2/chkjournal` **Acció de conformitat** Habilita el registre de diari al sistema de fitxers root.
GEN003660	2	El sistema ha de registrar les dades informatives d'autenticació.	**Ubicació** `/etc/security/pscexpert/dodv2/chsyslogdod` **Acció de conformitat** Habilita el registre de dades `auth` i `info`.
GEN003700	2	Cal haver inhabilitat o eliminat `inetd` i `xinetd` si no hi serveis de xarxa que els utilitzin.	**Ubicació** `/etc/security/pscexpert/dodv2/dodv2services` **Acció de conformitat** Garanteix que el sistema compleix els requeriments especificats.
GEN003810	2	Aquests serveis `portmap` o `rpcbind` no s'han d'executar a menys que sigui necessari.	**Ubicació** `/etc/security/pscexpert/dodv2/dodv2services` **Acció de conformitat** Garanteix que el sistema compleix els requeriments especificats.
GEN003815	2	Els serveis `portmap` o `rpcbind` no s'han d'instal•lar a menys que se s'estiguin utilitzant.	**Ubicació** `/etc/security/pscexpert/dodv2/dodv2services` **Acció de conformitat** Garanteix que el sistema compleix els requeriments especificats.
GEN003820-3860	1,2,3	Els daemons `rsh`, `rexexec` i `telnet`, i el servei `rlogind` no poden estar en execució.	**Ubicació** `/etc/security/pscexpert/dodv2/inetdservices` **Acció de conformitat** Inhabilita els daemons i serveis necessaris descomentant les entrades al fitxer `/etc/inetd.conf`.
GEN003865	2	No s'han d'haver instal•lat les eines d'anàlisi de xarxa.	**Ubicació** `/etc/security/pscexpert/dodv2/dodv2services` **Acció de conformitat** Garanteix que el sistema compleix els requeriments especificats.
GEN003900	2	El fitxer `hosts.lpd` (o un equivalent) no ha de contenir cap signe d'addició (+).	**Ubicació** `/etc/security/pscexpert/dodv2/printers` **Acció de conformitat** Garanteix que el sistema compleix els requeriments especificats.

Taula 2. Requeriments generals del departament de defensa (continuació)

ID de punt de comprovació de la guia per a la implementació tècnica de seguretat del departament de defensa	Categoria de la regla STIG	Descripció	Ubicació de l'script on es defineix l'acció i els resultats de l'acció que permeten la conformitat
GEN004220	1	Els comptes administratius no s'han d'executar en un navegador web a menys que els necessiti l'administració del servei local.	**Ubicació** `/etc/security/pscexpert/dodv2/dodv2cat1` **Acció de conformitat** Mostra els resultats de les proves de regles especificades.
GEN004460	2	Aquesta regla registra les dades `auth` i `info`.	**Ubicació** `/etc/security/pscexpert/dodv2/chsyslogdod` **Acció de conformitat** Habilita el registre de dades `auth` i `info`.

GEN004540	2	Aquesta regla inhabilita l'ordre d'ajuda `sendmail`.	**Ubicació**
			`/etc/security/pscexpert/dodv2/sendmailhelp`
			`/etc/security/pscexpert/dodv2/dodv2cmntrows`
			Acció de conformitat
			Inhabilita l'ordre especificada.

GEN004580	2	El sistema no ha d'utilitzar fitxers `.forward`.	**Ubicació** `/etc/security/pscexpert/dodv2/forward` **Acció de conformitat** Inhabilita els fitxers especificats. **Nota:** Aquest paràmetre no es canvia automàticament quan es restableix la política per defecte de l'AIX mitjançant el fitxer `DoDv2_to_ AIXDefault.xml`. Heu de canviar manualment aquest paràmetre.
GEN004600	1	El servei `SMTP` ha de ser la versió més recent.	**Ubicació** `/etc/security/pscexpert/dodv2/SMTP_ver` **Acció de conformitat** Garanteix que s'executi la versió més recent del servei especificat. **Nota:** Aquest paràmetre no es canvia automàticament quan es restableix la política per defecte de l'AIX mitjançant el fitxer `DoDv2_to_ AIXDefault.xml`. Heu de canviar manualment aquest paràmetre.
GEN004620	2	El servidor `sendmail` ha de tenir inhabilitada la funció de depuració.	**Ubicació** `/etc/security/pscexpert/dodv2/SMTP_ver` **Acció de conformitat** Inhabilita la característica de depuració `sendmail`.
GEN004640	1	El servei `SMTP` no ha de tenir cap àlies `uudecode` actiu.	**Ubicació** `/etc/security/pscexpert/dodv2/SMTPuucode` **Acció de conformitat** Inhabilita l'àlies `uudecode`.

Taula 2. Requeriments generals del departament de defensa (continuació)

ID de punt de comprovació de la guia per a la implementació tècnica de seguretat del departament de defensa	Categoria de la regla STIG	Descripció	Ubicació de l'script on es defineix l'acció i els resultats de l'acció que permeten la conformitat
GEN004710	2	Cal restringir la retransmissió de correu.	**Ubicació** `/etc/security/pscexpert/dodv2/sendmaildod` **Acció de conformitat** Restringeix la retransmissió de correu.
GEN004800	1,2,3	L'FTP no xifrat no s'ha d'utilitzar al sistema.	**Ubicació** `/etc/security/pscexpert/dodv2/inetdservices` **Acció de conformitat** Inhabilita els daemons i serveis necessaris descomentant les entrades al fitxer `/etc/inetd.conf`.
GEN004820	2	L'FTP anònim no ha d'estar actiu al sistema a menys que estigui autoritzat.	**Ubicació** `/etc/security/pscexpert/dodv2/anonuser` **Acció de conformitat** Inhabilita l'FTP anònim al sistema. **Nota:** Aquest paràmetre no es canvia automàticament quan es restableix la política per defecte de l'AIX mitjançant el fitxer `DoDv2_to_ AIXDefault.xml`. Heu de canviar manualment aquest paràmetre.
GEN004840	2	Si el sistema és un servidor FTP anònim, ha d'estar aïllat de la xarxa DMZ (zona desmilitaritzada).	**Ubicació** `/etc/security/pscexpert/dodv2/anonuser` **Acció de conformitat** Garanteix que l'FTP anònim del sistema estigui en la xarxa DMZ.
GEN004880	2	Ha d'existir el fitxer `ftpusers`.	**Ubicació** `/etc/security/pscexpert/dodv2/chdodftpusers` **Acció de conformitat** Garanteix que el fitxer especificat estigui al sistema.
GEN004900	2	El fitxer `ftpusers` ha de contenir els noms de comptes que no es permeten a l'hora d'utilitzar el protocol FTP.	**Ubicació** `/etc/security/pscexpert/dodv2/chdodftpusers` **Acció de conformitat** Garanteix que el fitxer conté els noms de comptes necessaris.
GEN005000	1	Els comptes d'FTP anònims no han de tenir cap intèrpret d'ordres funcional.	**Ubicació** `/etc/security/pscexpert/dodv2/usershells` **Acció de conformitat** Elimina els intèrprets d'ordres dels comptes FTP. **Nota:** Aquest paràmetre no es canvia automàticament quan es restableix la política per defecte de l'AIX mitjançant el fitxer `DoDv2_to_ AIXDefault.xml`. Heu de canviar manualment aquest paràmetre.
GEN005080	1	El daemon `TFTP` ha de funcionar en mode segur per proporcionar accés només a un únic directori al sistema de fitxers de l'amfitrió.	**Ubicació** `/etc/security/pscexpert/dodv2/tftpdod` **Acció de conformitat** Garanteix que el daemon compleix els requeriments especificats.

Taula 2. Requeriments generals del departament de defensa (continuació)

ID de punt de comprovació de la guia per a la implementació tècnica de seguretat del departament de defensa	Categoria de la regla STIG	Descripció	Ubicació de l'script on es defineix l'acció i els resultats de l'acció que permeten la conformitat
GEN005120	2	El daemon TFTP s'ha de configurar segons les especificacions del proveïdor, inclòs un compte d'usuari TFTP dedicat, un intèrpret d'ordres sense inici de sessió com, per exemple, un directori `/bin/false` i un directori base, que és propietat de l'usuari TFTP.	**Ubicació** `/etc/security/pscexpert/dodv2/tftpdod` **Acció de conformitat** Garanteix que el sistema compleix els requeriments especificats.
GEN005140	1,2,3	Qualsevol daemon TFTP ha d'estar autoritzat i aprovat al paquet d'acreditació del sistema.	**Ubicació** `/etc/security/pscexpert/dodv2/inetdservices` **Acció de conformitat** Garanteix que el daemon disposi d'autorització.
GEN005160	1,2	Qualsevol amfitrió del sistema X Window ha de registrar fitxers `.Xauthority`.	**Ubicació** `/etc/security/pscexpert/dodv2/dodv2disableX` **Acció de conformitat** Garanteix que l'amfitrió registri els fitxers especificats.
GEN005200	1,2	Les pantalles del sistema X Window no es poden exportar públicament.	**Ubicació** `/etc/security/pscexpert/dodv2/dodv2disableX` **Acció de conformitat** Inhabilita la difusió dels programes especificats.
GEN005220	1,2	S'han d'utilitzar els fitxers `.Xauthority` o `X*.hosts` (o algun d'equivalent) per restringir l'accés al servidor del sistema X Window.	**Ubicació** `/etc/security/pscexpert/dodv2/dodv2disableX` **Acció de conformitat** Garanteix que els fitxers especificats estan disponibles per restringits l'accés al servidor.
GEN005240	1,2	La utilitat .Xauthority ha de permetre l'accés només als amfitrions autoritzats.	**Ubicació** `/etc/security/pscexpert/dodv2/dodv2disableX` **Acció de conformitat** Garanteix que l'accés està limitat a amfitrions autoritzats.
GEN005260	2	Aquesta regla inhabilita les connexions del sistema X Window i del gestor d'inici de sessió de l'XServer.	**Ubicació** `/etc/security/pscexpert/dodv2/dodv2cmntrows` **Acció de conformitat** Inhabilita les connexions necessàries i el gestor d'inici de sessió.
GEN005280	1,2,3	El sistema no ha de tenir actiu el servei `UUCP`.	**Ubicació** `/etc/security/pscexpert/dodv2/inetdservices` **Acció de conformitat** Inhabilita els daemons i serveis necessaris descomentant les entrades al fitxer `/etc/inetd.conf`.

Taula 2. Requeriments generals del departament de defensa (continuació)

ID de punt de comprovació de la guia per a la implementació tècnica de seguretat del departament de defensa	Categoria de la regla STIG	Descripció	Ubicació de l'script on es defineix l'acció i els resultats de l'acció que permeten la conformitat
GEN005300	2	Cal canviar les comunitats SNMP dels paràmetres per defecte.	**Ubicació** `/etc/security/pscexpert/dodv2/chsnmp` **Acció de conformitat** Garanteix que el sistema compleix els requeriments especificats.
GEN005305	2	El servei SNMP ha d'utilitzar només la versió SNMPv3 o posterior.	**Ubicació** `/etc/security/pscexpert/dodv2/chsnmp` **Acció de conformitat** Garanteix que el sistema compleix els requeriments especificats.
GEN005306	2	El servei SNMP ha d'exigir que s'utilitzi la normativa 140-2 del FIPS.	**Ubicació** `/etc/security/pscexpert/dodv2/chsnmp` **Acció de conformitat** Garanteix que el sistema compleix els requeriments especificats.
GEN005440	2	El sistema ha d'utilitzar un servidor syslog remot (servidor amfitrió).	**Ubicació** `/etc/security/pscexpert/dodv2/EnableTrustedLogging` **Acció de conformitat** Garanteix que el sistema utilitzi un servidor syslog remot.
GEN005450	2	El sistema ha d'utilitzar un servidor syslog remot (servidor amfitrió).	**Ubicació** `/etc/security/pscexpert/dodv2/EnableTrustedLogging` **Acció de conformitat** Garanteix que el sistema utilitzi un servidor syslog remot.
GEN005460	2	El sistema ha d'utilitzar un servidor syslog remot (servidor amfitrió).	**Ubicació** `/etc/security/pscexpert/dodv2/EnableTrustedLogging` **Acció de conformitat** Garanteix que el sistema utilitzi un servidor syslog remot.
GEN005480	2	El sistema ha d'utilitzar un servidor syslog remot (servidor amfitrió).	**Ubicació** `/etc/security/pscexpert/dodv2/EnableTrustedLogging` **Acció de conformitat** Garanteix que el sistema utilitzi un servidor syslog remot.
GEN005500	2	El daemon `SSH` s'ha de configurar perquè utilitzi només el protocol Secure Shell, versió 2 (SSHv2).	**Ubicació** `/etc/security/pscexpert/dodv2/sshDoDconfig` **Acció de conformitat** Garanteix que el sistema compleix els requeriments especificats.

Taula 2. Requeriments generals del departament de defensa (continuació)

ID de punt de comprovació de la guia per a la implementació tècnica de seguretat del departament de defensa	Categoria de la regla STIG	Descripció	Ubicació de l'script on es defineix l'acció i els resultats de l'acció que permeten la conformitat
GEN005501	2	El client SSH s'ha de configurar perquè utilitzi només el protocol SSHv2.	**Ubicació** `/etc/security/pscexpert/dodv2/sshDoDconfig` **Acció de conformitat** Garanteix que el sistema compleix els requeriments especificats.
GEN005504	2	El daemon SSH només ha d'escoltar en adreces de xarxa de gestió a menys que disposi d'autorització per utilitzar-ne una altre que no sigui de gestió.	**Ubicació** `/etc/security/pscexpert/dodv2/sshDoDconfig` **Acció de conformitat** Garanteix que el sistema compleix els requeriments especificats.
GEN005505	2	El daemon SSH s'ha de configurar perquè utilitzi només xifrats compatibles amb els estàndards 140-2 del FIPS (Federal Information Processing Standards).	**Ubicació** `/etc/security/pscexpert/dodv2/sshDoDconfig` **Acció de conformitat** Garanteix que el sistema compleix els requeriments especificats.
GEN005506	2	El daemon SSH s'ha de configurar per utilitzar només xifrats compatibles amb els estàndards 140-2 del FIPS.	**Ubicació** `/etc/security/pscexpert/dodv2/sshDoDconfig` **Acció de conformitat** Garanteix que el sistema compleix els requeriments especificats.
GEN005507	2	El daemon SSH s'ha de configurar per utilitzar només MAC (Message Authentication Codes) amb algoritmes de hash criptogràfics compatibles amb els estàndards 140-2 del FIPS.	**Ubicació** `/etc/security/pscexpert/dodv2/sshDoDconfig` **Acció de conformitat** Garanteix que el sistema compleix els requeriments especificats.
GEN005510	2	El client SSH s'ha de configurar per utilitzar només MAC amb xifrats compatibles amb els estàndards 140-2 del FIPS.	**Ubicació** `/etc/security/pscexpert/dodv2/sshDoDconfig` **Acció de conformitat** Garanteix que el sistema compleix els requeriments especificats.
GEN005511	2	El client SSH s'ha de configurar per utilitzar només MAC amb xifrats compatibles amb els estàndards 140-2 del FIPS.	**Ubicació** `/etc/security/pscexpert/dodv2/sshDoDconfig` **Acció de conformitat** Garanteix que el sistema compleix els requeriments especificats.

Taula 2. Requeriments generals del departament de defensa (continuació)

ID de punt de comprovació de la guia per a la implementació tècnica de seguretat del departament de defensa	Categoria de la regla STIG	Descripció	Ubicació de l'script on es defineix l'acció i els resultats de l'acció que permeten la conformitat
GEN005512	2	El daemon SSH s'ha de configurar per utilitzar només MAC amb algoritmes de hash criptogràfics compatibles amb els estàndards 140-2 del FIPS.	**Ubicació** /etc/security/pscexpert/dodv2/sshDoDconfig **Acció de conformitat** Garanteix que el sistema compleix els requeriments especificats.
GEN005521	2	El daemon SSH ha de restringir l'inici de sessió a usuaris específics, grups específics o tots dos.	**Ubicació** /etc/security/pscexpert/dodv2/sshDoDconfig **Acció de conformitat** Garanteix que el sistema compleix els requeriments especificats.
GEN005536	2	El daemon SSH ha de realitzar la comprovació de mode estricte dels fitxers de configuració del directori inicial.	**Ubicació** /etc/security/pscexpert/dodv2/sshDoDconfig **Acció de conformitat** Garanteix que el sistema compleix els requeriments especificats.
GEN005537	2	El daemon SSH ha d'utilitzar la separació de privilegis.	**Ubicació** /etc/security/pscexpert/dodv2/sshDoDconfig **Acció de conformitat** Garanteix que el sistema compleix els requeriments especificats.
GEN005538	2	El daemon SSH no ha de permetre l'autenticació rhosts mitjançant l'RSA (Rivest-Shamir-Adleman).	**Ubicació** /etc/security/pscexpert/dodv2/sshDoDconfig **Acció de conformitat** Garanteix que el sistema compleix els requeriments especificats.
GEN005539	2	El daemon SSH no ha de permetre la compressió o ha de permetre la compressió només després d'una autenticació satisfactòria.	**Ubicació** /etc/security/pscexpert/dodv2/sshDoDconfig **Acció de conformitat** Garanteix que el sistema compleix els requeriments especificats.
GEN005550	2	El daemon SSH s'ha de configurar amb el bàner d'inici de sessió del departament de defensa.	**Ubicació** /etc/security/pscexpert/dodv2/sshDoDconfig **Acció de conformitat** Garanteix que el sistema compleix els requeriments especificats.

Taula 2. Requeriments generals del departament de defensa (continuació)

ID de punt de comprovació de la guia per a la implementació tècnica de seguretat del departament de defensa	Categoria de la regla STIG	Descripció	Ubicació de l'script on es defineix l'acció i els resultats de l'acció que permeten la conformitat
GEN005560	2	Determina si hi ha una passarel•la per defecte que s'hagi configurat per a l'IPv4.	**Ubicació** `/etc/security/pscexpert/dodv2/chkgtway` **Acció de conformitat** Garanteix que el sistema compleix els requeriments especificats. **Nota:** Aquest paràmetre no es canvia automàticament quan es restableix la política per defecte de l'AIX mitjançant el fitxer `DoDv2_to_ AIXDefault.xml`. Heu de canviar manualment aquest paràmetre. **Nota:** Si el sistema executa el protocol IPv6, assegureu-vos que el paràmetre *ipv6_enabled* del fitxer `/etc/security/pscexpert/ipv6.conf` s'hagi establert en el valor `yes`. Si el sistema no utilitza l'IPv6, assegueu-vos que el valor *ipv6_enabled* s'hagi establert en `no`.
GEN005570	2	Determina si hi ha una passarel•la per defecte que s'hagi configurat per a l'IPv6.	**Ubicació** `/etc/security/pscexpert/dodv2/chkgtway` **Acció de conformitat** Garanteix que el sistema compleix els requeriments especificats. **Nota:** Aquest paràmetre no es canvia automàticament quan es restableix la política per defecte de l'AIX mitjançant el fitxer `DoDv2_to_ AIXDefault.xml`. Heu de canviar manualment aquest paràmetre. **Nota:** Si el sistema executa el protocol IPv6, assegureu-vos que el paràmetre *ipv6_enabled* del fitxer `/etc/security/pscexpert/ipv6.conf` s'hagi establert en el valor `yes`. Si el sistema no utilitza l'IPv6, assegueu-vos que el valor *ipv6_enabled* s'hagi establert en `no`.
GEN005590	2	El sistema no ha d'executar cap daemon del protocol d'encaminament a menys que el sistema sigui un encaminador.	**Ubicació** `/etc/security/pscexpert/dodv2/dodv2cmntrows` **Acció de conformitat** Garanteix que el sistema compleix els requeriments especificats.
GEN005590	2	El sistema no ha d'executar cap daemon del protocol d'encaminament a menys que el sistema sigui un encaminador.	**Ubicació** `/etc/security/pscexpert/dodv2/dodv2cmntrows` **Acció de conformitat** Garanteix que el sistema compleix els requeriments especificats.
GEN005600	2	L'acció de remetre l'IP de l'IPv4 no ha d'estar habilitada a menys que el sistema sigui un encaminador.	**Ubicació** `/etc/security/pscexpert/dodv2/ntwkoptsdod` **Acció de conformitat** Estableix el valor de l'opció de xarxa `ipforwarding` a *0*.

Taula 2. Requeriments generals del departament de defensa (continuació)

ID de punt de comprovació de la guia per a la implementació tècnica de seguretat del departament de defensa	Categoria de la regla STIG	Descripció	Ubicació de l'script on es defineix l'acció i els resultats de l'acció que permeten la conformitat
GEN005610	2	El sistema no ha de tenir habilitada l'acció de remetre l'IP de l'IPv6 a menys que el sistema sigui un encaminador IPv6.	**Ubicació** `/etc/security/pscexpert/dodv2/ntwkoptsdod` **Acció de conformitat** Estableix el valor de l'opció de xarxa `ip6forwarding` a *1*.
GEN005820	2	Els UID i GID anònims de l'NFS s'han d'haver configurat en valors sense permisos.	**Ubicació** `/etc/security/pscexpert/dodv2/nfsoptions` **Acció de conformitat** Garanteix que els ID especificats no tindran permisos.
GEN005840	2	El servidor NFS s'han de configurar per restringir l'accés del sistema local als amfitrions locals.	**Ubicació** `/etc/security/pscexpert/dodv2/nfsoptions` **Acció de conformitat** Configura el servidor NFS perquè restringeixi l'accés als amfitrions locals.
GEN005880	2	El servidor NFS no ha de permetre l'accés root remot.	**Ubicació** `/etc/security/pscexpert/dodv2/nfsoptions` **Acció de conformitat** Inhabilita l'accés root remot en el servidor NFS.
GEN005900	2	L'opció *nosuid* ha d'estar habilitada en tots el muntatges de client NFS.	**Ubicació** `/etc/security/pscexpert/dodv2/nosuid` **Acció de conformitat** Habilita l'opció *nosuid* en tots els muntatges de client NFS.
GEN006060	2	El client no ha d'executar `Samba` a menys que sigui necessari.	**Ubicació** `/etc/security/pscexpert/dodv2/dodv2services` **Acció de conformitat** Garanteix que el sistema compleix els requeriments especificats.
GEN006380	1	El sistema no ha d'utilitzar UDP per a NIS o NIS+.	**Ubicació** `/etc/security/pscexpert/dodv2/dodv2cat1` **Acció de conformitat** Mostra els resultats de les proves de regles especificades.
GEN006400	2	El protocol NIS (Network Information System - sistema d'informació de xarxa) no s'ha d'utilitzar.	**Ubicació** `/etc/security/pscexpert/dodv2/nisplus` **Acció de conformitat** Inhabilita el protocol especificat. **Nota:** Aquest paràmetre no es canvia automàticament quan es restableix la política per defecte de l'AIX mitjançant el fitxer `DoDv2_to_ AIXDefault.xml`. Heu de canviar manualment aquest paràmetre.

Taula 2. Requeriments generals del departament de defensa (continuació)

ID de punt de comprovació de la guia per a la implementació tècnica de seguretat del departament de defensa	Categoria de la regla STIG	Descripció	Ubicació de l'script on es defineix l'acció i els resultats de l'acció que permeten la conformitat
GEN006420	2	Les correlacions NIS han d'estar protegides amb noms de domini difícils d'esbrinar.	**Ubicació** `/etc/security/pscexpert/dodv2/nisplus` **Acció de conformitat** Garanteix que els noms de domini no siguin fàcils de determinar.
GEN006460	2	Tot servidor NIS+ ha de funcionar amb un nivell de seguretat 2.	**Ubicació** `/etc/security/pscexpert/dodv2/nisplus` **Acció de conformitat** Garanteix que el servidor tingui el nivell de seguretat mínim especificat. **Nota:** Aquest paràmetre no es canvia automàticament quan es restableix la política per defecte de l'AIX mitjançant el fitxer `DoDv2_to_ AIXDefault.xml`. Heu de canviar manualment aquest paràmetre.
GEN006480	2	Cal comprovar setmanalment el sistema perquè no hi hagi fitxers `setuid` no autoritzats ni cap modificació de no autorització a fitxers `setuid` autoritzats.	**Ubicació** `/etc/security/pscexpert/dodv2/trust` **Acció de conformitat** Comprova setmanalment que s'identifiquin els canvis als fitxers especificats.
GEN006560	2	Cal comprovar setmanalment el sistema perquè no hi hagi fitxers `setuid` no autoritzats ni cap modificació de no autorització a fitxers `setuid` autoritzats.	**Ubicació** `/etc/security/pscexpert/dodv2/trust` **Acció de conformitat** Comprova setmanalment que s'identifiquin els canvis als fitxers especificats.
GEN006580	2	El sistema ha d'utilitzar un programa de control d'accés.	**Ubicació** `/etc/security/pscexpert/dodv2/checktcpd` **Acció de conformitat** Garanteix que el sistema compleix els requeriments especificats.
GEN006600	2	El programa de control d'accés del sistema ha d'enregistrar tots els intents d'accés del sistema.	**Ubicació** `/etc/security/pscexpert/dodv2/chsyslogdod` **Acció de conformitat** Garanteix que s'enregistrin els intents d'accés.
GEN006620	2	El programa de control d'accés del sistema s'ha de configurar per garantir o denegar l'accés del sistema a amfitrions específics.	**Ubicació** `/etc/security/pscexpert/dodv2/chetchostsdod` **Acció de conformitat** Configura els fitxers `hosts.deny` i `hosts.allow` als paràmetres necessaris.

Taula 2. Requeriments generals del departament de defensa (continuació)

ID de punt de comprovació de la guia per a la implementació tècnica de seguretat del departament de defensa	Categoria de la regla STIG	Descripció	Ubicació de l'script on es defineix l'acció i els resultats de l'acció que permeten la conformitat
GEN007020	2	El protocol SCTP (Stream Control Transmission Protocol) ha d'estar inhabilitat.	**Ubicació** `/etc/security/pscexpert/dodv2/dodv2netrules` **Acció de conformitat** Inhabilita el protocol especificat.
GEN007700	2	El manejador de protocol IPv6 no ha d'estar limitat a la pila de xarxa a menys que sigui necessari.	**Ubicació** `/etc/security/pscexpert/dodv2/rminet6` **Acció de conformitat** Inhabilita el manejador de protocol IPv6 de la pila de xarxa a menys que s'especifiqui el manejador al fitxer `/etc/ipv6.conf`. **Nota:** Si el sistema executa el protocol IPv6, assegureu-vos que el paràmetre *ipv6_enabled* del fitxer `/etc/security/pscexpert/ipv6.conf` s'hagi establert en el valor `yes`. Si el sistema no utilitza l'IPv6, assegueu-vos que el valor *ipv6_enabled* s'hagi establert en `no`.
GEN007780	2	El sistema no té habilitats el túnels `6to4`.	**Ubicació** `/etc/security/pscexpert/dodv2/rmiface` **Acció de conformitat** Inhabilita els túnels especificats. **Nota:** Aquest paràmetre no es canvia automàticament quan es restableix la política per defecte de l'AIX mitjançant el fitxer `DoDv2_to_ AIXDefault.xml`. Heu de canviar manualment aquest paràmetre.
GEN007820	2	El sistema no ha de tenir túnels d'IP configurats.	**Ubicació** `/etc/security/pscexpert/dodv2/rmtunnel` **Acció de conformitat** Inhabilita els túnels d'IP. **Nota:** Aquest paràmetre no es canvia automàticament quan es restableix la política per defecte de l'AIX mitjançant el fitxer `DoDv2_to_ AIXDefault.xml`. Heu de canviar manualment aquest paràmetre.
GEN007840	2	El client `DHCP` ha d'estar inhabilitat si no s'utilitza.	**Ubicació** `/etc/security/pscexpert/dodv2/dodv2services` **Acció de conformitat** Garanteix que el sistema compleix els requeriments especificats.
GEN007850	2	El client `DHCP` no ha d'enviar actualitzacions DNS dinàmiques.	**Ubicació** `/etc/security/pscexpert/dodv2/dodv2services` **Acció de conformitat** Garanteix que el sistema compleix els requeriments especificats.

Taula 2. Requeriments generals del departament de defensa (continuació)

ID de punt de comprovació de la guia per a la implementació tècnica de seguretat del departament de defensa	Categoria de la regla STIG	Descripció	Ubicació de l'script on es defineix l'acció i els resultats de l'acció que permeten la conformitat
GEN007860	2	El sistema ha d'ignorar els missatges de redirecció d'ICMP d'IPv6.	**Ubicació** `/etc/security/pscexpert/dodv2/ntwkoptsdod` **Acció de conformitat** Estableix el valor de l'opció de xarxa `ipignoreredirects` a *1*.
GEN007880	2	El sistema no ha d'enviar redireccions d'ICMP d'IPv6.	**Ubicació** `/etc/security/pscexpert/dodv2/ntwkoptsdod` **Acció de conformitat** Estableix el valor de l'opció de xarxa `ipsendredirects` a *0*.
GEN007900	2	El sistema ha d'utilitzar un filtre de camí d'accés invers adequat pel tràfic de xarxa IPv6, si el sistema utilitza IPv6.	**Ubicació** `/etc/security/pscexpert/dodv2/chuserstanzadod` **Acció de conformitat** Garanteix que el sistema compleix els requeriments especificats.
GEN007920	2	l sistema no ha de remetre paquets amb direccionament d'origen IPv6.	**Ubicació** `/etc/security/pscexpert/dodv2/ntwkoptsdod` **Acció de conformitat** Estableix el valor de l'opció de xarxa `ip6srcrouteforward` a *0*.
GEN007940: GEN003607	2	El sistema no ha d'acceptar paquets d'IPv4 i IPv6 amb direccionament d'origen.	**Ubicació** `/etc/security/pscexpert/dodv2/ntwkoptsdod` **Acció de conformitat** Estableix el valor de l'opció de xarxa `ipsrcrouterecv` a *0*.
GEN007950	2	El sistema no ha de respondre a les sol•licituds d'eco d'ICMPv6 que s'envien a una adreça de difusió.	**Ubicació** `/etc/security/pscexpert/dodv2/ntwkoptsdod` **Acció de conformitat** Estableix el valor de l'opció de xarxa `bcastping` a *0*.
GEN008000	2	Si el sistema utilitza l'LDAP (Lightweight Directory Access Protocol) per a la informació d'autenticació o de compte. Els certificats que s'utilitzen per autenticar el servidor LDAP s'han de proporcionar des de la PKI del departament de defensa o per una PKI externa aprovada pel departament de defensa.	**Ubicació** `/etc/security/pscexpert/dodv2/ldap_config` **Acció de conformitat** Garanteix que el sistema compleix els requeriments especificats.

Taula 2. Requeriments generals del departament de defensa (continuació)

ID de punt de comprovació de la guia per a la implementació tècnica de seguretat del departament de defensa	Categoria de la regla STIG	Descripció	Ubicació de l'script on es defineix l'acció i els resultats de l'acció que permeten la conformitat
GEN008020	2	Si el sistema utilitza LDAP per a la informació d'autenticació o de comptes, la connexió TLS (Transport Layer Security) d'LDAP ha de requerir que el servidor proporcioni un certificat amb un camí d'accés fiable vàlid.	**Ubicació** `/etc/security/pscexpert/dodv2/ldap_config` **Acció de conformitat** Garanteix que el sistema compleix els requeriments especificats.
GEN008050	2	Si el sistema utilitza LDAP per a la informació d'autenticació o de comptes, el fitxer `/etc/ldap.conf` (o un d'equivalent) no ha de contenir contrasenyes.	**Ubicació** `/etc/security/pscexpert/dodv2/ldap_config` **Acció de conformitat** Garanteix que el sistema compleix els requeriments especificats.
GEN008380	2	Cal comprovar setmanalment el sistema perquè no hi hagi fitxers `setuid` no autoritzats ni cap modificació de no autorització a fitxers `setuid` autoritzats.	**Ubicació** `/etc/security/pscexpert/dodv2/trust` **Acció de conformitat** Comprova setmanalment que s'identifiquin els canvis als fitxers especificats.
GEN008520	2	El sistema ha d'utilitzar un tallafoc local que protegeix l'amfitrió de les exploracions de port. El tallafoc ha de rebutjar els ports vulnerables durant 5 minuts per protegir l'amfitrió de les exploracions de port.	**Ubicació** `/etc/security/pscexpert/dodv2/ipsecshunports` **Acció de conformitat** Garanteix que el sistema compleix els requeriments especificats.
GEN008540	2	El tallafoc local del sistema ha d'implementar una política *deny-all, allow-by-exception*.	**Ubicació** `/etc/security/pscexpert/dodv2/ipsecshunhosthls` **Acció de conformitat** Garanteix que el sistema compleix els requeriments especificats. **Nota:** Podeu escriure regles de filtre addicionals al fitxer `/etc/security/aixpert/bin/filter.txt`. Aquestes regles s'integren a l'script `ipsecshunhosthls.sh` quan s'aplica el perfil. Les entrades han de tenir el format següent: *`número_port`*`:`*`adreça_ip`*`:` *`acció`* en què els valors possibles d'*acció* són `Allow` o `Deny`.

Taula 2. Requeriments generals del departament de defensa (continuació)

ID de punt de comprovació de la guia per a la implementació tècnica de seguretat del departament de defensa	Categoria de la regla STIG	Descripció	Ubicació de l'script on es defineix l'acció i els resultats de l'acció que permeten la conformitat
GEN008600	1	El sistema s'ha de configurar perquè s'inicií només des de la configuració d'engegada del sistema.	**Ubicació** `/etc/security/pscexpert/dodv2/dodv2cat1` **Acció de conformitat** Garanteix que l'inici del sistema utilitzi només la configuració d'engegada del sistema.
GEN008640	1	El sistema no ha d'utilitzar suports d'emmagatzematge extraïbles com a carregador d'engegada.	**Ubicació** `/etc/security/pscexpert/dodv2/dodv2cat1` **Acció de conformitat** Garanteix que el sistema no s'engega des d'una unitat extraïble.
GEN009140	1,2,3	El sistema no ha de tenir actiu el servei `chargen`.	**Ubicació** `/etc/security/pscexpert/dodv2/inetdservices` **Acció de conformitat** Inhabilita els daemons i serveis necessaris descomentant les entrades al fitxer `/etc/inetd.conf`.
GEN009160	1,2,3	El sistema no ha de tenir actiu el sistema `Calendar Management Service Daemon` (CMSD).	**Ubicació** `/etc/security/pscexpert/dodv2/inetdservices` **Acció de conformitat** Inhabilita els daemons i serveis necessaris descomentant les entrades al fitxer `/etc/inetd.conf`.
GEN009180	1,2,3	El sistema no ha de tenir actiu el servei `tool-talk database server` (ttdbserver).	**Ubicació** `/etc/security/pscexpert/dodv2/inetdservices` **Acció de conformitat** Inhabilita els daemons i serveis necessaris descomentant les entrades al fitxer `/etc/inetd.conf`.
GEN009190	1,2,3	El sistema no ha de tenir actiu el servei `comsat`.	**Ubicació** `/etc/security/pscexpert/dodv2/inetdservices` **Acció de conformitat** Inhabilita els daemons i serveis necessaris descomentant les entrades al fitxer `/etc/inetd.conf`.
GEN009200-9330	1,2,3	El sistema no pot tenir actius altres serveis i daemons.	**Ubicació** `/etc/security/pscexpert/dodv2/inetdservices` **Acció de conformitat** Inhabilita els daemons i serveis necessaris descomentant les entrades al fitxer `/etc/inetd.conf`.
GEN009210	2	El sistema no ha de tenir actiu el servei `discard`.	**Ubicació** `/etc/security/pscexpert/dodv2/inetdservices` **Acció de conformitat** Inhabilita els daemons i serveis necessaris descomentant les entrades al fitxer `/etc/inetd.conf`.

Taula 2. Requeriments generals del departament de defensa (continuació)

ID de punt de comprovació de la guia per a la implementació tècnica de seguretat del departament de defensa	Categoria de la regla STIG	Descripció	Ubicació de l'script on es defineix l'acció i els resultats de l'acció que permeten la conformitat
GEN009220	2	El sistema no ha de tenir actiu el servei `dtspc`.	**Ubicació** `/etc/security/pscexpert/dodv2/inetdservices` **Acció de conformitat** Inhabilita els daemons i serveis necessaris descomentant les entrades al fitxer `/etc/inetd.conf`.
GEN009230	2	El sistema no ha de tenir actiu el servei `echo`.	**Ubicació** `/etc/security/pscexpert/dodv2/inetdservices` **Acció de conformitat** Inhabilita els daemons i serveis necessaris descomentant les entrades al fitxer `/etc/inetd.conf`.
GEN009240	2	El sistema no ha de tenir actiu el servei `Internet Message Access Protocol (IMAP)`.	**Ubicació** `/etc/security/pscexpert/dodv2/inetdservices` **Acció de conformitat** Inhabilita els daemons i serveis necessaris descomentant les entrades al fitxer `/etc/inetd.conf`.
GEN009250	2	El sistema no ha de tenir actiu el servei `PostOffice Protocol (POP3)`.	**Ubicació** `/etc/security/pscexpert/dodv2/inetdservices` **Acció de conformitat** Inhabilita els daemons i serveis necessaris descomentant les entrades al fitxer `/etc/inetd.conf`.
GEN009260	2	El sistema no ha de tenir actiu els serveis de diàleg o `ntalk`.	**Ubicació** `/etc/security/pscexpert/dodv2/inetdservices` **Acció de conformitat** Inhabilita els daemons i serveis necessaris descomentant les entrades al fitxer `/etc/inetd.conf`.
GEN009270	2	El sistema no ha de tenir actiu el servei `netstat` al procés InetD.	**Ubicació** `/etc/security/pscexpert/dodv2/inetdservices` **Acció de conformitat** Inhabilita els daemons i serveis necessaris descomentant les entrades al fitxer `/etc/inetd.conf`.
GEN009280	2	El sistema no ha de tenir actiu el servei `PCNFS`.	**Ubicació** `/etc/security/pscexpert/dodv2/inetdservices` **Acció de conformitat** Inhabilita els daemons i serveis necessaris descomentant les entrades al fitxer `/etc/inetd.conf`.
GEN009290	2	El sistema no ha de tenir actiu el servei `systat`.	**Ubicació** `/etc/security/pscexpert/dodv2/inetdservices` **Acció de conformitat** Inhabilita els daemons i serveis necessaris descomentant les entrades al fitxer `/etc/inetd.conf`.

Taula 2. Requeriments generals del departament de defensa (continuació)

ID de punt de comprovació de la guia per a la implementació tècnica de seguretat del departament de defensa	Categoria de la regla STIG	Descripció	Ubicació de l'script on es defineix l'acció i els resultats de l'acció que permeten la conformitat
GEN009300	2	El servei `inetd time` no ha d'estar actiu al daemon `inetd` del sistema.	**Ubicació** `/etc/security/pscexpert/dodv2/inetdservices` **Acció de conformitat** Inhabilita els daemons i serveis necessaris descomentant les entrades al fitxer `/etc/inetd.conf`.
GEN009310	2	El sistema no ha de tenir actiu el servei `rusersd`.	**Ubicació** `/etc/security/pscexpert/dodv2/inetdservices` **Acció de conformitat** Inhabilita els daemons i serveis necessaris descomentant les entrades al fitxer `/etc/inetd.conf`.
GEN009320	2	El sistema no ha de tenir actiu el servei `sprayd`.	**Ubicació** `/etc/security/pscexpert/dodv2/inetdservices` **Acció de conformitat** Inhabilita els daemons i serveis necessaris descomentant les entrades al fitxer `/etc/inetd.conf`.
GEN009330	2	El sistema no ha de tenir actiu el servei `rstatd`.	**Ubicació** `/etc/security/pscexpert/dodv2/inetdservices` **Acció de conformitat** Inhabilita els daemons i serveis necessaris descomentant les entrades al fitxer `/etc/inetd.conf`.
GEN009340	2	Els gestor d'inici de sessió del servidor X no ha d'estar en execució a menys que sigui necessari per a la gestió de sessions d'X11.	**Ubicació** `/etc/security/pscexpert/dodv2/dodv2cmntrows` **Acció de conformitat** Aquesta regla inhabilita les connexions del sistema X Window i del gestor d'inici de sessió de l'XServer.

Taula 3. Requeriments de propietat del departament de defensa

ID de punt de comprovació de la guia per a la implementació tècnica de seguretat del departament de defensa	Descripció	Ubicació de l'script on es defineix l'acció i els resultats de l'acció que permeten la conformitat
AIX00085	El fitxer `/etc/netsvc.conf` ha de ser propietat de l'usuari root.	**Ubicació** `/etc/security/pscexpert/dodv2/chowndodfiles` **Acció de conformitat** Garanteix que el fitxer especificat sigui propietat de l'usuari root.

Taula 3. Requeriments de propietat del departament de defensa (continuació)

ID de punt de comprovació de la guia per a la implementació tècnica de seguretat del departament de defensa	Descripció	Ubicació de l'script on es defineix l'acció i els resultats de l'acció que permeten la conformitat
AIX00090	El fitxer `/etc/netsvc.conf` ha de ser propietat de grup de l'usuari bin, sys o system.	**Ubicació** `/etc/security/pscexpert/dodv2/chowndodfiles` **Acció de conformitat** Garanteix que el fitxer especificat sigui propietat de grup de l'usuari bin, sys o system.
AIX00320	El fitxer `/etc/ftpaccess.ctl` ha de ser propietat de l'usuari root.	**Ubicació** `/etc/security/pscexpert/dodv2/chowndodfiles` **Acció de conformitat** Garanteix que el fitxer especificat sigui propietat de l'usuari root.
AIX00330	El fitxer `/etc/ftpaccess.ctl` ha de ser propietat de grup de l'usuari bin, sys o system.	**Ubicació** `/etc/security/pscexpert/dodv2/chowndodfiles` **Acció de conformitat** Garanteix que el fitxer especificat sigui propietat de grup de l'usuari bin, sys o system.
GEN000250	El fitxer de configuració de sincronització horària (com, per exemple, `/etc/ntp.conf`) ha de ser propietat de l'usuari root.	**Ubicació** `/etc/security/pscexpert/dodv2/chowndodfiles` **Acció de conformitat** Garanteix que el fitxer especificat sigui propietat de l'usuari root.
GEN000251	El fitxer de configuració de sincronització horària (com, per exemple `/etc/ntp.conf`) ha de ser propietat de grup de l'usuari bin, sys o system.	**Ubicació** `/etc/security/pscexpert/dodv2/chowndodfiles` **Acció de conformitat** Garanteix que el fitxer especificat sigui propietat de grup de l'usuari bin, sys o system.
GEN001160	Tots els fitxers i els directoris han de tenir un propietari vàlid.	**Ubicació** `/etc/security/pscexpert/dodv2/chowndodfiles` **Acció de conformitat** Garanteix tots els fitxers i directoris que tinguin un propietari vàlid.
GEN001170	Tots els fitxers i els directoris han de tenir un propietari de grup vàlid.	**Ubicació** `/etc/security/pscexpert/dodv2/chowndodfiles` **Acció de conformitat** Garanteix tots els fitxers i directoris que tinguin un propietari vàlid.

Taula 3. Requeriments de propietat del departament de defensa (continuació)

ID de punt de comprovació de la guia per a la implementació tècnica de seguretat del departament de defensa	Descripció	Ubicació de l'script on es defineix l'acció i els resultats de l'acció que permeten la conformitat
GEN001220	Tots els fitxers, programes i directoris del sistema han de ser propietat d'un compte del sistema.	**Ubicació** `/etc/security/pscexpert/dodv2/chowndodfiles` **Acció de conformitat** Garanteix que els fitxers, programes i directoris del sistema siguin propietat d'un compte del sistema.
GEN001240	Els fitxers, programes i directoris del sistema han de ser propietat de grup d'un grup del sistema.	**Ubicació** `/etc/security/pscexpert/dodv2/chowndodfiles` **Acció de conformitat** Tots els fitxers, programes i directoris del sistema han de ser propietat de grup d'un grup del sistema.
GEN001320	Els fitxers Network Information Systems (NIS)/NIS+/yp han de ser propietat de l'usuari root, sys o bin.	**Ubicació** `/etc/security/pscexpert/dodv2/chowndodfiles` **Acció de conformitat** Garanteix que els fitxers especificats siguin propietat de l'usuari root, sys o bin.
GEN001340	Els fitxers NIS/NIS+/yp han de ser propietat de grup de l'usuari sys, bin, other o system.	**Ubicació** `/etc/security/pscexpert/dodv2/chowndodfiles` **Acció de conformitat** Garanteix que els fitxers especificats siguin propietat de l'usuari sys, bin, other o system.
GEN001362	El fitxer `/etc/resolv.conf` ha de ser propietat de l'usuari root.	**Ubicació** `/etc/security/pscexpert/dodv2/chowndodfiles` **Acció de conformitat** Garanteix que el fitxer especificat sigui propietat de l'usuari root.
GEN001363	El fitxer `/etc/resolv.conf` ha de ser propietat de grup de l'usuari bin, sys o system.	**Ubicació** `/etc/security/pscexpert/dodv2/chowndodfiles` **Acció de conformitat** Garanteix que el fitxer especificat sigui propietat de grup de l'usuari bin, sys o system.
GEN001366	El fitxer `/etc/hosts` ha de ser propietat de l'usuari root.	**Ubicació** `/etc/security/pscexpert/dodv2/chowndodfiles` **Acció de conformitat** Garanteix que el fitxer especificat sigui propietat de l'usuari root.

Taula 3. Requeriments de propietat del departament de defensa (continuació)

ID de punt de comprovació de la guia per a la implementació tècnica de seguretat del departament de defensa	Descripció	Ubicació de l'script on es defineix l'acció i els resultats de l'acció que permeten la conformitat
GEN001367	El fitxer `/etc/hosts` ha de ser propietat de grup de l'usuari bin, sys o system.	**Ubicació** `/etc/security/pscexpert/dodv2/chowndodfiles` **Acció de conformitat** Garanteix que el fitxer especificat sigui propietat de grup de l'usuari bin, sys o system.
GEN001371	El fitxer `/etc/nsswitch.conf` ha de ser propietat de l'usuari root.	**Ubicació** `/etc/security/pscexpert/dodv2/chowndodfiles` **Acció de conformitat** Garanteix que el fitxer especificat sigui propietat de l'usuari root.
GEN001372	El fitxer `/etc/nsswitch.conf` ha de ser propietat de grup de l'usuari root, bin, sys o system.	**Ubicació** `/etc/security/pscexpert/dodv2/chowndodfiles` **Acció de conformitat** Garanteix que el fitxer especificat sigui propietat de grup de l'usuari root, bin, sys o system.
GEN001378	El fitxer `/etc/passwd` ha de ser propietat de l'usuari root.	**Ubicació** `/etc/security/pscexpert/dodv2/chowndodfiles` **Acció de conformitat** Garanteix que el fitxer especificat sigui propietat de l'usuari root.
GEN001379	El fitxer `/etc/passwd` ha de ser propietat de grup de l'usuari bin, security, sys o system.	**Ubicació** `/etc/security/pscexpert/dodv2/chowndodfiles` **Acció de conformitat** Garanteix que el fitxer especificat sigui propietat de grup de l'usuari bin, security, sys o system.
GEN001391	El fitxer `/etc/group` ha de ser propietat de l'usuari root	**Ubicació** `/etc/security/pscexpert/dodv2/chowndodfiles` **Acció de conformitat** Garanteix que el fitxer especificat sigui propietat de l'usuari root.
GEN001392	El fitxer `/etc/group` ha de ser propietat de grup de l'usuari bin, security, sys o system.	**Ubicació** `/etc/security/pscexpert/dodv2/chowndodfiles` **Acció de conformitat** Garanteix que el fitxer especificat sigui propietat de grup de l'usuari bin, security, sys o system.

Taula 3. Requeriments de propietat del departament de defensa (continuació)

ID de punt de comprovació de la guia per a la implementació tècnica de seguretat del departament de defensa	Descripció	Ubicació de l'script on es defineix l'acció i els resultats de l'acció que permeten la conformitat
GEN001400	El fitxer `/etc/security/passwd` ha de ser propietat de l'usuari root.	**Ubicació** `/etc/security/pscexpert/dodv2/chowndodfiles` **Acció de conformitat** Garanteix que el fitxer especificat sigui propietat de l'usuari root.
GEN001410	El fitxer `/etc/security/passwd` ha de ser propietat de grup de l'usuari bin, security, sys o system.	**Ubicació** `/etc/security/pscexpert/dodv2/chowndodfiles` **Acció de conformitat** Garanteix que el fitxer especificat sigui propietat de grup de l'usuari bin, security, sys o system.
GEN001500	Tots els directoris inicials d'usuaris interactius han de ser propietat dels respectius usuaris.	**Ubicació** `/etc/security/pscexpert/dodv2/chowndodfiles` **Acció de conformitat** Garanteix que tots els directoris inicials d'usuaris interactius siguin propietat dels respectius usuaris.
GEN001520	Tots els directoris inicials dels usuaris interactius han de ser propietat de grup del grup principal dels propietaris del directori inicial.	**Ubicació** `/etc/security/pscexpert/dodv2/chowndodfiles` **Acció de conformitat** Garanteix que tots els directoris inicials dels usuaris interactius siguin propietat de grup del grup principal dels propietaris del directori inicial.
GEN001540	Tots els fitxers i directoris que es troben als directoris inicials de l'usuari interactiu han de ser propietat del propietari del directori.	**Ubicació** `/etc/security/pscexpert/dodv2/chowndodfiles` **Acció de conformitat** Garanteix que tots els fitxers i directoris que es troben als directoris inicials de l'usuari interactiu siguin propietat del propietari del directori inicial.
GEN001550	Tots els fitxers i directoris que es troben als directoris inicials de l'usuari han de ser propietat de grup d'un grup on el propietari del directori inicial sigui un membre.	**Ubicació** `/etc/security/pscexpert/dodv2/chowndodfiles` **Acció de conformitat** Garanteix que tots els fitxers i directoris que es troben als directoris inicials de l'usuari siguin propietat de grup d'un grup on el propietari del directori inicial sigui un membre.

Taula 3. Requeriments de propietat del departament de defensa (continuació)

ID de punt de comprovació de la guia per a la implementació tècnica de seguretat del departament de defensa	Descripció	Ubicació de l'script on es defineix l'acció i els resultats de l'acció que permeten la conformitat
GEN001660	Tots els fitxers d'inici del sistema han de ser propietat de l'usuari root.	**Ubicació** `/etc/security/pscexpert/dodv2/chowndodfiles` **Acció de conformitat** Garanteix que els fitxers especificats siguin propietat de l'usuari root.
GEN001680	Tots els fitxers d'inici del sistema han de ser propietat de grup de l'usuari sys, bin, other o system.	**Ubicació** `/etc/security/pscexpert/dodv2/chowndodfiles` **Acció de conformitat** Garanteix que els fitxers especificats siguin propietat de grup de l'usuari sys, bin, other o system.
GEN001740	Tots els fitxers d'inicialització global han de ser propietat de l'usuari root.	**Ubicació** `/etc/security/pscexpert/dodv2/chowndodfiles` **Acció de conformitat** Garanteix que els fitxers especificats siguin propietat de l'usuari root.
GEN001760	Tots els fitxers d'inicialització global han de ser propietat de grup de l'usuari sys, bin, system o security.	**Ubicació** `/etc/security/pscexpert/dodv2/chowndodfiles` **Acció de conformitat** Garanteix que els fitxers especificats siguin propietat de grup de l'usuari sys, bin, system o security.
GEN001820	Tots els fitxers i directoris esquelet (que normalment es troben a `/etc/skel`) han de ser propietat de l'usuari root o bin.	**Ubicació** `/etc/security/pscexpert/dodv2/chowndodfiles` **Acció de conformitat** Garanteix que els fitxers i directoris especificats siguin propietat de l'usuari root o bin.
GEN001830	Tots els fitxers d'esquelet (que normalment es troben a `/etc/skel`) han de ser propietat de grup de l'usuari security.	**Ubicació** `/etc/security/pscexpert/dodv2/chowndodfiles` **Acció de conformitat** Garanteix que els fitxers especificats siguin propietat de grup de l'usuari security.
GEN001860	Tots els fitxers d'inicialització local han de ser propietat de l'usuari o de l'usuari arrel.	**Ubicació** `/etc/security/pscexpert/dodv2/chowndodfiles` **Acció de conformitat** Garanteix que els fitxers especificats siguin propietat de l'usuari o de l'usuari root.

Taula 3. Requeriments de propietat del departament de defensa (continuació)

ID de punt de comprovació de la guia per a la implementació tècnica de seguretat del departament de defensa	Descripció	Ubicació de l'script on es defineix l'acció i els resultats de l'acció que permeten la conformitat
GEN001870	Els fitxers d'inicialització local han de ser propietat de grup del grup primari de l'usuari o de l'usuari root.	**Ubicació** `/etc/security/pscexpert/dodv2/chowndodfiles` **Acció de conformitat** Garanteix que els fitxers d'inicialització local siguin propietat de grup del grup primari de l'usuari o de l'usuari root.

GEN002060	Només l'usuari o el propietari han de poder accedir als fitxers `.rhosts`, `.shosts`, `.netrc` o `hosts.equiv`.	**Ubicació**
		`/etc/security/pscexpert/dodv2/chowndodfiles`
		`/etc/security/pscexpert/dodv2/fpmdodfiles`
		Acció de conformitat
		Garanteix que només l'usuari root o el propietari puguin accedir als fitxers especificats.

GEN002100	El Pluggable Authentication Module (PAM) no ha d'admetre el fitxer `.rhosts`.	**Ubicació** `/etc/security/pscexpert/dodv2/chowndodfiles` **Acció de conformitat** Garanteix que el fitxer especificat no estigui disponible pel PAM.
GEN002200	Tots els fitxers de l'intèrpret d'ordres han de ser propietat de l'usuari root o bin.	**Ubicació** `/etc/security/pscexpert/dodv2/chowndodfiles` **Acció de conformitat** Garanteix que els fitxers especificats siguin propietat de l'usuari root o bin.
GEN002210	Tots els fitxers de l'intèrpret d'ordres han de ser propietat de grup de l'usuari root, bin, sys o system.	**Ubicació** `/etc/security/pscexpert/dodv2/chowndodfiles` **Acció de conformitat** Garanteix que els fitxers especificats siguin propietat de grup de l'usuari root, bin, sys o system.
GEN002340	Els dispositius d'àudio han de ser propietat de l'usuari root.	**Ubicació** `/etc/security/pscexpert/dodv2/chowndodfiles` **Acció de conformitat** Garanteix que tots els dispositius d'àudio siguin propietat de l'usuari root.

Taula 3. Requeriments de propietat del departament de defensa (continuació)

ID de punt de comprovació de la guia per a la implementació tècnica de seguretat del departament de defensa	Descripció	Ubicació de l'script on es defineix l'acció i els resultats de l'acció que permeten la conformitat
GEN002360	Els dispositius d'àudio han de ser propietat de grup de l'usuari root, sys, bin o system.	**Ubicació** `/etc/security/pscexpert/dodv2/chowndodfiles` **Acció de conformitat** Garanteix que tots els dispositius d'àudio siguin propietat de grup de l'usuari root, sys, bin o system.
GEN002520	Tots els directoris públics han de ser propietat de l'usuari root o d'un compte de l'aplicació.	**Ubicació** `/etc/security/pscexpert/dodv2/chowndodfiles` **Acció de conformitat** Garanteix que tots els directoris públics siguin propietat de l'usuari root o d'un compte de l'aplicació.
GEN002540	Tots els directoris públics han de ser propietat de grup d'un usuari system o d'un grup de l'aplicació.	**Ubicació** `/etc/security/pscexpert/dodv2/chowndodfiles` **Acció de conformitat** Garanteix que tots els directoris públics siguin propietat de grup de l'usuari system o d'un grup de l'aplicació.
GEN002680	Els registres d'auditoria del sistema han de ser propietat de l'usuari root.	**Ubicació** `/etc/security/pscexpert/dodv2/chowndodfiles` **Acció de conformitat** Garanteix que els fitxers especificats siguin propietat de l'usuari root.
GEN002690	Els registres d'auditoria del sistema han de ser propietat de grup de l'usuari bin, sys o system.	**Ubicació** `/etc/security/pscexpert/dodv2/chowndodfiles` **Acció de conformitat** Garanteix que els fitxers especificats siguin propietat de grup de l'usuari bin, sys o system.
GEN003020	La tasca `cron` no s'ha d'executar en programes de directoris amb permís d'escriptura global ni programes subordinats a aquest tipus de directoris.	**Ubicació** `/etc/security/pscexpert/dodv2/chowndodfiles` **Acció de conformitat** Evita que la tasca `cron` executi programes en directoris amb permís d'escriptura global, o programes que hi estiguin subordinats.

Taula 3. Requeriments de propietat del departament de defensa (continuació)

ID de punt de comprovació de la guia per a la implementació tècnica de seguretat del departament de defensa	Descripció	Ubicació de l'script on es defineix l'acció i els resultats de l'acció que permeten la conformitat
GEN003040	Les tasques `crontabs` han de ser propietat de l'usuari root o del creador de la tasca crontab.	**Ubicació** `/etc/security/pscexpert/dodv2/chowndodfiles` **Acció de conformitat** Garanteix que les tasques crontabs siguin propietat de l'usuari root o del creador de la tasca crontab.
GEN003050	Els fitxers de la tasca `crontab` han de ser propietat de grup de l'usuari system, cron o del grup primari del creador de la tasca crontab.	**Ubicació** `/etc/security/pscexpert/dodv2/chowndodfiles` **Acció de conformitat** Garanteix que els fitxers `crontab` siguin propietat de grup de l'usuari system, cron o del grup primari del creador de la tasca crontab.
GEN003110	Els directoris `cron` i `crontab` no ha de tenir llistes de control d'accés ampliades.	**Ubicació** `/etc/security/pscexpert/dodv2/chowndodfiles` **Acció de conformitat** Garanteix que els directoris especificats no tinguin llistes de control d'accés ampliades.
GEN003120	Els directoris `cron` i `crontab` han de ser propietat de l'usuari root o bin.	**Ubicació** `/etc/security/pscexpert/dodv2/chowndodfiles` **Acció de conformitat** Garanteix que els directoris cron i crontab siguin propietat de l'usuari root o bin.
GEN003140	Els directoris `cron` i `crontab` han de ser propietat de grup de l'usuari system, sys, bin o cron.	**Ubicació** `/etc/security/pscexpert/dodv2/chowndodfiles` **Acció de conformitat** Garanteix que els directoris especificats siguin propietat de grup de l'usuari system, sys, bin o cron.
GEN003160	El registre cron ha d'estar implementat.	**Ubicació** `/etc/security/pscexpert/dodv2/chowndodfiles` **Acció de conformitat** Garanteix que el registre cron s'hagi implementat.
GEN003240	El fitxer `cron.allow` ha de ser propietat de l'usuari root, bin o sys.	**Ubicació** `/etc/security/pscexpert/dodv2/chowndodfiles` **Acció de conformitat** Garanteix que el fitxer especificat sigui propietat de l'usuari root, bin o sys.

Taula 3. Requeriments de propietat del departament de defensa (continuació)

ID de punt de comprovació de la guia per a la implementació tècnica de seguretat del departament de defensa	Descripció	Ubicació de l'script on es defineix l'acció i els resultats de l'acció que permeten la conformitat
GEN003250	El fitxer `cron.allow` ha de ser propietat de l'usuari system, bin, sys o cron.	**Ubicació** `/etc/security/pscexpert/dodv2/chowndodfiles` **Acció de conformitat** Garanteix que el fitxer especificat sigui propietat de grup de l'usuari system, bin, sys o cron.
GEN003260	El fitxer `cron.deny` ha de ser propietat de l'usuari root, bin o sys.	**Ubicació** `/etc/security/pscexpert/dodv2/chowndodfiles` **Acció de conformitat** Garanteix que el fitxer especificat sigui propietat de l'usuari root, bin o sys.
GEN003270	El fitxer `cron.deny` ha de ser propietat de l'usuari system, bin, sys o cron.	**Ubicació** `/etc/security/pscexpert/dodv2/chowndodfiles` **Acció de conformitat** Garanteix que el fitxer especificat sigui propietat de grup de l'usuari system, bin, sys o cron.
GEN003420	El directori `at` ha de ser propietat de l'usuari root, bin, sys, daemon o cron.	**Ubicació** `/etc/security/pscexpert/dodv2/chowndodfiles` **Acció de conformitat** Garanteix que el directori especificat sigui propietat de l'usuari root, sys, daemon o cron.
GEN003430	El directori `at` ha de ser propietat de grup de l'usuari system, bin, sys o cron.	**Ubicació** `/etc/security/pscexpert/dodv2/chowndodfiles` **Acció de conformitat** Garanteix que el directori especificat sigui propietat de grup de l'usuari system, bin, sys o cron.
GEN003460	El fitxer `at.allow` ha de ser propietat de l'usuari root, bin o sys.	**Ubicació** `/etc/security/pscexpert/dodv2/chowndodfiles` **Acció de conformitat** Garanteix que el fitxer especificat sigui propietat de l'usuari root, bin o sys.
GEN003470	El fitxer `at.allow` ha de ser propietat de l'usuari system, bin, sys o cron.	**Ubicació** `/etc/security/pscexpert/dodv2/chowndodfiles` **Acció de conformitat** Garanteix que el fitxer especificat sigui propietat de grup de l'usuari system, bin, sys o cron.

Taula 3. Requeriments de propietat del departament de defensa (continuació)

ID de punt de comprovació de la guia per a la implementació tècnica de seguretat del departament de defensa	Descripció	Ubicació de l'script on es defineix l'acció i els resultats de l'acció que permeten la conformitat
GEN003480	El fitxer `at.deny` ha de ser propietat de l'usuari root, bin o sys.	**Ubicació** `/etc/security/pscexpert/dodv2/chowndodfiles` **Acció de conformitat** Garanteix que el fitxer especificat sigui propietat de l'usuari root, bin o sys.
GEN003490	El fitxer `at.deny` ha de ser propietat de l'usuari system, bin, sys o cron.	**Ubicació** `/etc/security/pscexpert/dodv2/chowndodfiles` **Acció de conformitat** Garanteix que el fitxer especificat sigui propietat de grup de l'usuari system, bin, sys o cron.
GEN003720	El fitxer `inetd.conf`, el fitxer `xinetd.conf` i el directori `xinetd.d` han de ser propietat de l'usuari root o bin.	**Ubicació** `/etc/security/pscexpert/dodv2/chowndodfiles` **Acció de conformitat** Garanteix que els fitxers i el directori especificats siguin propietat de l'usuari root o bin.
GEN003730	El fitxer `inetd.conf`, el fitxer `xinetd.conf` i el directori `xinetd.d` han de ser propietat de grup de l'usuari bin, sys o system.	**Ubicació** `/etc/security/pscexpert/dodv2/chowndodfiles` **Acció de conformitat** Garanteix que els fitxers i el directori especificats siguin propietat de grup de l'usuari bin, sys o system.
GEN003760	El fitxer `services` ha de ser propietat de l'usuari root o bin.	**Ubicació** `/etc/security/pscexpert/dodv2/chowndodfiles` **Acció de conformitat** Garanteix que el fitxer especificat sigui propietat de l'usuari root o bin.
GEN003770	El fitxer `services` ha de ser propietat de grup de l'usuari bin, sys o system.	**Ubicació** `/etc/security/pscexpert/dodv2/chowndodfiles` **Acció de conformitat** Garanteix que el fitxer especificat sigui propietat de grup de l'usuari bin, sys o system.
GEN003920	El fitxer `hosts.lpd` (o un d'equivalent) ha de ser propietat de l'usuari root, bin, sys o lp.	**Ubicació** `/etc/security/pscexpert/dodv2/chowndodfiles` **Acció de conformitat** Garanteix que el fitxer especificat sigui propietat de l'usuari root, bin, sys o lp.

Taula 3. Requeriments de propietat del departament de defensa (continuació)

ID de punt de comprovació de la guia per a la implementació tècnica de seguretat del departament de defensa	Descripció	Ubicació de l'script on es defineix l'acció i els resultats de l'acció que permeten la conformitat
GEN003930	El fitxer `hosts.lpd` (o un d'equivalent) ha de ser propietat de grup de l'usuari bin, sys o system.	**Ubicació** `/etc/security/pscexpert/dodv2/chowndodfiles` **Acció de conformitat** Garanteix que el fitxer especificat sigui propietat de grup de l'usuari bin, sys o system.
GEN003960	El propietari de l'ordre **traceroute** ha de ser l'usuari root.	**Ubicació** `/etc/security/pscexpert/dodv2/chowndodfiles` **Acció de conformitat** Garanteix que el propietari de l'ordre sigui l'usuari root.
GEN003980	L'ordre **traceroute** ha de ser propietat de grup de l'usuari sys, bin o system.	**Ubicació** `/etc/security/pscexpert/dodv2/chowndodfiles` **Acció de conformitat** Garanteix que l'ordre sigui propietat de grup de l'usuari sys, bin o system.
GEN004360	El fitxer `alias` ha de ser propietat de l'usuari root.	**Ubicació** `/etc/security/pscexpert/dodv2/chowndodfiles` **Acció de conformitat** Garanteix que el fitxer especificat sigui propietat de l'usuari root.
GEN004370	El fitxer `aliases` ha de ser propietat de grup de l'usuari sys, bin o system.	**Ubicació** `/etc/security/pscexpert/dodv2/chowndodfiles` **Acció de conformitat** Garanteix que el fitxer especificat sigui propietat de grup de l'usuari sys, bin o system.
GEN004400	Els fitxers que s'executen a través del fitxer `aliases` de correu han de ser propietat de l'usuari root i s'han de trobar al directori que és propietat de l'usuari root i només aquest usuari hi pugui escriure.	**Ubicació** `/etc/security/pscexpert/dodv2/chowndodfiles` **Acció de conformitat** Garanteix que els fitxers que s'executen a través d'un fitxer `aliases` de correu han de ser propietat de l'usuari root i s'han de trobar al directori que és propietat de l'usuari root i només aquest usuari hi pot escriure.

Taula 3. Requeriments de propietat del departament de defensa (continuació)

ID de punt de comprovació de la guia per a la implementació tècnica de seguretat del departament de defensa	Descripció	Ubicació de l'script on es defineix l'acció i els resultats de l'acció que permeten la conformitat
GEN004410	Els fitxers que s'executen a través d'un fitxer `aliases` de correu ha de ser propietat de grup de l'usuari root, bin, sys o other. També s'han de trobar al directori que és propietat de grup de l'usuari root, bin, sys o other.	**Ubicació** `/etc/security/pscexpert/dodv2/chowndodfiles` **Acció de conformitat** Garanteix que els fitxers que s'executen a través d'un fitxer `aliases` de correu ha de ser propietat de grup de l'usuari root, bin, sys o other i han d'estar en un directori que sigui propietat de grup de l'usuari root, bin, sys o other.
GEN004480	El fitxer de registres de serveis SMTP ha de ser propietat de l'usuari root.	**Ubicació** `/etc/security/pscexpert/dodv2/chowndodfiles` **Acció de conformitat** Garanteix que el fitxer especificat sigui propietat de l'usuari root.
GEN004920	El fitxer `ftpusers` ha de ser propietat de l'usuari root.	**Ubicació** `/etc/security/pscexpert/dodv2/chowndodfiles` **Acció de conformitat** Garanteix que el fitxer especificat sigui propietat de l'usuari root.
GEN004930	El fitxer `ftpusers` ha de ser propietat de grup de l'usuari bin, sys o system.	**Ubicació** `/etc/security/pscexpert/dodv2/chowndodfiles` **Acció de conformitat** Garanteix que el fitxer especificat sigui propietat de grup de l'usuari bin, sys o system.
GEN005360	El fitxer `snmpd.conf` ha de ser propietat de l'usuari root.	**Ubicació** `/etc/security/pscexpert/dodv2/chowndodfiles` **Acció de conformitat** Garanteix que el fitxer especificat sigui propietat de l'usuari root.
GEN005365	El fitxer `snmpd.conf` ha de ser propietat de grup de l'usuari bin, sys o system.	**Ubicació** `/etc/security/pscexpert/dodv2/chowndodfiles` **Acció de conformitat** Garanteix que el fitxer especificat sigui propietat de grup de l'usuari bin, sys o system.

Taula 3. Requeriments de propietat del departament de defensa (continuació)

ID de punt de comprovació de la guia per a la implementació tècnica de seguretat del departament de defensa	Descripció	Ubicació de l'script on es defineix l'acció i els resultats de l'acció que permeten la conformitat
GEN005400	El fitxer `/etc/syslog.conf` ha de ser propietat de l'usuari root.	**Ubicació** `/etc/security/pscexpert/dodv2/chowndodfiles` **Acció de conformitat** Garanteix que el fitxer especificat sigui propietat de l'usuari root.
GEN005420	El fitxer `/etc/syslog.conf` ha de ser propietat de grup de l'usuari bin, sys o system.	**Ubicació** `/etc/security/pscexpert/dodv2/chowndodfiles` **Acció de conformitat** Garanteix que el fitxer especificat sigui propietat de grup de l'usuari bin, sys o system.
GEN005610	El sistema no ha de tenir habilitada l'acció de remetre l'IP de l'IPv6, a menys que el sistema sigui un encaminador IPv6.	**Ubicació** `/etc/security/pscexpert/dodv2/chowndodfiles` **Acció de conformitat** Garanteix l'acció de remetre l'IP de l'IPv6 no estigui habilitada a menys que el sistema s'estigui utilitzant com a encaminador d'IPv6.
GEN005740	El fitxer de configuració d'exportació NFS ha de ser propietat de l'usuari root.	**Ubicació** `/etc/security/pscexpert/dodv2/chowndodfiles` **Acció de conformitat** Garanteix que el fitxer especificat sigui propietat de l'usuari root.
GEN005750	El fitxer de configuració d'exportació NFS ha de ser propietat de grup de l'usuari root, bin, sys o system.	**Ubicació** `/etc/security/pscexpert/dodv2/chowndodfiles` **Acció de conformitat** Garanteix que el fitxer especificat sigui propietat de grup de l'usuari root, bin, sys o system.
GEN005800	Tots els fitxers del sistema exportats d'NFS i els directoris del sistema han de ser propietat de l'usuari root.	**Ubicació** `/etc/security/pscexpert/dodv2/chowndodfiles` **Acció de conformitat** Garanteix que el fitxer especificat sigui propietat de l'usuari root.
GEN005810	Tots els fitxers de sistema exportats d'NFS i els directoris del sistema han de ser propietat de grup de l'usuari root, bin, sys o system.	**Ubicació** `/etc/security/pscexpert/dodv2/chowndodfiles` **Acció de conformitat** Garanteix que els fitxers i directoris especificats siguin propietat de grup de l'usuari root, bin, sys o system.

Taula 3. Requeriments de propietat del departament de defensa (continuació)

ID de punt de comprovació de la guia per a la implementació tècnica de seguretat del departament de defensa	Descripció	Ubicació de l'script on es defineix l'acció i els resultats de l'acció que permeten la conformitat
GEN006100	El fitxer `/usr/lib/smb.conf` ha de ser propietat de l'usuari root.	**Ubicació** `/etc/security/pscexpert/dodv2/chowndodfiles` **Acció de conformitat** Garanteix que el fitxer especificat sigui propietat de l'usuari root.
GEN006120	El fitxer `/usr/lib/smb.conf` ha de ser propietat de grup de l'usuari bin, sys o system.	**Ubicació** `/etc/security/pscexpert/dodv2/chowndodfiles` **Acció de conformitat** Garanteix que el fitxer especificat sigui propietat de grup de l'usuari bin, sys o system.
GEN006160	El fitxer `/var/private/smbpasswd` ha de ser propietat de l'usuari root.	**Ubicació** `/etc/security/pscexpert/dodv2/chowndodfiles` **Acció de conformitat** Garanteix que el fitxer especificat sigui propietat de l'usuari root.
GEN006180	El fitxer `/var/private/smbpasswd` ha de ser propietat de grup de l'usuari sys o system.	**Ubicació** `/etc/security/pscexpert/dodv2/chowndodfiles` **Acció de conformitat** Garanteix que el fitxer especificat sigui propietat de grup de l'usuari sys o system.
GEN006340	Els fitxers del directori `/etc/news` ha de ser propietat de l'usuari root o news.	**Ubicació** `/etc/security/pscexpert/dodv2/chowndodfiles` **Acció de conformitat** Garanteix que el directori especificat sigui propietat de l'usuari root o news.
GEN006360	Els fitxers del directori `/etc/news` han de ser propietat de grup de l'usuari system o news.	**Ubicació** `/etc/security/pscexpert/dodv2/chowndodfiles` **Acció de conformitat** Garanteix que els fitxers especificats siguin propietat de grup de l'usuari system o news.
GEN008080	Si el sistema utilitza LDAP per a la informació d'autenticació o de comptes, el fitxer `/etc/ldap.conf` (o un d'equivalent) ha de ser propietat de l'usuari root.	**Ubicació** `/etc/security/pscexpert/dodv2/chowndodfiles` **Acció de conformitat** Garanteix que el fitxer especificat sigui propietat de l'usuari root.

Taula 3. Requeriments de propietat del departament de defensa (continuació)

ID de punt de comprovació de la guia per a la implementació tècnica de seguretat del departament de defensa	Descripció	Ubicació de l'script on es defineix l'acció i els resultats de l'acció que permeten la conformitat
GEN008100	Si el sistema utilitza LDAP per a la informació d'autenticació o de comptes, el fitxer `/etc/ldap.conf` (o un d'equivalent) ha de ser propietat de grup de l'usuari security, bin, sys o system.	**Ubicació** `/etc/security/pscexpert/dodv2/chowndodfiles` **Acció de conformitat** Garanteix que el fitxer especificat sigui propietat de grup de l'usuari bin, sys o system.
GEN008140	Si el sistema utilitza LDAP per a la informació d'autenticació o de comptes, el fitxer o directori d'entitats certificadores de TLS ha de ser propietat de l'usuari root.	**Ubicació** `/etc/security/pscexpert/dodv2/chowndodfiles` **Acció de conformitat** Garanteix que el fitxer especificat sigui propietat de l'usuari root.
GEN008160	Si el sistema utilitza LDAP per a la informació d'autenticació o de comptes, el fitxer o directori d'entitats certificadores de TLS ha de ser propietat de grup de l'usuari root, bin, sys o system.	**Ubicació** `/etc/security/pscexpert/dodv2/chowndodfiles` **Acció de conformitat** Garanteix que el fitxer especificat sigui propietat de grup de l'usuari bin, sys o system.

Taula 4. Estàndards del departament de defensa per a permisos de fitxers

ID de punt de comprovació de la guia per a la implementació tècnica de seguretat del departament de defensa	Descripció	Ubicació de l'script on es defineix l'acció i els resultats de l'acció que permeten la conformitat
AIX00100	El fitxer `/etc/netsvc.conf` ha de tenir el mode 0644 o un mode que sigui menys permissiu.	**Ubicació** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Acció de conformitat** Garanteix que el fitxer s'estableixi en el mode de permís especificat o en un que sigui menys permissiu.
AIX00340	El fitxer `/etc/ftpaccess.ctl` ha de tenir el mode 0640 o un mode que sigui menys permissiu.	**Ubicació** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Acció de conformitat** Garanteix que el fitxer s'estableixi en el mode de permís especificat o en un que sigui menys permissiu.

Taula 4. Estàndards del departament de defensa per a permisos de fitxers (continuació)

ID de punt de comprovació de la guia per a la implementació tècnica de seguretat del departament de defensa	Descripció	Ubicació de l'script on es defineix l'acció i els resultats de l'acció que permeten la conformitat
GEN000252	El fitxer de configuració de sincronització horària (com per exemple `/etc/ntp.conf`) ha de tenir el mode 0640 o un mode que sigui menys permissiu.	**Ubicació** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Acció de conformitat** Garanteix que el fitxer s'estableixi en el mode de permís especificat o en un que sigui menys permissiu.
GEN000920	El directori inicial del compte root (diferent de /) ha de tenir el mode 0700.	**Ubicació** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Acció de conformitat** Garanteix que el directori s'estableixi en el mode de permís especificat o en un que sigui menys permissiu.
GEN001140	Els fitxers i directoris del sistema no han de tenir permisos d'accés desiguals.	**Ubicació** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Acció de conformitat** Garanteix que els permisos d'accés siguin coherents.
GEN001180	Tots els fitxers daemon de serveis de xarxa han de tenir el mode 0755 o un mode que sigui menys permissiu.	**Ubicació** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Acció de conformitat** Garanteix que els fitxers s'estableixin en el mode de permís especificat o en un que sigui menys permissiu.
GEN001200	Tots els fitxers d'ordres del sistema han de tenir el mode 0755 o un mode que sigui menys permissiu.	**Ubicació** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Acció de conformitat** Garanteix que els fitxers s'estableixin en el mode de permís especificat o en un que sigui menys permissiu.
GEN001260	Els fitxers de registre del sistema han de tenir el mode 0640 o un mode que sigui menys permissiu.	**Ubicació** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Acció de conformitat** Garanteix que els fitxers s'estableixin en el mode de permís especificat o en un que sigui menys permissiu.

Taula 4. Estàndards del departament de defensa per a permisos de fitxers (continuació)

ID de punt de comprovació de la guia per a la implementació tècnica de seguretat del departament de defensa	Descripció	Ubicació de l'script on es defineix l'acció i els resultats de l'acció que permeten la conformitat
GEN001280	Els fitxers de pàgines manuals han de tenir el mode 0644 o un mode que sigui menys permissiu.	**Ubicació** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Acció de conformitat** Garanteix que els fitxers s'estableixin en el mode de permís especificat o en un que sigui menys permissiu.
GEN001300	Els fitxers de biblioteques han de tenir el mode 0755 o un mode que sigui menys permissiu.	**Ubicació** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Acció de conformitat** Garanteix que els fitxers s'estableixin en el mode de permís especificat o en un que sigui menys permissiu.
GEN001360	Els fitxers NIS/NIS+/yp han de tenir el mode 0755 o un mode que sigui menys permissiu.	**Ubicació** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Acció de conformitat** Garanteix que els fitxers s'estableixin en el mode de permís especificat o en un que sigui menys permissiu.
GEN001364	El fitxer `/etc/resolv.conf` ha de tenir el mode 0644 o un mode que sigui menys permissiu.	**Ubicació** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Acció de conformitat** Garanteix que el fitxer s'estableixi en el mode de permís especificat o en un que sigui menys permissiu.
GEN001368	El fitxer `/etc/hosts` ha de tenir el mode 0644 o un mode que sigui menys permissiu.	**Ubicació** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Acció de conformitat** Garanteix que el fitxer s'estableixi en el mode de permís especificat o en un que sigui menys permissiu.
GEN001373	El fitxer `/etc/nsswitch.conf` ha de tenir el mode 0644 o un mode que sigui menys permissiu.	**Ubicació** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Acció de conformitat** Garanteix que el fitxer s'estableixi en el mode de permís especificat o en un que sigui menys permissiu.

Taula 4. Estàndards del departament de defensa per a permisos de fitxers (continuació)

ID de punt de comprovació de la guia per a la implementació tècnica de seguretat del departament de defensa	Descripció	Ubicació de l'script on es defineix l'acció i els resultats de l'acció que permeten la conformitat
GEN001380	El fitxer `/etc/passwd` ha de tenir el mode 0644 o un mode que sigui menys permissiu.	**Ubicació** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Acció de conformitat** Garanteix que el fitxer s'estableixi en el mode de permís especificat o en un que sigui menys permissiu.
GEN001393	El fitxer `/etc/group` ha de tenir el mode 0644 o un mode que sigui menys permissiu.	**Ubicació** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Acció de conformitat** Garanteix que el fitxer s'estableixi en el mode de permís especificat o en un que sigui menys permissiu.
GEN001420	El fitxer `/etc/security/passwd` ha de tenir el mode 0400.	**Ubicació** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Acció de conformitat** Garanteix que el fitxer s'estableixi en el mode de permís especificat o en un que sigui menys permissiu.
GEN001480	Tots els directoris inicials de l'usuari han de tenir un mode de 0750 o menys permissiu.	**Ubicació** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Acció de conformitat** Garanteix que el fitxer s'estableixi en el mode de permís especificat o en un que sigui menys permissiu.
GEN001560	Tots els fitxers i directoris que es troben en un directori inicial d'usuari han de tenir el mode 0750 o un mode que sigui menys permissiu.	**Ubicació** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Acció de conformitat** Garanteix que els fitxers s'estableixin en el mode de permís especificat o en un que sigui menys permissiu.
GEN001580	Tots els scripts de control d'execució han de tenir el mode 0755 o un mode que sigui menys permissiu.	**Ubicació** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Acció de conformitat** Garanteix que els fitxers s'estableixin en el mode de permís especificat o en un que sigui menys permissiu.

Taula 4. Estàndards del departament de defensa per a permisos de fitxers (continuació)

ID de punt de comprovació de la guia per a la implementació tècnica de seguretat del departament de defensa	Descripció	Ubicació de l'script on es defineix l'acció i els resultats de l'acció que permeten la conformitat
GEN001640	Els scripts de control d'execució no han d'executar programes o scripts amb permís d'escriptura global.	**Ubicació** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Acció de conformitat** Comprova si els programes com, per exemple, `cron`, son programes o scripts amb permís d'escriptura global.
GEN001720	Tots els fitxers d'inicialització global han de tenir el mode 0644 o un mode que sigui menys permissiu.	**Ubicació** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Acció de conformitat** Garanteix que els fitxers s'estableixin en el mode de permís especificat o en un que sigui menys permissiu.
GEN001800	Tots els fitxers d'esquelet (per exemple, els fitxers de `/etc/skel`) han de tenir el mode 0644 o un mode que sigui menys permissiu.	**Ubicació** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Acció de conformitat** Garanteix que els fitxers s'estableixin en el mode de permís especificat o en un que sigui menys permissiu.
GEN001880	Tots els fitxers d'inicialització locals han de tenir el mode 0740 o un mode que sigui menys permissiu.	**Ubicació** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Acció de conformitat** Garanteix que els fitxers s'estableixin en el mode de permís especificat o en un que sigui menys permissiu.
GEN002220	Tots els fitxers de l'intèrpret d'ordres han de tenir el mode 0755 o un mode que sigui menys permissiu.	**Ubicació** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Acció de conformitat** Garanteix que els fitxers s'estableixin en el mode de permís especificat o en un que sigui menys permissiu.
GEN002320	Els dispositius d'àudio han de tenir el mode 0660 o un mode que sigui menys permissiu.	**Ubicació** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Acció de conformitat** Garanteix que els dispositius d'àudio s'hagin establert en el mode de permís especificat o en un que sigui menys permissiu.

Taula 4. Estàndards del departament de defensa per a permisos de fitxers (continuació)

ID de punt de comprovació de la guia per a la implementació tècnica de seguretat del departament de defensa	Descripció	Ubicació de l'script on es defineix l'acció i els resultats de l'acció que permeten la conformitat
GEN002560	El sistema i l'usuari per defecte **umask** ha de ser 077.	**Ubicació** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Acció de conformitat** Garanteix que els paràmetres especificats siguin *077*.
GEN002700	Els registres d'auditoria del sistema han de tenir el mode 0640 o un mode que sigui menys permissiu.	**Ubicació** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Acció de conformitat** Garanteix que els fitxers s'estableixin en el mode de permís especificat o en un que sigui menys permissiu.
GEN002717	Els fitxers executables de l'eina d'auditoria del sistema han de tenir el mode 0750 o un mode que sigui menys permissiu.	**Ubicació** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Acció de conformitat** Garanteix que els fitxers s'estableixin en el mode de permís especificat o en un que sigui menys permissiu.
GEN002980	El fitxer `cron.allow` ha de tenir el mode 0600 o	**Ubicació** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Acció de conformitat** Garanteix que el fitxer s'estableixi en el mode de permís especificat o en un que sigui menys permissiu.
GEN003080	Els fitxers crontab han de tenir el mode 0600 o un mode que sigui menys permissiu.	**Ubicació** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Acció de conformitat** Garanteix que els fitxers s'estableixin en el mode de permís especificat o en un que sigui menys permissiu.
GEN003090	Els fitxers `crontab` no han de tenir llistes de control d'accés ampliades (ACL).	**Ubicació** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Acció de conformitat** Garanteix que els fitxers especificats no tinguin cap ACL ampliada.

Taula 4. Estàndards del departament de defensa per a permisos de fitxers (continuació)

ID de punt de comprovació de la guia per a la implementació tècnica de seguretat del departament de defensa	Descripció	Ubicació de l'script on es defineix l'acció i els resultats de l'acció que permeten la conformitat
GEN003100	Els directoris cron i crontab han de tenir el mode 0755 o un mode que sigui menys permissiu.	**Ubicació** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Acció de conformitat** Garanteix que els directoris especificats s'estableixin en el mode de permís especificat o en un que sigui menys permissiu.
GEN003180	El fitxer `cronlog` ha de tenir el mode 0600 o un que sigui menys permissiu.	**Ubicació** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Acció de conformitat** Garanteix que el fitxer s'estableixi en el mode de permís especificat o en un que sigui menys permissiu.
GEN003200	El fitxer `cron.deny` ha de tenir el mode 0600 o un que sigui menys permissiu.	**Ubicació** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Acció de conformitat** Garanteix que el fitxer s'estableixi en el mode de permís especificat o en un que sigui menys permissiu.
GEN003252	El fitxer `at.deny` ha de tenir el mode 0640 o un que sigui menys permissiu.	**Ubicació** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Acció de conformitat** Garanteix que el fitxer s'estableixi en el mode de permís especificat o en un que sigui menys permissiu.
GEN003340	El fitxer `at.allow` ha de tenir el mode 0600 o un que sigui menys permissiu.	**Ubicació** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Acció de conformitat** Garanteix que el fitxer s'estableixi en el mode de permís especificat o en un que sigui menys permissiu.
GEN003400	El directori `at` ha de tenir el mode 0755 o un mode que sigui menys permissiu.	**Ubicació** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Acció de conformitat** Garanteix que el directori s'estableixi en el mode de permís especificat o en un que sigui menys permissiu.

Taula 4. Estàndards del departament de defensa per a permisos de fitxers (continuació)

ID de punt de comprovació de la guia per a la implementació tècnica de seguretat del departament de defensa	Descripció	Ubicació de l'script on es defineix l'acció i els resultats de l'acció que permeten la conformitat
GEN003440	Els treballs `At` no han de tenir establert el paràmetre **`umask`** en un valor menys restrictiu de 077.	**Ubicació** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Acció de conformitat** Garanteix que el paràmetre s'estableixi en el mode de permís especificat o en un que sigui menys permissiu.
GEN003740	Els fitxers `inetd.conf` i `xinetd.conf` han de tenir el mode 0440 o un mode que sigui menys permissiu.	**Ubicació** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Acció de conformitat** Garanteix que els fitxers s'estableixin en el mode de permís especificat o en un que sigui menys permissiu.
GEN003780	El fitxer `services` ha de tenir el mode 0444 o un que sigui menys permissiu.	**Ubicació** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Acció de conformitat** Garanteix que el fitxer s'estableixi en el mode de permís especificat o en un que sigui menys permissiu.
GEN003940	El fitxer `hosts.lpd` (o un d'equivalent) ha de tenir el mode 0644 o un mode que sigui menys permissiu.	**Ubicació** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Acció de conformitat** Garanteix que el fitxer s'estableixi en el mode de permís especificat o en un que sigui menys permissiu.
GEN004000	El fitxer `traceroute` ha de tenir el mode 0700 o un mode que sigui menys permissiu.	**Ubicació** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Acció de conformitat** Garanteix que el fitxer s'estableixi en el mode de permís especificat o en un que sigui menys permissiu.
GEN004380	El fitxer `alias` ha de tenir el mode 0644 o un mode que sigui menys permissiu.	**Ubicació** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Acció de conformitat** Garanteix que el fitxer s'estableixi en el mode de permís especificat o en un que sigui menys permissiu.

Taula 4. Estàndards del departament de defensa per a permisos de fitxers (continuació)

ID de punt de comprovació de la guia per a la implementació tècnica de seguretat del departament de defensa	Descripció	Ubicació de l'script on es defineix l'acció i els resultats de l'acció que permeten la conformitat
GEN004420	Els fitxers que s'executen a través d'un fitxer `aliases` de correu han de tenir el mode 0755 o un mode que sigui menys permissiu.	**Ubicació** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Acció de conformitat** Garanteix que els fitxers s'estableixin en el mode de permís especificat o en un que sigui menys permissiu.
GEN004500	El fitxer de registre de servei SMTP ha de tenir el mode 0644 o un mode que sigui menys permissiu.	**Ubicació** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Acció de conformitat** Garanteix que el fitxer s'estableixi en el mode de permís especificat o en un que sigui menys permissiu.
GEN004940	El fitxer `ftpusers` ha de tenir el mode 0640 o un mode que sigui menys permissiu.	**Ubicació** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Acció de conformitat** Garanteix que el fitxer s'estableixi en el mode de permís especificat o en un que sigui menys permissiu.
GEN005040	Tots els usuaris FTP han de tenir un paràmetre **`umask`** per defecte de 077.	**Ubicació** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Acció de conformitat** Garanteix que el paràmetre sigui correcte.
GEN005100	El daemon `TFTP` ha de tenir el mode 0755 o un mode que sigui menys permissiu.	**Ubicació** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Acció de conformitat** Garanteix que el daemon s'estableixi en el mode especificat o en un que sigui menys permissiu.
GEN005180	Tots els fitxers `.Xauthority` han de tenir el mode 0600 o un mode que sigui menys permissiu.	**Ubicació** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Acció de conformitat** Garanteix que els fitxers s'estableixin en el mode de permís especificat o en un que sigui menys permissiu.

Taula 4. Estàndards del departament de defensa per a permisos de fitxers (continuació)

ID de punt de comprovació de la guia per a la implementació tècnica de seguretat del departament de defensa	Descripció	Ubicació de l'script on es defineix l'acció i els resultats de l'acció que permeten la conformitat
GEN005320	El fitxer `snmpd.conf` ha de tenir el mode 0600 o un mode que sigui menys permissiu.	**Ubicació** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Acció de conformitat** Garanteix que el fitxer s'estableixi en el mode de permís especificat o en un que sigui menys permissiu.
GEN005340	Els fitxers MIB (Management Information Base) han de tenir el mode 0640 o un mode que sigui menys permissiu.	**Ubicació** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Acció de conformitat** Garanteix que els fitxers s'estableixin en el mode de permís especificat o en un que sigui menys permissiu.
GEN005390	El fitxer `/etc/syslog.conf` ha de tenir el mode 0640 o un mode que sigui menys permissiu.	**Ubicació** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Acció de conformitat** Garanteix que el fitxer s'estableixi en el mode de permís especificat o en un que sigui menys permissiu.
GEN005522	Els fitxers clau de l'amfitrió públic SSH han de tenir un mode 0644 o un mode que sigui menys permissiu.	**Ubicació** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Acció de conformitat** Garanteix que els fitxers s'estableixin en el mode de permís especificat o en un que sigui menys permissiu.
GEN005523	Els fitxers clau de l'amfitrió privat SSH han de tenir un mode 0600 o un mode que sigui menys permissiu.	**Ubicació** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Acció de conformitat** Garanteix que els fitxers s'estableixin en el mode de permís especificat o en un que sigui menys permissiu.
GEN006140	El fitxer `/usr/lib/smb.conf` ha de tenir el mode 0644 o un mode que sigui menys permissiu.	**Ubicació** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Acció de conformitat** Garanteix que el fitxer s'estableixi en el mode de permís especificat o en un que sigui menys permissiu.

Taula 4. Estàndards del departament de defensa per a permisos de fitxers (continuació)

ID de punt de comprovació de la guia per a la implementació tècnica de seguretat del departament de defensa	Descripció	Ubicació de l'script on es defineix l'acció i els resultats de l'acció que permeten la conformitat
GEN006200	El fitxer `/var/private/smbpasswd` ha de tenir el mode 0600 o un mode que sigui menys permissiu.	**Ubicació** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Acció de conformitat** Garanteix que el fitxer s'estableixi en el mode de permís especificat o en un que sigui menys permissiu.
GEN006260	El fitxer `/etc/news/hosts.nntp` (o un d'equivalent) ha de tenir el mode 0600 o un mode que sigui menys permissiu.	**Ubicació** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Acció de conformitat** Garanteix que el fitxer s'estableixi en el mode de permís especificat o en un que sigui menys permissiu.
GEN006280	El fitxer `/etc/news/hosts.nntp.nolimit` (o un d'equivalent) ha de tenir el mode 0600 o un mode que sigui menys permissiu.	**Ubicació** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Acció de conformitat** Garanteix que el fitxer s'estableixi en el mode de permís especificat o en un que sigui menys permissiu.
GEN006300	El fitxer `/etc/news/nnrp.access` (o un d'equivalent) ha de tenir el mode 0600 o un mode que sigui menys permissiu.	**Ubicació** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Acció de conformitat** Garanteix que el fitxer s'estableixi en el mode de permís especificat o en un que sigui menys permissiu.
GEN006320	El fitxer `/etc/news/passwd.nntp` (o un d'equivalent) ha de tenir el mode 0600 o un mode que sigui menys permissiu.	**Ubicació** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Acció de conformitat** Garanteix que el fitxer s'estableixi en el mode de permís especificat o en un que sigui menys permissiu.
GEN008060	Si el sistema utilitza LDAP per a la informació d'autenticació o de comptes, el fitxer `/etc/ldap.conf` (o un d'equivalent) ha de tenir el mode 0644 o un de menys permissiu.	**Ubicació** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Acció de conformitat** Garanteix que el fitxer s'estableixi en el mode de permís especificat o en un que sigui menys permissiu.

Taula 4. Estàndards del departament de defensa per a permisos de fitxers (continuació)

ID de punt de comprovació de la guia per a la implementació tècnica de seguretat del departament de defensa	Descripció	Ubicació de l'script on es defineix l'acció i els resultats de l'acció que permeten la conformitat
GEN008180	Si el sistema utilitza LDAP per a la informació d'autenticació o de comptes, el fitxer de l'entitat certificadora TLS, o el directori, o ambdós, han de tenir el mode 0644 (0755 per a directoris) o un de menys permissiu.	**Ubicació** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Acció de conformitat** Garanteix que el fitxer especificat, els directoris especificats, o ambdós, s'estableixin al mode de permissió especificat o en un que sigui menys permissiu.

Taula 5. Requeriments de la llista de control d'accés (ACL) del departament de defensa

ID de punt de comprovació de la guia per a la implementació tècnica de seguretat del departament de defensa	Descripció	Ubicació de l'script on es defineix l'acció i els resultats de l'acció que permeten la conformitat
AIX00110	El fitxer `/etc/netsvc.conf` no ha de tenir cap llista de control d'accés (ACL) ampliada.	**Ubicació** `/etc/security/pscexpert/dodv2/acldodfiles` **Acció de conformitat** Inhabilita l'ACL ampliada que s'ha especificat. **Nota:** Aquest paràmetre no es canvia automàticament quan es restableix la política per defecte de l'AIX mitjançant el fitxer `DoDv2_to_ AIXDefault.xml`. Heu de canviar manualment aquest paràmetre.
AIX00350	El fitxer `/etc/ftpaccess.ctl` no ha de tenir cap ACL ampliada.	**Ubicació** `/etc/security/pscexpert/dodv2/acldodfiles` **Acció de conformitat** Inhabilita l'ACL ampliada que s'ha especificat. **Nota:** Aquest paràmetre no es canvia automàticament quan es restableix la política per defecte de l'AIX mitjançant el fitxer `DoDv2_to_ AIXDefault.xml`. Heu de canviar manualment aquest paràmetre.
GEN000253	El fitxer de configuració de sincronització horària (com, per exemple, `/etc/ntp.conf`) no ha de tenir cap ACL ampliada.	**Ubicació** `/etc/security/pscexpert/dodv2/acldodfiles` **Acció de conformitat** Inhabilita l'ACL ampliada que s'ha especificat. **Nota:** Aquest paràmetre no es canvia automàticament quan es restableix la política per defecte de l'AIX mitjançant el fitxer `DoDv2_to_ AIXDefault.xml`. Heu de canviar manualment aquest paràmetre.

Taula 5. Requeriments de la llista de control d'accés (ACL) del departament de defensa (continuació)

ID de punt de comprovació de la guia per a la implementació tècnica de seguretat del departament de defensa	Descripció	Ubicació de l'script on es defineix l'acció i els resultats de l'acció que permeten la conformitat
GEN000930	El directori inicial del compte arrel no ha de tenir cap ACL ampliada.	**Ubicació** `/etc/security/pscexpert/dodv2/acldodfiles` **Acció de conformitat** Inhabilita l'ACL ampliada que s'ha especificat. **Nota:** Aquest paràmetre no es canvia automàticament quan es restableix la política per defecte de l'AIX mitjançant el fitxer `DoDv2_to_ AIXDefault.xml`. Heu de canviar manualment aquest paràmetre.
GEN001190	Cap dels fitxers daemon de serveis de xarxa ha de tenir ACL ampliades.	**Ubicació** `/etc/security/pscexpert/dodv2/acldodfiles` **Acció de conformitat** Inhabilita l'ACL ampliada que s'ha especificat. **Nota:** Aquest paràmetre no es canvia automàticament quan es restableix la política per defecte de l'AIX mitjançant el fitxer `DoDv2_to_ AIXDefault.xml`. Heu de canviar manualment aquest paràmetre.
GEN001210	Cap dels fitxers d'ordres del sistema ha de tenir ACL ampliades.	**Ubicació** `/etc/security/pscexpert/dodv2/acldodfiles` **Acció de conformitat** Inhabilita l'ACL ampliada que s'ha especificat. **Nota:** Aquest paràmetre no es canvia automàticament quan es restableix la política per defecte de l'AIX mitjançant el fitxer `DoDv2_to_ AIXDefault.xml`. Heu de canviar manualment aquest paràmetre.
GEN001270	Els fitxers de registre del sistema no han de tenir ACL ampliades, excepte si són necessàries per donar suport al programari autoritzat.	**Ubicació** `/etc/security/pscexpert/dodv2/acldodfiles` **Acció de conformitat** Inhabilita l'ACL ampliada que s'ha especificat. **Nota:** Aquest paràmetre no es canvia automàticament quan es restableix la política per defecte de l'AIX mitjançant el fitxer `DoDv2_to_ AIXDefault.xml`. Heu de canviar manualment aquest paràmetre.

Taula 5. Requeriments de la llista de control d'accés (ACL) del departament de defensa (continuació)

ID de punt de comprovació de la guia per a la implementació tècnica de seguretat del departament de defensa	Descripció	Ubicació de l'script on es defineix l'acció i els resultats de l'acció que permeten la conformitat
GEN001310	Cap dels fitxers de biblioteca ha de tenir ACL ampliades.	**Ubicació** `/etc/security/pscexpert/dodv2/acldodfiles` **Acció de conformitat** Inhabilita l'ACL ampliada que s'ha especificat. **Nota:** Aquest paràmetre no es canvia automàticament quan es restableix la política per defecte de l'AIX mitjançant el fitxer `DoDv2_to_ AIXDefault.xml`. Heu de canviar manualment aquest paràmetre.
GEN001361	Els fitxer d'ordres NIS/NIS+/yp no han de tenir ACL ampliades.	**Ubicació** `/etc/security/pscexpert/dodv2/acldodfiles` **Acció de conformitat** Inhabilita l'ACL ampliada que s'ha especificat. **Nota:** Aquest paràmetre no es canvia automàticament quan es restableix la política per defecte de l'AIX mitjançant el fitxer `DoDv2_to_ AIXDefault.xml`. Heu de canviar manualment aquest paràmetre.
GEN001365	El fitxer `/etc/resolv.conf` no ha de tenir cap ACL ampliada.	**Ubicació** `/etc/security/pscexpert/dodv2/acldodfiles` **Acció de conformitat** Inhabilita l'ACL ampliada que s'ha especificat. **Nota:** Aquest paràmetre no es canvia automàticament quan es restableix la política per defecte de l'AIX mitjançant el fitxer `DoDv2_to_ AIXDefault.xml`. Heu de canviar manualment aquest paràmetre.
GEN001369	El fitxer `/etc/hosts` no ha de tenir cap ACL ampliada.	**Ubicació** `/etc/security/pscexpert/dodv2/acldodfiles` **Acció de conformitat** Inhabilita l'ACL ampliada que s'ha especificat. **Nota:** Aquest paràmetre no es canvia automàticament quan es restableix la política per defecte de l'AIX mitjançant el fitxer `DoDv2_to_ AIXDefault.xml`. Heu de canviar manualment aquest paràmetre.

Taula 5. Requeriments de la llista de control d'accés (ACL) del departament de defensa (continuació)

ID de punt de comprovació de la guia per a la implementació tècnica de seguretat del departament de defensa	Descripció	Ubicació de l'script on es defineix l'acció i els resultats de l'acció que permeten la conformitat
GEN001374	El fitxer `/etc/nsswitch.conf` no ha de tenir cap ACL ampliada.	**Ubicació** `/etc/security/pscexpert/dodv2/acldodfiles` **Acció de conformitat** Inhabilita l'ACL ampliada que s'ha especificat. **Nota:** Aquest paràmetre no es canvia automàticament quan es restableix la política per defecte de l'AIX mitjançant el fitxer `DoDv2_to_ AIXDefault.xml`. Heu de canviar manualment aquest paràmetre.
GEN001390	El fitxer `/etc/passwd` no ha de tenir cap ACL ampliada.	**Ubicació** `/etc/security/pscexpert/dodv2/acldodfiles` **Acció de conformitat** Inhabilita l'ACL ampliada que s'ha especificat. **Nota:** Aquest paràmetre no es canvia automàticament quan es restableix la política per defecte de l'AIX mitjançant el fitxer `DoDv2_to_ AIXDefault.xml`. Heu de canviar manualment aquest paràmetre.
GEN001394	El fitxer `/etc/group` no ha de tenir cap ACL ampliada.	**Ubicació** `/etc/security/pscexpert/dodv2/acldodfiles` **Acció de conformitat** Inhabilita l'ACL ampliada que s'ha especificat. **Nota:** Aquest paràmetre no es canvia automàticament quan es restableix la política per defecte de l'AIX mitjançant el fitxer `DoDv2_to_ AIXDefault.xml`. Heu de canviar manualment aquest paràmetre.
GEN001430	El fitxer `/etc/security/passwd` no ha de tenir cap ACL ampliada.	**Ubicació** `/etc/security/pscexpert/dodv2/acldodfiles` **Acció de conformitat** Inhabilita l'ACL ampliada que s'ha especificat. **Nota:** Aquest paràmetre no es canvia automàticament quan es restableix la política per defecte de l'AIX mitjançant el fitxer `DoDv2_to_ AIXDefault.xml`. Heu de canviar manualment aquest paràmetre.

Taula 5. Requeriments de la llista de control d'accés (ACL) del departament de defensa (continuació)

ID de punt de comprovació de la guia per a la implementació tècnica de seguretat del departament de defensa	Descripció	Ubicació de l'script on es defineix l'acció i els resultats de l'acció que permeten la conformitat
GEN001570	Cap dels fitxers ni directoris que es troben al directoris inicials d'usuaris han de contenir ACL ampliades.	**Ubicació** `/etc/security/pscexpert/dodv2/acldodfiles` **Acció de conformitat** Inhabilita l'ACL ampliada que s'ha especificat. **Nota:** Aquest paràmetre no es canvia automàticament quan es restableix la política per defecte de l'AIX mitjançant el fitxer `DoDv2_to_ AIXDefault.xml`. Heu de canviar manualment aquest paràmetre.
GEN001590	Cap dels scripts de control d'execució ha de tenir ACL ampliades.	**Ubicació** `/etc/security/pscexpert/dodv2/acldodfiles` **Acció de conformitat** Inhabilita l'ACL ampliada que s'ha especificat. **Nota:** Aquest paràmetre no es canvia automàticament quan es restableix la política per defecte de l'AIX mitjançant el fitxer `DoDv2_to_ AIXDefault.xml`. Heu de canviar manualment aquest paràmetre.
GEN001730	Cap dels fitxers d'inicialització global ha de tenir ACL ampliades.	**Ubicació** `/etc/security/pscexpert/dodv2/acldodfiles` **Acció de conformitat** Inhabilita l'ACL ampliada que s'ha especificat. **Nota:** Aquest paràmetre no es canvia automàticament quan es restableix la política per defecte de l'AIX mitjançant el fitxer `DoDv2_to_ AIXDefault.xml`. Heu de canviar manualment aquest paràmetre.
GEN001810	Els fitxers d'esquelet no han de tenir ACL ampliades.	**Ubicació** `/etc/security/pscexpert/dodv2/acldodfiles` **Acció de conformitat** Inhabilita l'ACL ampliada que s'ha especificat. **Nota:** Aquest paràmetre no es canvia automàticament quan es restableix la política per defecte de l'AIX mitjançant el fitxer `DoDv2_to_ AIXDefault.xml`. Heu de canviar manualment aquest paràmetre.

Taula 5. Requeriments de la llista de control d'accés (ACL) del departament de defensa (continuació)

ID de punt de comprovació de la guia per a la implementació tècnica de seguretat del departament de defensa	Descripció	Ubicació de l'script on es defineix l'acció i els resultats de l'acció que permeten la conformitat
GEN001890	Els fitxers d'inicialització local no han de tenir ACL ampliades.	**Ubicació** `/etc/security/pscexpert/dodv2/acldodfiles` **Acció de conformitat** Inhabilita l'ACL ampliada que s'ha especificat. **Nota:** Aquest paràmetre no es canvia automàticament quan es restableix la política per defecte de l'AIX mitjançant el fitxer `DoDv2_to_ AIXDefault.xml`. Heu de canviar manualment aquest paràmetre.
GEN002230	Cap dels fitxers de l'intèrpret d'ordres ha de tenir ACL ampliades.	**Ubicació** `/etc/security/pscexpert/dodv2/acldodfiles` **Acció de conformitat** Inhabilita l'ACL ampliada que s'ha especificat. **Nota:** Aquest paràmetre no es canvia automàticament quan es restableix la política per defecte de l'AIX mitjançant el fitxer `DoDv2_to_ AIXDefault.xml`. Heu de canviar manualment aquest paràmetre.
GEN002330	Els dispositius d'àudio no han de tenir ACL ampliades.	**Ubicació** `/etc/security/pscexpert/dodv2/acldodfiles` **Acció de conformitat** Inhabilita l'ACL ampliada que s'ha especificat. **Nota:** Aquest paràmetre no es canvia automàticament quan es restableix la política per defecte de l'AIX mitjançant el fitxer `DoDv2_to_ AIXDefault.xml`. Heu de canviar manualment aquest paràmetre.
GEN002710	Cap dels fitxers d'auditoria del sistema ha de tenir ACL ampliades.	**Ubicació** `/etc/security/pscexpert/dodv2/acldodfiles` **Acció de conformitat** Inhabilita l'ACL ampliada que s'ha especificat. **Nota:** Aquest paràmetre no es canvia automàticament quan es restableix la política per defecte de l'AIX mitjançant el fitxer `DoDv2_to_ AIXDefault.xml`. Heu de canviar manualment aquest paràmetre.

Taula 5. Requeriments de la llista de control d'accés (ACL) del departament de defensa (continuació)

ID de punt de comprovació de la guia per a la implementació tècnica de seguretat del departament de defensa	Descripció	Ubicació de l'script on es defineix l'acció i els resultats de l'acció que permeten la conformitat
GEN002990	Les ACL ampliades s'han d'inhabilitar pels fitxers `cron.allow` i `cron.deny`.	**Ubicació** `/etc/security/pscexpert/dodv2/acldodfiles` **Acció de conformitat** Inhabilita l'ACL ampliada que s'ha especificat. **Nota:** Aquest paràmetre no es canvia automàticament quan es restableix la política per defecte de l'AIX mitjançant el fitxer `DoDv2_to_ AIXDefault.xml`. Heu de canviar manualment aquest paràmetre.
GEN003090	Els fitxers crontab no han de tenir ACL ampliades.	**Ubicació** `/etc/security/pscexpert/dodv2/acldodfiles` **Acció de conformitat** Inhabilita l'ACL ampliada que s'ha especificat. **Nota:** Aquest paràmetre no es canvia automàticament quan es restableix la política per defecte de l'AIX mitjançant el fitxer `DoDv2_to_ AIXDefault.xml`. Heu de canviar manualment aquest paràmetre.
GEN003110	Els directoris cron i crontab no han de tenir ACL ampliades.	**Ubicació** `/etc/security/pscexpert/dodv2/acldodfiles` **Acció de conformitat** Inhabilita l'ACL ampliada que s'ha especificat. **Nota:** Aquest paràmetre no es canvia automàticament quan es restableix la política per defecte de l'AIX mitjançant el fitxer `DoDv2_to_ AIXDefault.xml`. Heu de canviar manualment aquest paràmetre.
GEN003190	Els fitxers de registre cron no han de tenir ACL ampliades.	**Ubicació** `/etc/security/pscexpert/dodv2/acldodfiles` **Acció de conformitat** Inhabilita l'ACL ampliada que s'ha especificat. **Nota:** Aquest paràmetre no es canvia automàticament quan es restableix la política per defecte de l'AIX mitjançant el fitxer `DoDv2_to_ AIXDefault.xml`. Heu de canviar manualment aquest paràmetre.

Taula 5. Requeriments de la llista de control d'accés (ACL) del departament de defensa (continuació)

ID de punt de comprovació de la guia per a la implementació tècnica de seguretat del departament de defensa	Descripció	Ubicació de l'script on es defineix l'acció i els resultats de l'acció que permeten la conformitat
GEN003210	El fitxer `cron.deny` no ha de tenir cap ACL ampliada.	**Ubicació** `/etc/security/pscexpert/dodv2/acldodfiles` **Acció de conformitat** Inhabilita l'ACL ampliada que s'ha especificat. **Nota:** Aquest paràmetre no es canvia automàticament quan es restableix la política per defecte de l'AIX mitjançant el fitxer `DoDv2_to_ AIXDefault.xml`. Heu de canviar manualment aquest paràmetre.
GEN003245	El fitxer `at.allow` no ha de tenir cap ACL ampliada.	**Ubicació** `/etc/security/pscexpert/dodv2/acldodfiles` **Acció de conformitat** Inhabilita l'ACL ampliada que s'ha especificat. **Nota:** Aquest paràmetre no es canvia automàticament quan es restableix la política per defecte de l'AIX mitjançant el fitxer `DoDv2_to_ AIXDefault.xml`. Heu de canviar manualment aquest paràmetre.
GEN003255	El fitxer `at.deny` no ha de tenir cap ACL ampliada.	**Ubicació** `/etc/security/pscexpert/dodv2/acldodfiles` **Acció de conformitat** Inhabilita l'ACL ampliada que s'ha especificat. **Nota:** Aquest paràmetre no es canvia automàticament quan es restableix la política per defecte de l'AIX mitjançant el fitxer `DoDv2_to_ AIXDefault.xml`. Heu de canviar manualment aquest paràmetre.
GEN003410	El directori `at` no ha de tenir cap ACL ampliada.	**Ubicació** `/etc/security/pscexpert/dodv2/acldodfiles` **Acció de conformitat** Inhabilita l'ACL ampliada que s'ha especificat. **Nota:** Aquest paràmetre no es canvia automàticament quan es restableix la política per defecte de l'AIX mitjançant el fitxer `DoDv2_to_ AIXDefault.xml`. Heu de canviar manualment aquest paràmetre.

Taula 5. Requeriments de la llista de control d'accés (ACL) del departament de defensa (continuació)

ID de punt de comprovació de la guia per a la implementació tècnica de seguretat del departament de defensa	Descripció	Ubicació de l'script on es defineix l'acció i els resultats de l'acció que permeten la conformitat
GEN003745	Els fitxers `inetd.conf` i `xinetd.conf` no han de tenir ACL ampliades.	**Ubicació** `/etc/security/pscexpert/dodv2/acldodfiles` **Acció de conformitat** Inhabilita l'ACL ampliada que s'ha especificat. **Nota:** Aquest paràmetre no es canvia automàticament quan es restableix la política per defecte de l'AIX mitjançant el fitxer `DoDv2_to_ AIXDefault.xml`. Heu de canviar manualment aquest paràmetre.
GEN003790	El fitxer de servei no ha de tenir cap ACL ampliada.	**Ubicació** `/etc/security/pscexpert/dodv2/acldodfiles` **Acció de conformitat** Inhabilita l'ACL ampliada que s'ha especificat. **Nota:** Aquest paràmetre no es canvia automàticament quan es restableix la política per defecte de l'AIX mitjançant el fitxer `DoDv2_to_ AIXDefault.xml`. Heu de canviar manualment aquest paràmetre.
GEN003950	El fitxer `hosts.lpd` (o un d'equivalent) no ha de tenir cap ACL ampliada.	**Ubicació** `/etc/security/pscexpert/dodv2/acldodfiles` **Acció de conformitat** Inhabilita l'ACL ampliada que s'ha especificat. **Nota:** Aquest paràmetre no es canvia automàticament quan es restableix la política per defecte de l'AIX mitjançant el fitxer `DoDv2_to_ AIXDefault.xml`. Heu de canviar manualment aquest paràmetre.
GEN004010	El fitxer `traceroute` no ha de tenir cap ACL ampliada.	**Ubicació** `/etc/security/pscexpert/dodv2/acldodfiles` **Acció de conformitat** Inhabilita l'ACL ampliada que s'ha especificat. **Nota:** Aquest paràmetre no es canvia automàticament quan es restableix la política per defecte de l'AIX mitjançant el fitxer `DoDv2_to_ AIXDefault.xml`. Heu de canviar manualment aquest paràmetre.

Taula 5. Requeriments de la llista de control d'accés (ACL) del departament de defensa (continuació)

ID de punt de comprovació de la guia per a la implementació tècnica de seguretat del departament de defensa	Descripció	Ubicació de l'script on es defineix l'acció i els resultats de l'acció que permeten la conformitat
GEN004390	El fitxer `alias` no ha de tenir cap ACL ampliada.	**Ubicació** `/etc/security/pscexpert/dodv2/acldodfiles` **Acció de conformitat** Inhabilita l'ACL ampliada que s'ha especificat. **Nota:** Aquest paràmetre no es canvia automàticament quan es restableix la política per defecte de l'AIX mitjançant el fitxer `DoDv2_to_ AIXDefault.xml`. Heu de canviar manualment aquest paràmetre.
GEN004430	Els fitxers que s'executen a través d'un fitxer `aliases` de correu no han de tenir ACL ampliades.	**Ubicació** `/etc/security/pscexpert/dodv2/acldodfiles` **Acció de conformitat** Inhabilita l'ACL ampliada que s'ha especificat. **Nota:** Aquest paràmetre no es canvia automàticament quan es restableix la política per defecte de l'AIX mitjançant el fitxer `DoDv2_to_ AIXDefault.xml`. Heu de canviar manualment aquest paràmetre.
GEN004510	El fitxer de registre de servei SMTP no ha de tenir cap ACL ampliada.	**Ubicació** `/etc/security/pscexpert/dodv2/acldodfiles` **Acció de conformitat** Inhabilita l'ACL ampliada que s'ha especificat. **Nota:** Aquest paràmetre no es canvia automàticament quan es restableix la política per defecte de l'AIX mitjançant el fitxer `DoDv2_to_ AIXDefault.xml`. Heu de canviar manualment aquest paràmetre.
GEN004950	El fitxer `ftpusers` no ha de tenir cap ACL ampliada.	**Ubicació** `/etc/security/pscexpert/dodv2/acldodfiles` **Acció de conformitat** Inhabilita l'ACL ampliada que s'ha especificat. **Nota:** Aquest paràmetre no es canvia automàticament quan es restableix la política per defecte de l'AIX mitjançant el fitxer `DoDv2_to_ AIXDefault.xml`. Heu de canviar manualment aquest paràmetre.

Taula 5. Requeriments de la llista de control d'accés (ACL) del departament de defensa (continuació)

ID de punt de comprovació de la guia per a la implementació tècnica de seguretat del departament de defensa	Descripció	Ubicació de l'script on es defineix l'acció i els resultats de l'acció que permeten la conformitat
GEN005190	Els fitxers `.Xauthority` no han de tenir ACL ampliades.	**Ubicació** `/etc/security/pscexpert/dodv2/acldodfiles` **Acció de conformitat** Inhabilita l'ACL ampliada que s'ha especificat. **Nota:** Aquest paràmetre no es canvia automàticament quan es restableix la política per defecte de l'AIX mitjançant el fitxer `DoDv2_to_ AIXDefault.xml`. Heu de canviar manualment aquest paràmetre.
GEN005350	Els fitxers MIB (Management Information Base) no han de tenir ACL ampliades.	**Ubicació** `/etc/security/pscexpert/dodv2/acldodfiles` **Acció de conformitat** Inhabilita l'ACL ampliada que s'ha especificat. **Nota:** Aquest paràmetre no es canvia automàticament quan es restableix la política per defecte de l'AIX mitjançant el fitxer `DoDv2_to_ AIXDefault.xml`. Heu de canviar manualment aquest paràmetre.
GEN005375	El fitxer `snmpd.conf` no ha de tenir cap ACL ampliada	**Ubicació** `/etc/security/pscexpert/dodv2/acldodfiles` **Acció de conformitat** Inhabilita l'ACL ampliada que s'ha especificat. **Nota:** Aquest paràmetre no es canvia automàticament quan es restableix la política per defecte de l'AIX mitjançant el fitxer `DoDv2_to_ AIXDefault.xml`. Heu de canviar manualment aquest paràmetre.
GEN005395	El fitxer `/etc/syslog.conf` no ha de tenir cap ACL ampliada.	**Ubicació** `/etc/security/pscexpert/dodv2/acldodfiles` **Acció de conformitat** Inhabilita l'ACL ampliada que s'ha especificat. **Nota:** Aquest paràmetre no es canvia automàticament quan es restableix la política per defecte de l'AIX mitjançant el fitxer `DoDv2_to_ AIXDefault.xml`. Heu de canviar manualment aquest paràmetre.

Taula 5. Requeriments de la llista de control d'accés (ACL) del departament de defensa (continuació)

ID de punt de comprovació de la guia per a la implementació tècnica de seguretat del departament de defensa	Descripció	Ubicació de l'script on es defineix l'acció i els resultats de l'acció que permeten la conformitat
GEN006150	El fitxer `/usr/lib/smb.conf` no ha de tenir cap ACL ampliada.	**Ubicació** `/etc/security/pscexpert/dodv2/acldodfiles` **Acció de conformitat** Inhabilita l'ACL ampliada que s'ha especificat. **Nota:** Aquest paràmetre no es canvia automàticament quan es restableix la política per defecte de l'AIX mitjançant el fitxer `DoDv2_to_ AIXDefault.xml`. Heu de canviar manualment aquest paràmetre.
GEN006210	El fitxer `/var/private/smbpasswd` no ha de tenir cap ACL ampliada.	**Ubicació** `/etc/security/pscexpert/dodv2/acldodfiles` **Acció de conformitat** Inhabilita l'ACL ampliada que s'ha especificat. **Nota:** Aquest paràmetre no es canvia automàticament quan es restableix la política per defecte de l'AIX mitjançant el fitxer `DoDv2_to_ AIXDefault.xml`. Heu de canviar manualment aquest paràmetre.
GEN006270	El fitxer `/etc/news/hosts.nntp` no ha de tenir cap ACL ampliada.	**Ubicació** `/etc/security/pscexpert/dodv2/acldodfiles` **Acció de conformitat** Inhabilita l'ACL ampliada que s'ha especificat. **Nota:** Aquest paràmetre no es canvia automàticament quan es restableix la política per defecte de l'AIX mitjançant el fitxer `DoDv2_to_ AIXDefault.xml`. Heu de canviar manualment aquest paràmetre.
GEN006290	El fitxer `/etc/news/hosts.nntp.nolimit` no ha de tenir cap ACL ampliada.	**Ubicació** `/etc/security/pscexpert/dodv2/acldodfiles` **Acció de conformitat** Inhabilita l'ACL ampliada que s'ha especificat. **Nota:** Aquest paràmetre no es canvia automàticament quan es restableix la política per defecte de l'AIX mitjançant el fitxer `DoDv2_to_ AIXDefault.xml`. Heu de canviar manualment aquest paràmetre.

Taula 5. Requeriments de la llista de control d'accés (ACL) del departament de defensa (continuació)

ID de punt de comprovació de la guia per a la implementació tècnica de seguretat del departament de defensa	Descripció	Ubicació de l'script on es defineix l'acció i els resultats de l'acció que permeten la conformitat
GEN006310	El fitxer `/etc/news/nnrp.access` no ha de tenir cap ACL ampliada.	**Ubicació** `/etc/security/pscexpert/dodv2/acldodfiles` **Acció de conformitat** Inhabilita l'ACL ampliada que s'ha especificat. **Nota:** Aquest paràmetre no es canvia automàticament quan es restableix la política per defecte de l'AIX mitjançant el fitxer `DoDv2_to_ AIXDefault.xml`. Heu de canviar manualment aquest paràmetre.
GEN006330	El fitxer `/etc/news/passwd.nntp` no ha de tenir cap ACL ampliada.	**Ubicació** `/etc/security/pscexpert/dodv2/acldodfiles` **Acció de conformitat** Inhabilita l'ACL ampliada que s'ha especificat. **Nota:** Aquest paràmetre no es canvia automàticament quan es restableix la política per defecte de l'AIX mitjançant el fitxer `DoDv2_to_ AIXDefault.xml`. Heu de canviar manualment aquest paràmetre.
GEN008120	Si el sistema utilitza LDAP per a la informació d'autenticació o de comptes, el fitxer `/etc/ldap.conf` (o un d'equivalent) no ha de tenir cap llista control d'accés (ACL) ampliada.	**Ubicació** `/etc/security/pscexpert/dodv2/acldodfiles` **Acció de conformitat** Garanteix que els fitxers especificats no tenen cap ACL ampliada. **Nota:** Aquest paràmetre no es canvia automàticament quan es restableix la política per defecte de l'AIX mitjançant el fitxer `DoDv2_to_ AIXDefault.xml`. Heu de canviar manualment aquest paràmetre.
GEN008200	Si el sistema utilitza LDAP per a la informació d'autenticació o de comptes, el fitxer o directori d'entitats certificadores de TLS de l'LDAP (segons correspongui) no ha de tenir cap ACL ampliada.	**Ubicació** `/etc/security/pscexpert/dodv2/acldodfiles` **Acció de conformitat** Garanteix que el directori o el fitxer especificat no té cap ACL ampliada. **Nota:** Aquest paràmetre no es canvia automàticament quan es restableix la política per defecte de l'AIX mitjançant el fitxer `DoDv2_to_ AIXDefault.xml`. Heu de canviar manualment aquest paràmetre.

Informació relacionada:

Conformitat amb la STIG del departament de defensa

Normativa de seguretat de la informació en la indústria de mitjans de pagament

La Normativa de seguretat de la informació en la indústria de mitjans de pagament (PCI - DSS) categoritza la seguretat de TI en 12 seccions que s'anomenen els 12 requeriments i procediments d'assessoria de la seguretat.

Els 12 requeriments i procediments d'assessoria de la seguretat de TI que defineix la PCI - DSS inclouen els elements següents:

Requeriment 1: Instal•leu i feu el manteniment d'una configuració de tallafoc per protegir les dades del titular de targetes.

Llista de serveis i ports documentats necessaris per a l'empresa. Aquest requeriment s'implementa mitjançant la inhabilitació de serveis no necessaris i no protegits.

Requeriment 2: No utilitzeu els valors per defecte subministrats pel proveïdor per a contrasenyes del sistema i altres paràmetres de seguretat.

Canvieu sempre els valors per defecte subministrats pel proveïdor abans d'instal•lar un sistema a la xarxa. Aquest requeriment s'implementa inhabilitant el daemon Simple Network Management Protocol (SNMP).

Requeriment 3: Protegiu les dades emmagatzemades del titular de targetes.

Aquest requeriment s'implementa habilitant la funció Encrypted File System (EFS) que se subministra amb el sistema operatiu AIX.

Requeriment 4: Xifreu dades del titular de targetes quan transmeteu les dades a través de xarxes públiques obertes.

Aquest requeriment s'implementa habilitant la funció IP Security (IPSEC) que se subministra amb el sistema operatiu AIX.

Requeriment 5: Utilitzeu i actualitzeu regularment els programes de programari antivirus.

Aquest requeriment s'implementa mitjançant el programa de polítiques d'execució fiable. L'execució fiable és el programari antivirus recomanat i és natiu per al sistema operatiu AIX. El PCI requereix que captureu els registres del programa d'execució fiable habilitant el SIEM (Security Information and Event Management - gestió de la informació i dels esdeveniment de seguretat) per supervisar les alertes. Amb l'execució del programa d'execució fiable en mode de només registre no s'aturen les comprovacions quan es genera un error per una manca de coincidència de hash.

Requeriment 6: Desenvolupeu i conserveu els sistemes i les aplicacions segurs.

Per implementar aquest requeriment, heu d'instal•lar manualment els pedaços necessaris pel vostre sistema. Si heu adquirit el producte PowerSC Standard Edition, podeu utilitzar la funció Trusted Network Connect (TNC).

Requeriment 7: Restringiu l'accés a les dades del titular de la targeta, segons la necessitat empresarial que conegueu.

Podeu implementar les mesures de control d'accés estrictes utilitzant la funció RBAC per tal d'habilitar les regles i els rols. L'RBAC no es pot automatitzar perquè requereix que hi hagi habilitada l'entrada d'un administrador.

Amb `RbacEnablement` es comprova el sistema per determinar si existeixen les propietats isso, so i sa pels rols al sistema. Si no existeixen aquestes propietats, l'script les crea. Aquest script també s'executa com a part de les comprovacions de pscexpert que du a terme quan executa ordres com, per exemple, l'ordre `pscxpert -c`.

Requeriment 8: Assigneu un ID únic a cada persona que tingui accés al sistema.

Podeu implementar aquest requeriment habilitant els perfils PCI. Les regles següents s'apliquen al perfil PCI:

- Canviar les contrasenyes d'usuari com a mínim cada 90 dies.
- Exigir una longitud mínima de contrasenya de 7 caràcters.

- Utilitzar una contrasenya que contingui caràcters numèrics i alfabètics.
- No permetre que cap persona enviï una contrasenya nova que sigui la mateixa que una de les quatre darreres contrasenyes utilitzades.
- Limitar els intents d'accés repetits bloquejant l'ID d'usuari després de sis intents no satisfactoris.
- Establir la duració del bloqueig en 30 minuts o fins que una administrador torni a habilitar l'ID d'usuari.
- Requerir que l'usuari torni a escriure la contrasenya per reactivar un terminal després que hagi estat inactiu durant 15 minuts o més.

Requeriment 9: Restringiu l'accés físic a les dades del titular de targetes.
Emmagatzema dipòsits que contenen dades confidencials del titular de targetes en un espai d'accés restringit.

Requeriment 10: Feu un seguiment i supervisar tots els accessos als recursos de xarxa i a les dades del titular de targetes.
Aquest requeriment s'implementa registrant l'accés als components del sistema mitjançant l'habilitació de registres automàtics als components del sistema.

Requeriment 11: Comproveu freqüentment els sistemes i els processos de seguretat.
Aquest requeriment s'implementa utilitzant la funció Real-Time Compliance.

Requeriment 12: Conserveu una política de seguretat que inclogui la seguretat d'informació per a empleats i contractistes.
Activació de mòdems per a proveïdors només quan ho necessitin els proveïdor amb una desactivació immediata després de l'ús. Aquest requeriment s'implementa inhabilitant l'inici de sessió root remot, duent a terme l'activació en una base necessària mitjançant un administrador del sistema i efectuant una desactivació quan ja no calgui.

El PowerSC Standard Edition redueix la gestió de la configuració que és necessària per complir les directrius definides per la versió 2.0 de PCI DSS i la versió 3.0 de PCI DSS. Això no obstant, no es pot automatitzar el procés complet.

Per exemple, la restricció de l'accés a les dades del titular de targetes en funció del requeriment empresarial no es pot automatitzar. El sistema operatiu AIX proporciona potents tecnologies de seguretat com, per exemple, Role Based Access Control (RBAC); això no obstant, elPowerSC Standard Edition no pot automatitzar aquesta configuració perquè no pot determinar les persones que necessiten accés i les que no. L'IBM Compliance Expert pot automatitzar la configuració d'altres paràmetres de seguretat que són coherents amb els requeriments PCI.

Quan s'aplica el perfil PCI a un entorn de base de dades, hi ha diversos ports de TCP i UDP que utilitza la pila de programari que s'inhabiliten per les restriccions. Heu d'habilitar aquests ports i inhabilitar la funció Trusted Execution per tal d'executar l'aplicació i la càrrega de treball. Executeu les ordres següents per eliminar les restriccions als ports i inhabilitar la funció d'execució fiable:

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

Nota: Tots els fitxers d'scripts personalitzats que es proporcionen per mantenir la conformitat PCI - DSS es troben al directori `/etc/security/pscexpert/bin`.

A la taula següent es mostra la forma en què gestiona el PowerSC Standard Edition els requeriments de la normativa PCI DSS utilitzant les funcions de la utilitat AIX Security Expert:

Taula 6. Paràmetres relacionats amb les normatives de les versions 2.0 i 3.0 de conformitat amb la PCI DSS

Implementa aquestes normatives PCI DSS	Especificació de la implementació	La implementació de l'AIX Security Expert	Ubicació de l'script que modifica el valor
2.1	Canviar sempre els valors per defecte subministrats pel proveïdor abans d'instal•lar un sistema a la xarxa. Per exemple, incloure contrasenyes, cadenes simples de la comunitat de protocol de gestió de xarxes i eliminar els comptes innecessaris.	Estableix el nombre mínim de setmanes que han de passar abans que pugueu canviar una contrasenya a 0 setmanes definint el paràmetre **minage** en un valor de 0.	/etc/security/pscexpert/bin/chusrattr
PCI versió 2 8.5.9 **PCI versió 3** 8.2.4	Canviar les contrasenyes d'usuari com a mínim cada 90 dies.	Estableix el nombre màxim de setmanes que és vàlida una contrasenya a 13 setmanes definint el paràmetre **maxage** en un valor de 13.	/etc/security/pscexpert/bin/chusrattr
2.1	Canviar sempre els valors per defecte subministrats pel proveïdor abans d'instal•lar un sistema a la xarxa. Per exemple, incloure contrasenyes, cadenes simples de la comunitat de protocol de gestió de xarxes i eliminar els comptes innecessaris.	Estableix en 8 el nombre de setmanes que un compte amb una contrasenya caducada es manté al sistema definint el paràmetre **maxexpired** en un valor de 8.	/etc/security/pscexpert/bin/chusrattr
PCI versió 2 8.5.10 **PCI versió 3** 8.2.3	Exigir una longitud mínima de contrasenya d'almenys 7 caràcters.	Estableix la longitud mínima de contrasenya en 7 caràcters definint el paràmetre **minlen** en un valor de 7.	/etc/security/pscexpert/bin/chusrattr
PCI versió 2 8.5.11 **PCI versió 3** 8.2.3	Utilitzar contrasenyes que continguin caràcters tan numèrics com alfabètics.	Estableix en 1 el nombre mínim de caràcters necessaris en una contrasenya. Aquest paràmetre garanteix que la contrasenya contingui caràcters alfabètics establint el paràmetre **minalpha** en un valor d'1.	/etc/security/pscexpert/bin/chusrattr
PCI versió 2 8.5.11 **PCI versió 3** 8.2.3	Utilitzar contrasenyes que continguin caràcters tan numèrics com alfabètics.	Estableix en 1 el nombre mínim de caràcters no alfabètics necessaris en una contrasenya. Aquest paràmetre garanteix que la contrasenya contingui caràcters no alfabètics establint el paràmetre **minother** en un valor d'1.	/etc/security/pscexpert/bin/chusrattr

Taula 6. Paràmetres relacionats amb les normatives de les versions 2.0 i 3.0 de conformitat amb la PCI DSS (continuació)

Implementa aquestes normatives PCI DSS	Especificació de la implementació	La implementació de l'AIX Security Expert	Ubicació de l'script que modifica el valor
PCI versió 2 2.1 **PCI versió 3** 8.2.2	Canviar sempre els valors per defecte subministrats pel proveïdor abans d'instal•lar un sistema a la xarxa. Per exemple, incloure contrasenyes, cadenes simples de la comunitat de protocol de gestió de xarxes i eliminar els comptes innecessaris.	Estableix en 8 el nombre màxim de vegades que es pot repetir un caràcter en una contrasenya establint el paràmetre **maxrepeats** en un valor de 8. Aquest valor indica que es pot repetir un caràcter en una contrasenya un nombre il•limitat de vegades quan compleixi les altres limitacions de contrasenya.	`/etc/security/pscexpert/bin/chusrattr`
PCI versió 2 8.5.12 **PCI versió 3** 8.2.5	No permetre que cap persona enviï una contrasenya nova que sigui la mateixa que una de les quatre darreres contrasenyes utilitzades.	Estableix en 52 el nombre de setmanes que es pot reutilitzar una contrasenya definint el paràmetre **histexpire** en un valor de 52.	`/etc/security/pscexpert/bin/chusrattr`
PCI versió 2 8.5.12 **PCI versió 3** 8.2.5	No permetre que cap persona enviï una contrasenya nova que sigui la mateixa que una de les quatre darreres contrasenyes utilitzades.	Estableix en 4 el nombre de contrasenyes anteriors que no es poden utilitzant establint el paràmetre **histsize** en un valor de 4.	`/etc/security/pscexpert/bin/chusrattr`
PCI versió 2 8.5.13 **PCI versió 3** 8.1.6	Limitar els intents repetits d'accés bloquejant l'ID d'usuari després de com a màxim sis intents.	Estableix el nombre d'intents consecutius d'inici de sessió no aconseguits que inhabilita el compte en 6 intents per a cada compte no root establint el paràmetre **loginentries** en un valor de 6.	`/etc/security/pscexpert/bin/chusrattr`
PCI versió 2 8.5.13 **PCI versió 3** 8.1.6	Limitar els intents repetits d'accés bloquejant l'ID d'usuari després de com a màxim sis intents.	Estableix el nombre d'intents consecutius d'inici de sessió no aconseguits que inhabilita un port en 6 intents establint el paràmetre **logindisable** en un valor de 6.	• `/etc/security/pscexpert/bin/chdefstanza` • `/etc/security/login.cfg`
PCI versió 2 8.5.14 **PCI versió 3** 8.1.7	Establir la duració de bloqueig en un mínim de 30 minuts o fins que l'administrador habiliti l'ID d'usuari.	Estableix la duració de temps en què un port està bloquejat una vegada inhabilitat per l'atribut *logindisable* en 30 minuts establint el paràmetre **loginreenable** en un valor de 30.	• `/etc/security/pscexpert/bin/chdefstanza` • `/etc/security/login.cfg`
12.3.9	Activació de tecnologies d'accés remot per a proveïdors i socis només quan aquests ho necessitin, amb una desactivació immediata després d'utilitzar-les.	Inhabilita la funció d'inici de sessió com a root remot establint aquest valor com a fals. L'administrador del sistema pot activar la funció d'inici de sessió remot quan calgui i, a continuació, desactivar-la quan es completi la tasca.	• `/etc/security/pscexpert/bin/chuserstanza` • `/etc/security/user`

Taula 6. Paràmetres relacionats amb les normatives de les versions 2.0 i 3.0 de conformitat amb la PCI DSS (continuació)

Implementa aquestes normatives PCI DSS	Especificació de la implementació	La implementació de l'AIX Security Expert	Ubicació de l'script que modifica el valor
8.1.1	Assignar a tots els usuaris un ID únic abans de permetre'ls accedir als components del sistema o a les dades de titulars de targetes.	Habilita la funció que garanteix que tots els usuaris tinguin un nom d'usuari exclusiu abans de poder accedir als components del sistema o a les dades dels titulars de targetes establint aquesta funció en un valor de true.	• `/etc/security/pscexpert/bin/chuserstanza` • `/etc/security/user`
10.2	Habilitar l'auditoria al sistema.	Habilita l'auditoria dels fitxers binaris al sistema.	`/etc/security/pscexpert/bin/pciaudit`
PCI versió 2 1.1.5 2.2.2 **PCI versió 3** 2.2.2	Inhabilitar els serveis innecessaris i no segurs, que inclou l'entorn d'escriptori comú (CDE - Common Desktop Environment).	Inhabilita la funció del CDE qua no s'ha configurat l'LFT (Layer Four Traceroute).	`/etc/security/pscexpert/bin/comntrows`
PCI versió 2 1.1.5 2.2.2 **PCI versió 3** 2.2.2	Inhabilitar els serveis innecessaris i no segurs, que inclou el daemon `timed`.	Atura el daemon `timed` i descomenta l'entrada corresponent al fitxer `/etc/rc.tcpip` que inicia automàticament el daemon.	`/etc/security/pscexpert/bin/rctcpip`
PCI versió 2 1.1.5 2.2.2 **PCI versió 3** 2.2.2	Inhabilitar els serveis innecessaris i no segurs, que inclou el daemon `rwhod`.	Atura el daemon `rwhod` i descomenta l'entrada corresponent al fitxer `/etc/rc.tcpip` que inicia automàticament el daemon.	`/etc/security/pscexpert/bin/rctcpip`
PCI versió 2 2.1 **PCI versió 3** 2.1.1	Canviar els valors per defecte subministrats pel proveïdor abans d'instal•lar un sistema a la xarxa, que inclou la inhabilitació del daemon `SNMP`.	Atura el daemon `SNMP` i descomenta l'entrada corresponent al fitxer `/etc/rc.tcpip` que inicia automàticament el daemon.	`/etc/security/pscexpert/bin/rctcpip`
PCI versió 2 2.1 **PCI versió 3** 2.1.1	Canviar els valors per defecte subministrats pel proveïdor abans d'instal•lar un sistema a la xarxa, que inclou la inhabilitació del daemon `SNMPMIBD`.	Inhabilita el daemon `SNMPMIBD` descomentant l'entrada corresponent al fitxer `/etc/rc.tcpip` que inicia automàticament el daemon.	`/etc/security/pscexpert/bin/rctcpip`
2.1	Canviar els valors per defecte subministrats pel proveïdor abans d'instal•lar un sistema a la xarxa, que inclou la inhabilitació del daemon `AIXMIBD`.	Inhabilita el daemon `AIXMIBD` descomentant l'entrada corresponent al fitxer `/etc/rc.tcpip` que inicia automàticament el daemon.	`/etc/security/pscexpert/bin/rctcpip`

Taula 6. Paràmetres relacionats amb les normatives de les versions 2.0 i 3.0 de conformitat amb la PCI DSS (continuació)

Implementa aquestes normatives PCI DSS	Especificació de la implementació	La implementació de l'AIX Security Expert	Ubicació de l'script que modifica el valor
2.1	Canviar els valors per defecte subministrats pel proveïdor abans d'instal•lar un sistema a la xarxa, que inclou la inhabilitació del daemon HOSTMIBD.	Inhabilita el daemon HOSTMIBD descomentant l'entrada corresponent al fitxer /etc/rc.tcpip que inicia automàticament el daemon.	/etc/security/pscexpert/bin/rctcpip
PCI versió 2 1.1.5 2.2.2 **PCI versió 3** 2.2.2	Inhabilitar els serveis innecessaris i no segurs, que inclou el daemon DPID2.	Atura el daemon DPID2 i descomenta l'entrada corresponent al fitxer /etc/rc.tcpip que inicia automàticament el daemon.	/etc/security/pscexpert/bin/rctcpip
PCI versió 2 2.1 **PCI versió 3** 2.2.2	Canviar els valors per defecte subministrats pel proveïdor abans d'instal•lar un sistema a la xarxa, que inclou l'aturada del servidor DHCP.	Inhabilita el servidor DHCP.	/etc/security/pscexpert/bin/rctcpip
PCI versió 2 1.1.5 2.2.2 **PCI versió 3** 2.2.2	Inhabilitar els serveis innecessaris i no segurs, que inclou l'agent DHCP.	Atura i inhabilita l'agent de retransmissió del DHCP i descomenta l'entrada corresponent al fitxer /etc/rc.tcpip que inicia automàticament l'agent.	/etc/security/pscexpert/bin/rctcpip
PCI versió 2 1.1.5 2.2.2 **PCI versió 3** 2.2.2	Inhabilitar els serveis innecessaris i no segurs, que inclou el daemon rshd.	Atura i inhabilita totes les instàncies del daemon rshd i el servei de l'intèrpret d'ordres, i descomenta les entrades corresponents al fitxer /etc/inetd.conf que inicia automàticament les instàncies.	/etc/security/pscexpert/bin/cominetdconf
PCI versió 2 1.1.5 2.2.2 **PCI versió 3** 2.2.2	Inhabilitar els serveis innecessaris i no segurs, que inclou el daemon rlogind.	Atura i inhabilita totes les instàncies del daemon rlogind i el servei rlogin. La utilitat AIX Security Expert també descomenta les entrades corresponents al fitxer /etc/inetd.conf que automàticament inicia les instàncies.	/etc/security/pscexpert/bin/cominetdconf
PCI versió 2 1.1.5 2.2.2 **PCI versió 3** 2.2.2	Inhabilitar els serveis innecessaris i no segurs, que inclou el daemon rexecd.	Atura i inhabilita totes les instàncies del daemon rexecd. La utilitat AIX Security Expert també descomenta l'entrada corresponent al fitxer /etc/inetd.conf que automàticament inicia el daemon.	/etc/security/pscexpert/bin/cominetdconf

Taula 6. Paràmetres relacionats amb les normatives de les versions 2.0 i 3.0 de conformitat amb la PCI DSS (continuació)

Implementa aquestes normatives PCI DSS	Especificació de la implementació	La implementació de l'AIX Security Expert	Ubicació de l'script que modifica el valor
PCI versió 2 1.1.5 2.2.2 **PCI versió 3** 2.2.2	Inhabilitar els serveis innecessaris i no segurs, que inclou el daemon `comsat`.	Atura i inhabilita totes les instàncies del daemon `comsat`. La utilitat AIX Security Expert també descomenta l'entrada corresponent al fitxer `/etc/inetd.conf` que automàticament inicia el daemon.	`/etc/security/pscexpert/bin/cominetdconf`
PCI versió 2 1.1.5 2.2.2 **PCI versió 3** 2.2.2	Inhabilitar els serveis innecessaris i no segurs, que inclou el daemon `fingerd`.	Atura i inhabilita totes les instàncies del daemon `fingerd`. La utilitat AIX Security Expert també descomenta l'entrada corresponent al fitxer `/etc/inetd.conf` que automàticament inicia el daemon.	`/etc/security/pscexpert/bin/cominetdconf`
PCI versió 2 1.1.5 2.2.2 **PCI versió 3** 2.2.2	Inhabilitar els serveis innecessaris i no segurs, que inclou el daemon `systat`.	Atura i inhabilita totes les instàncies del daemon `systat`. La utilitat AIX Security Expert també descomenta l'entrada corresponent al fitxer `/etc/inetd.conf` que automàticament inicia el daemon.	`/etc/security/pscexpert/bin/cominetdconf`
2.1	Canviar els valors per defecte subministrats pel proveïdor abans d'instal•lar un sistema a la xarxa, que inclou la inhabilitació de l'ordre `netstat`.	Inhabilita l'ordre `netstat` descomentant l'entrada corresponent al fitxer `/etc/inetd.conf`.	`/etc/security/pscexpert/bin/cominetdconf`
PCI versió 2 1.1.5 2.2.2 **PCI versió 3** 2.2.3	Inhabilitar els serveis innecessaris i no segurs, que inclou el daemon `tftp`.	Atura i inhabilita totes les instàncies del daemon `tftp`. La utilitat AIX Security Expert també descomenta l'entrada corresponent al fitxer `/etc/inetd.conf` que automàticament inicia el daemon.	`/etc/security/pscexpert/bin/cominetdconf`
PCI versió 2 1.1.5 2.2.2 **PCI versió 3** 2.2.2	Inhabilitar els serveis innecessaris i no segurs, que inclou el daemon `talkd`.	Atura i inhabilita totes les instàncies del daemon `talkd`. La utilitat AIX Security Expert també descomenta l'entrada corresponent al fitxer `/etc/inetd.conf` que automàticament inicia el daemon.	`/etc/security/pscexpert/bin/cominetdconf`
PCI versió 2 1.1.5 2.2.2 **PCI versió 3** 2.2.2	Inhabilitar els serveis innecessaris i no segurs, que inclou el daemon `rquotad`.	Atura i inhabilita totes les instàncies del daemon `rquotad`. La utilitat AIX Security Expert també descomenta l'entrada corresponent al fitxer `/etc/inetd.conf` que automàticament inicia el daemon.	`/etc/security/pscexpert/bin/cominetdconf`

Taula 6. Paràmetres relacionats amb les normatives de les versions 2.0 i 3.0 de conformitat amb la PCI DSS (continuació)

Implementa aquestes normatives PCI DSS	Especificació de la implementació	La implementació de l'AIX Security Expert	Ubicació de l'script que modifica el valor
PCI versió 2 1.1.5 2.2.2 **PCI versió 3** 2.2.2	Inhabilitar els serveis innecessaris i no segurs, que inclou el daemon `rstatd`.	Atura i inhabilita totes les instàncies del daemon `rstatd`. La utilitat AIX Security Expert també descomenta l'entrada corresponent al fitxer `/etc/inetd.conf` que automàticament inicia el daemon.	`/etc/security/pscexpert/bin/cominetdconf`
PCI versió 2 1.1.5 2.2.2 **PCI versió 3** 2.2.2	Inhabilitar els serveis innecessaris i no segurs, que inclou el daemon `rusersd`.	Atura i inhabilita totes les instàncies del daemon `rusersd`. La utilitat AIX Security Expert també descomenta l'entrada corresponent al fitxer `/etc/inetd.conf` que automàticament inicia el daemon.	`/etc/security/pscexpert/bin/cominetdconf`
PCI versió 2 1.1.5 2.2.2 **PCI versió 3** 2.2.2	Inhabilitar els serveis innecessaris i no segurs, que inclou el daemon `rwalld`.	Atura i inhabilita totes les instàncies del daemon `rwalld`. La utilitat AIX Security Expert també descomenta l'entrada corresponent al fitxer `/etc/inetd.conf` que automàticament inicia el daemon.	`/etc/security/pscexpert/bin/cominetdconf`
PCI versió 2 1.1.5 2.2.2 **PCI versió 3** 2.2.2	Inhabilitar els serveis innecessaris i no segurs, que inclou el daemon `sprayd`.	Atura i inhabilita totes les instàncies del daemon `sprayd`. La utilitat AIX Security Expert també descomenta l'entrada corresponent al fitxer `/etc/inetd.conf` que automàticament inicia el daemon.	`/etc/security/pscexpert/bin/cominetdconf`
PCI versió 2 1.1.5 2.2.2 **PCI versió 3** 2.2.2	Inhabilitar els serveis innecessaris i no segurs, que inclou el daemon `pcnfsd`.	Atura i inhabilita totes les instàncies del daemon `pcnfsd`. La utilitat AIX Security Expert també descomenta l'entrada corresponent al fitxer `/etc/inetd.conf` que automàticament inicia el daemon.	`/etc/security/pscexpert/bin/cominetdconf`
PCI versió 2 1.1.5 2.2.2 **PCI versió 3** 2.2.2	Inhabilitar els serveis innecessaris i no segurs, que inclou el servei `TCP echo`.	Atura i inhabilita totes les instàncies del servei `echo`. La utilitat AIX Security Expert també descomenta l'entrada corresponent al fitxer `/etc/inetd.conf` que automàticament inicia el servei.	`/etc/security/pscexpert/bin/cominetdconf`
PCI versió 2 1.1.5 2.2.2 **PCI versió 3** 2.2.2	Inhabilitar els serveis innecessaris i no segurs, que inclou el servei `TCP discard`.	Atura i inhabilita totes les instàncies del servei `discard`. La utilitat AIX Security Expert també descomenta l'entrada corresponent al fitxer `/etc/inetd.conf` que automàticament inicia el servei.	`/etc/security/pscexpert/bin/cominetdconf`

Taula 6. Paràmetres relacionats amb les normatives de les versions 2.0 i 3.0 de conformitat amb la PCI DSS (continuació)

Implementa aquestes normatives PCI DSS	Especificació de la implementació	La implementació de l'AIX Security Expert	Ubicació de l'script que modifica el valor
PCI versió 2 1.1.5 2.2.2 **PCI versió 3** 2.2.2	Inhabilitar els serveis innecessaris i no segurs, que inclou el servei TCP `chargen`.	Atura i inhabilita totes les instàncies del servei `chargen`. La utilitat AIX Security Expert també descomenta l'entrada corresponent al fitxer `/etc/inetd.conf` que automàticament inicia el servei.	`/etc/security/pscexpert/bin/cominetdconf`
PCI versió 2 1.1.5 2.2.2 **PCI versió 3** 2.2.2	Inhabilitar els serveis innecessaris i no segurs, que inclou el servei TCP `daytime`.	Atura i inhabilita totes les instàncies del servei `daytime`. La utilitat AIX Security Expert també descomenta l'entrada corresponent al fitxer `/etc/inetd.conf` que automàticament inicia el servei.	`/etc/security/pscexpert/bin/cominetdconf`
PCI versió 2 1.1.5 2.2.2 **PCI versió 3** 2.2.2	Inhabilitar els serveis innecessaris i no segurs, que inclou el servei TCP `time`.	Atura i inhabilita totes les instàncies del servei `timed`. La utilitat AIX Security Expert també descomenta l'entrada corresponent al fitxer `/etc/inetd.conf` que automàticament inicia el servei.	`/etc/security/pscexpert/bin/cominetdconf`
PCI versió 2 1.1.5 2.2.2 **PCI versió 3** 2.2.2	Inhabilitar els serveis innecessaris i no segurs, que inclou el servei UDP `echo`.	Atura i inhabilita totes les instàncies del servei `echo(udp)`. La utilitat AIX Security Expert també descomenta l'entrada corresponent al fitxer `/etc/inetd.conf` que automàticament inicia el servei.	`/etc/security/pscexpert/bin/cominetdconf`
PCI versió 2 1.1.5 2.2.2 **PCI versió 3** 2.2.2	Inhabilitar els serveis innecessaris i no segurs, que inclou el servei UDP `discard`.	Atura i inhabilita totes les instàncies del servei `discard(udp)`. La utilitat AIX Security Expert també descomenta l'entrada corresponent al fitxer `/etc/inetd.conf` que automàticament inicia el servei.	`/etc/security/pscexpert/bin/cominetdconf`
PCI versió 2 1.1.5 2.2.2 **PCI versió 3** 2.2.2	Inhabilitar els serveis innecessaris i no segurs, que inclou el servei UDP `chargen`.	Atura i inhabilita totes les instàncies del servei `chargen(udp)`. La utilitat AIX Security Expert també descomenta l'entrada corresponent al fitxer `/etc/inetd.conf` que automàticament inicia el servei.	`/etc/security/pscexpert/bin/cominetdconf`
PCI versió 2 1.1.5 2.2.2 **PCI versió 3** 2.2.2	Inhabilitar els serveis innecessaris i no segurs, que inclou el servei UDP `daytime`.	Atura i inhabilita totes les instàncies del servei `daytime(udp)`. La utilitat AIX Security Expert també descomenta l'entrada corresponent al fitxer `/etc/inetd.conf` que automàticament inicia el servei.	`/etc/security/pscexpert/bin/cominetdconf`

Taula 6. Paràmetres relacionats amb les normatives de les versions 2.0 i 3.0 de conformitat amb la PCI DSS (continuació)

Implementa aquestes normatives PCI DSS	Especificació de la implementació	La implementació de l'AIX Security Expert	Ubicació de l'script que modifica el valor
PCI versió 2 1.1.5 2.2.2 **PCI versió 3** 2.2.2	Inhabilitar els serveis innecessaris i no segurs, que inclou el servei `UDP time`.	Atura i inhabilita totes les instàncies del servei `timed(udp)`. La utilitat AIX Security Expert també descomenta l'entrada corresponent al fitxer `/etc/inetd.conf` que automàticament inicia el servei.	`/etc/security/pscexpert/bin/cominetdconf`
PCI versió 2 1.1.5 2.2.2 **PCI versió 3** 2.2.3	Inhabilitar els serveis innecessaris i no segurs, que inclou el servei `FTP`.	Atura i inhabilita totes les instàncies del daemon `ftpd`. La utilitat AIX Security Expert també descomenta l'entrada corresponent al fitxer `/etc/inetd.conf` que automàticament inicia el daemon.	`/etc/security/pscexpert/bin/cominetdconf`
PCI versió 2 1.1.5 2.2.2 **PCI versió 3** 2.2.3	Inhabilitar els serveis innecessaris i no segurs, que inclou el servei `telnet`.	Atura i inhabilita totes les instàncies del daemon `telnetd`. La utilitat AIX Security Expert també descomenta l'entrada corresponent al fitxer `/etc/inetd.conf` que automàticament inicia el daemon.	`/etc/security/pscexpert/bin/cominetdconf`
PCI versió 2 1.1.5 2.2.2 **PCI versió 3** 2.2.2	Inhabilitar els serveis innecessaris i no segurs, que inclou el servei `dtspc`.	Atura i inhabilita totes les instàncies del daemon `dtspc`. La utilitat AIX Security Expert també descomenta l'entrada corresponent al fitxer `/etc/inittab` que automàticament inicia el daemon quan no s'ha configurat l'LFT i el CDE està inhabilitat al fitxer `/etc/inittab`.	`/etc/security/pscexpert/bin/cominetdconf`
PCI versió 2 1.1.5 2.2.2 **PCI versió 3** 2.2.2	Inhabilitar els serveis innecessaris i no segurs, que inclou el servei `ttdbserver`.	Atura i inhabilita totes les instàncies del servei `ttdbserver`. La utilitat AIX Security Expert també descomenta l'entrada corresponent al fitxer `/etc/inetd.conf` que automàticament inicia el servei.	`/etc/security/pscexpert/bin/cominetdconf`
PCI versió 2 1.1.5 2.2.2 **PCI versió 3** 2.2.2	Inhabilitar els serveis innecessaris i no segurs, que inclou el servei `cmsd`.	Atura i inhabilita totes les instàncies del servei `cmsd`. La utilitat AIX Security Expert també descomenta l'entrada corresponent al fitxer `/etc/inetd.conf` que automàticament inicia el servei.	`/etc/security/pscexpert/bin/cominetdconf`

Taula 6. Paràmetres relacionats amb les normatives de les versions 2.0 i 3.0 de conformitat amb la PCI DSS (continuació)

Implementa aquestes normatives PCI DSS	Especificació de la implementació	La implementació de l'AIX Security Expert	Ubicació de l'script que modifica el valor
PCI versió 2 2.2.3 **PCI versió 3** 2.2.4	Configurar els paràmetres de seguretat del sistema per evitar-ne un mal ús.	Elimina les ordres d'establiment d'ID d'usuari (SUID) descomentant l'entrada corresponent al fitxer `/etc/inetd.conf` que automàticament habilita les ordres.	`/etc/security/pscexpert/bin/rmsuidfrmrcmds`
PCI versió 2 2.2.3 **PCI versió 3** 2.2.4	Configurar els paràmetres de seguretat del sistema per evitar-ne un mal ús.	Habilita el nivell de seguretat més baix pel Gestor de permisos de fitxer.	`/etc/security/pscexpert/bin/filepermgr`
PCI versió 2 2.2.3 **PCI versió 3** 2.2.4	Configurar els paràmetres de seguretat del sistema per evitar-ne un mal ús.	Modifica el protocol del sistema de fitxers de xarxa amb els paràmetres restringits que compleixen els requeriments de seguretat PCI. Aquests paràmetres restringits inclouen la inhabilitació de l'accés root remot i l'accés UID i GID anònim.	`/etc/security/pscexpert/bin/nfsconfig`
PCI versió 2 2.2.2 **PCI versió 3** 2.2.3	Inhabilitar només els serveis, protocols, daemons, etc. necessaris i segurs, quan calguin per al funcionament correcte del sistema. Implementar les funcions de seguretat per als serveis, protocols o daemons necessaris que es consideren no segurs.	Inhabilita els daemons `rlogind`, `rshd` i `tftpd` que no siguin segurs.	`/etc/security/pscexpert/bin/disrmtdmns`
PCI versió 2 2.2.2 **PCI versió 3** 2.2.3	Inhabilitar només els serveis, protocols, daemons, etc. necessaris i segurs, quan calguin per al funcionament correcte del sistema. Implementar les funcions de seguretat per als serveis, protocols o daemons necessaris que es consideren no segurs.	Inhabilita els daemons `rlogind`, `rshd` i `tftpd` que no siguin segurs.	`/etc/security/pscexpert/bin/rmrhostsnetrc`
PCI versió 2 2.2.2 **PCI versió 3** 2.2.3	Inhabilitar només els serveis, protocols, daemons, etc. necessaris i segurs, quan calguin per al funcionament correcte del sistema. Implementar les funcions de seguretat per als serveis, protocols o daemons necessaris que es consideren no segurs.	Inhabilita els daemons `logind`, `rshd` i `tftpdpci_rmetchostsequiv` que no siguin segurs.	`/etc/security/pscexpert/bin/rmetchostsequiv`

Taula 6. Paràmetres relacionats amb les normatives de les versions 2.0 i 3.0 de conformitat amb la PCI DSS (continuació)

Implementa aquestes normatives PCI DSS	Especificació de la implementació	La implementació de l'AIX Security Expert	Ubicació de l'script que modifica el valor
PCI versió 2 1.3.6 **PCI versió 3** 2.2.3	Implementar la inspecció amb estat, o el filtrat de paquets, en què només es permeten a la xarxa les connexions establertes.	Habilita l'opció de xarxa **clean_partial_conns** establint-ne el valor en 1.	/etc/security/pscexpert/bin/ntwkopts
PCI versió 2 2.2.2 **PCI versió 3** 2.2.3	Implementar la inspecció amb estat, o el filtrat de paquets, en què només es permeten a la xarxa les connexions establertes.	Habilita la seguretat TCP establint l'opció de xarxa **tcp_tcpsecure** en un valor de 7. Aquest paràmetre proporciona protecció envers els atacs a dades, restabliments (RST) i sol•licituds de connexió TCP (SYN).	/etc/security/pscexpert/bin/ntwkopts
1.2	Protegir l'accés no autoritzat a ports no utilitzats.	Configura el sistema per rebutjar els amfitrions durant 5 minuts per tal d'evitar que altres sistemes accedeixin a ports no utilitzats.	/etc/security/pscexpert/bin/ipsecshunhosthls **Nota:** Podeu escriure regles de filtre addicionals al fitxer /etc/security/aixpert/bin/filter.txt. Aquestes regles s'integren a l'script ipsecshunhosthls.sh quan s'aplica el perfil. Les entrades han de tenir el format següent: *número_port*:*adreça_IP*:*acció* en què els valors possibles d'*acció* són Allow o Deny.
1.2	Protegir l'amfitrió de les exploracions dels ports.	Configura el sistema per rebutjar els ports vulnerables durant 5 minuts, el que evita les exploracions dels ports.	/etc/security/pscexpert/bin/ipsecshunports **Nota:** Podeu escriure regles de filtre addicionals al fitxer /etc/security/aixpert/bin/filter.txt. Aquestes regles s'integren a l'script ipsecshunhosthls.sh quan s'aplica el perfil. Les entrades han de tenir el format següent: *número_port*:*adreça_IP*:*acció* en què els valors possibles d'*acció* són Allow o Deny.
7.1.1	Limitar els permisos de creació d'objectes.	Estableix els permisos per defecte de creació d'objectes en 22 establint el paràmetre **umask** en un valor de 22.	/etc/security/pscexpert/bin/chusrattr
7.1.1	Limitar l'accés del sistema.	Garanteix que l'ID arrel sigui l'únic que apareix llistat el fitxer cron.allow i elimina el fitxer cron.deny del sistema.	/etc/security/pscexpert/bin/limitsysacc
6.5.8	Eliminar el punt del camí d'accés root.	Elimina els punts de la variable d'entorn PATH dels fitxers següents que es troben al directori inicial arrel: • .cshrc • .kshrc • .login • .profile	/etc/security/pscexpert/bin/rmdotfrmpathroot

Taula 6. Paràmetres relacionats amb les normatives de les versions 2.0 i 3.0 de conformitat amb la PCI DSS (continuació)

Implementa aquestes normatives PCI DSS	Especificació de la implementació	La implementació de l'AIX Security Expert	Ubicació de l'script que modifica el valor
6.5.8	Eliminar el punt del camí d'accés no root:	Elimina els punts de la variable d'entorn *PATH* dels fitxers següents que es troben al directori inicial de l'usuari: • .cshrc • .kshrc • .login • .profile	`/etc/security/pscexpert/bin/rmdotfrmpathnroot`
2.2.3	Limitar l'accés del sistema.	Afegeix la prestació de l'usuari root i el nom d'usuari al fitxer `/etc/ftpusers`.	`/etc/security/pscexpert/bin/chetcftpusers`
2.1	Eliminar el compte de convidat.	Elimina el compte de convidat i els fitxers que contingui.	`/etc/security/pscexpert/bin/execmds`
6.5.2	Evitar els programes d'inici a l'espai de contingut.	Habilita la funció d'inhabilitació d'execució de pila.	`/etc/security/pscexpert/bin/sedconfig`
8.2	Assegurar que la contrasenya per a l'arrel no sigui dèbil.	Inicia una comprovació d'integritat de contrasenya de root respecte de la contrasenya root, garantint d'aquesta forma una contrasenya de root potent.	`/etc/security/pscexpert/bin/chuserstanza`
PCI versió 2 8.5.15 **PCI versió 3** 8.1.8	Limitar l'accés al sistema establint el temps d'inactivitat de la sessió.	Estableix el límit del temps d'inactivitat en 15 minuts. Si la sessió està inactiva durant un període superior als 15 minuts, heu de tornar a escriure la contrasenya.	`/etc/security/pscexpert/bin/autologoff`
1.3.5	Limitar l'accés de trànsit a la informació del titular de targetes.	Estableix la regulació de trànsit del TCP en el paràmetre més elevat, forçant la mitigació de denegació de servei en ports.	`/etc/security/pscexpert/bin/tcptr_pscexpert`
1.3.5	Mantenir una connexió segura quan es migrin dades.	Habilita la creació de túnel de seguretat IP (IPSec) automatitzada entre els servidors d'E/S virtuals durant la migració de partició en directe.	`/etc/security/pscexpert/bin/cfgsecmig`
1.3.5	Limitar els paquets d'orígens desconeguts.	Permet els paquets de la consola de gestió de maquinari.	`/etc/security/pscexpert/bin/ipsecpermithostorport`
5.1.1	Mantenir el programari antivirus.	Conserva la integritat del sistema gràcies la detecció, l'eliminació i la protecció de tipus coneguts de programari malintencionat.	`/etc/security/pscexpert/bin/manageITsecurity`
PCI versió 2 Secció 7 **PCI versió 3** Secció 7	Mantenir l'accés actiu qual calgui.	Habilita el control d'accés basat en rols (RBAC) creant els rols d'usuari operador del sistema, administrador del sistema i */*oficial de seguretat del sistema amb els permisos necessaris.	`/etc/security/pscexpert/bin/EnableRbac`

Taula 6. Paràmetres relacionats amb les normatives de les versions 2.0 i 3.0 de conformitat amb la PCI DSS (continuació)

Implementa aquestes normatives PCI DSS	Especificació de la implementació	La implementació de l'AIX Security Expert	Ubicació de l'script que modifica el valor
PCI versió 2 No s'inclou al perfil de la versió 2, s'ha afegit a la versió 3. **PCI versió 3** 2.3	Implementar més les funcions de seguretat per als serveis, protocols o daemons necessaris que es consideren no segurs.	Utilitza tecnologies protegides com per exemple l'intèrpret d'ordres segur (SSH - Secure Shell), el protocol de transferència de fitxers de l'SSH (SSH File Transfer Protocol, S-FTP), Secure Sockets Layer (SSL) o la xarxa privada virtual de seguretat del protocol d'Internet (IPsec VPN) per protegir els serveis no segurs com per exemple NetBIOS, compartició de fitxers, Telnet i FTP. També configura el daemon de l'SSH per utilitzar només el protocol SSHv2.	`/etc/security/pscexpert/bin/sshPCIconfig`
PCI versió 2 No s'inclou al perfil de la versió 2, s'ha afegit a la versió 3. **PCI versió 3** 2.3	El client SSH s'ha de configurar perquè utilitzi només el protocol SSHv2.	Configura el client SSH perquè utilitzi el protocol SSHv2.	`/etc/security/pscexpert/bin/sshPCIconfig`
PCI versió 2 No s'inclou al perfil de la versió 2, s'ha afegit a la versió 3. **PCI versió 3** 2.3	El daemon SSH només ha d'escoltar en adreces de xarxa de gestió a menys que disposi d'autorització per a utilitzacions diferents de la gestió.	Garanteix que el daemon SSH es configuri només perquè romangui a l'escolta.	`/etc/security/pscexpert/bin/sshPCIconfig`
PCI versió 2 No s'inclou al perfil de la versió 2, s'ha afegit a la versió 3. **PCI versió 3** 2.3	El daemon SSH s'ha de configurar perquè utilitzi només el xifrat aprovat FIPS 140-2	Garanteix que el daemon SSH només utilitzi els xifrats FIPS 140-2.	`/etc/security/pscexpert/bin/sshPCIconfig`
PCI versió 2 No s'inclou al perfil de la versió 2, s'ha afegit a la versió 3. **PCI versió 3** 2.3	El daemon SSH s'ha de configurar perquè utilitzi només MAC (Message Authentication Codes) que fan servir algoritmes de hash criptogràfics compatibles amb FIPS 140-2.	Garanteix que els MAC executin els algoritmes aprovats.	`/etc/security/pscexpert/bin/sshPCIconfig`

Taula 6. Paràmetres relacionats amb les normatives de les versions 2.0 i 3.0 de conformitat amb la PCI DSS (continuació)

Implementa aquestes normatives PCI DSS	Especificació de la implementació	La implementació de l'AIX Security Expert	Ubicació de l'script que modifica el valor
PCI versió 2 No s'inclou al perfil de la versió 2, s'ha afegit a la versió 3. **PCI versió 3** 2.3	El daemon SSH ha de restringir la possibilitat d'inici de sessió a usuaris o grups específics.	Restringeix l'inici de sessió al sistema a usuaris i grups específics.	`/etc/security/pscexpert/bin/sshPCIconfig`
PCI versió 2 No s'inclou al perfil de la versió 2, s'ha afegit a la versió 3. **PCI versió 3** 2.3	El sistema ha de mostrar la data i l'hora del darrer inici de sessió correcte al compte després d'iniciar sessió.	Manté la informació des del darrer inici de sessió correcte i el mostra després de següent l'inici de sessió correcte.	`/etc/security/pscexpert/bin/sshPCIconfig`
PCI versió 2 No s'inclou al perfil de la versió 2, s'ha afegit a la versió 3. **PCI versió 3** 2.3	El daemon SSH ha de realitzar la comprovació de mode estricte dels fitxers de configuració del directori inicial.	Garanteix que els fitxers de configuració del directori inicial es defineixin en els modes correctes.	`/etc/security/pscexpert/bin/sshPCIconfig`
PCI versió 2 No s'inclou al perfil de la versió 2, s'ha afegit a la versió 3. **PCI versió 3** 2.3	El daemon SSH ha d'utilitzar la separació de privilegis.	Garanteix que el daemon SSH tingui la quantitat correcta de separació dels privilegis.	`/etc/security/pscexpert/bin/sshPCIconfig`
PCI versió 2 No s'inclou al perfil de la versió 2, s'ha afegit a la versió 3. **PCI versió 3** 2.3	El daemon SSH no ha de permetre que els rhost disposin d'autenticació RSA.	Inhabilita l'autenticació RSA dels rhosts quan s'utilitza el daemon SSH.	`/etc/security/pscexpert/bin/sshPCIconfig`
PCI versió 2 1.1.5 2.2.2 **PCI versió 3** 10.4	Examinar els estàndards i processos de configuració per verificar que s'implementi la tecnologia de sincronització horària i que es mantingui actualitzada pel que fa als requeriments de la versió 6.1. i 6.2 de PCI DSS.	Habilita el daemon ntp.	`/etc/security/pscexpert/bin/rctcpip`

Taula 6. Paràmetres relacionats amb les normatives de les versions 2.0 i 3.0 de conformitat amb la PCI DSS (continuació)

Implementa aquestes normatives PCI DSS	Especificació de la implementació	La implementació de l'AIX Security Expert	Ubicació de l'script que modifica el valor
PCI versió 2 No s'inclou al perfil de la versió 2, s'ha afegit a la versió 3. **PCI versió 3** 8.1.5	Inhabilitar un compte d'usuari quan no s'utilitzi.	Inhabilita els comptes després de 35 dies d'inactivitat.	`/etc/security/pscexpert/bin/disableacctpci`
PCI versió 3 2.2.3	Inhabilitar la versió 3 del Secure Sockets Layer (SSL) i la versió 1.0 del Transport Layer Security (TLS) en les aplicacions.	Inhabilita les versions 3 de l'SSL i 1.0 del TLS en la configuració del servidor Courier POP3 (Pop3d).	`/etc/security/pscexpert/bin/disableSSL`
PCI versió 3 2.2.3	Inhabilitar la versió 3 de l'SSL i la versió 1.0 del TLS en aplicacions.	Inhabilita la versió 3 de l'SSL i la versió 1.0 del TLS al servidor Courier IMAP (imapd).	`/etc/security/pscexpert/bin/disableSSL`
PCI versió 3 8.2.1	Inhabilitar la versió 3 de l'SSL i la versió 1.0 del TLS en aplicacions.	Comprova si la versió del fitxer de configuració del Network Time Protocol (NTP) és TLS 1.1 o si s'ha adoptat una mesura de seguretat posterior.	`/etc/security/pscexpert/bin/checkNTP`
PCI versió 3 2.2.3	Inhabilitar la versió 3 de l'SSL i la versió 1.0 del TLS en aplicacions.	Comprova si el fitxer de configuració del File Transfer Protocol Daemon (FTPD) és TLS 1.1, o si s'ha adoptat una mesura de seguretat posterior.	`/etc/security/pscexpert/bin/secureFTP`
PCI versió 3 2.2.3	Inhabilitar la versió 3 de l'SSL i la versió 1.0 del TLS en aplicacions.	Comprova si el fitxer de configuració del File Transfer Protocol (FTP) és TLS 1.1, o si s'ha adoptat una mesura de seguretat posterior.	`/etc/security/pscexpert/bin/secureFTP`
PCI versió 3 2.2.3	Inhabilitar la versió 3 de l'SSL i la versió 1.0 del TLS en aplicacions.	Inhabilita la versió 3 de l'SSL i la versió 1.0 del TLS en la configuració de sendmail.	`/etc/security/pscexpert/bin/sendmailPCIConfig`
PCI versió 3 2.2.3	Inhabilitar la versió 3 de l'SSL i la versió 1.0 del TLS en aplicacions.	Comprova si la versió de l'SSL a l'AIX és superior a 1.0.2.	`/etc/security/pscexpert/bin/sslversion`
PCI versió 3 8.2.1	Imposar dos factors d'autenticació.	Imposa dos factors d'autenticació com per exemple SHA-256 o SHA-512.	`/etc/security/pscexpert/bin/pwdalgchk`

Informació relacionada:

Normativa de seguretat de la informació en la indústria de mitjans de pagament

Conformitat amb la llei Sarbanes-Oxley i el COBIT

La llei Sarbanes-Oxley (SOX) de 2002 que es basa en el 107è congrés dels Estats Units d'Amèrica supervisa les auditories de les empreses públiques subjectes a normatives de seguretat i assumptes relacionats amb la finalitat de protegir els interessos dels inversors.

La secció 404 del SOX exigeix que es produeixi un assessorament en la gestió respecte dels controls interns. Per a la majoria d'organitzacions, els controls interns abarca els sistemes de tecnologia de la

informació, que processen i informen de les dades financeres de l'empresa. La llei SOX proporciona detalls específics sobre la TI i la seguretat de la TI. Molts auditors del SOX confien en estàndards com, per exemple, el COBIT com a mètode per mesurar i auditar el governament i el control de la TI. L'opció de configuració SOX/COBIT XML del PowerSC Standard Edition proporciona la configuració de seguretat dels sistemes AIX i servidor d'E/S virtual (VIOS necessària per complir les instruccions de conformitat del COBIT.

L'IBM Compliance Expert Express Edition s'executa en la versió següent del sistema operatiu AIX:

- AIX 6.1
- AIX 7.1
- AIX 7.2

La conformitat amb els estàndards externs és responsabilitat d'una càrrega de treball de l'administrador del sistema AIX. L'IBM Compliance Expert Express Edition s'ha dissenyat per simplificar la gestió dels paràmetres i informes del sistema operatiu necessaris pel compliment d'estàndards.

Els perfils de conformitat preconfigurats que se subministren amb l'IBM Compliance Expert Express Edition redueixen la càrrega de treball administrativa que implica la interpretació de la documentació de conformitat i la implementació d'aquests estàndards com a paràmetres específics de configuració del sistema.

Les prestacions de l'IBM Compliance Expert Express Edition s'ha dissenyat per ajudar els clients a gestionar de forma efectiva les necessitats del sistema, associades amb el compliment d'estàndards externs que suposadament redueixen costos mentre que en milloren la conformitat. Tots els estàndards de seguretat externs inclouen aspectes diferents als paràmetres de configuració del sistema. L'ús de l'IBM Compliance Expert Express Edition no pot garantir el compliment d'estàndards. El producte Compliance Expert s'ha dissenyat per simplificar la gestió dels paràmetres de configuració de sistemes de forma que ajuda els administradors a centrar-se en altres aspectes del compliment d'estàndards.

Informació relacionada:

Conformitat amb el COBIT

Llei de responsabilitat i portabilitat de l'assegurança mèdica (HIPAA)

La Llei de responsabilitat i portabilitat de l'assegurança mèdica (HIPAA) és un perfil de seguretat que se centra en la protecció la informació d'assegurances protegida electrònicament (EPHI).

La normativa de seguretat HIPAA se centra específicament en la protecció d'EPHI i només un conjunt d'agències està subjecte a aquesta normativa de seguretat HIPAA basada en les seves funcions i en l'ús de l'EPHI.

Totes les entitats HIPAA compreses, igual que algunes agències federals, han de complir la normativa de seguretat HIPAA.

La normativa de seguretat HIPAA se centra en la protecció de la confidencialitat, la integritat i la disponibilitat de l'EPHI, tal com es defineix a la normativa de seguretat.

L'EPHI que crea, rep, conserva o transmet una entitat coberta ha d'estar protegit contra les amenaces anticipades raonablement, els perills i els usos i divulgacions inadmissibles.

Els requisits, els estàndards i les especificacions d'implementació de la normativa de seguretat HIPAA s'apliquen a les següents entitats cobertes:

- Proveïdors sanitaris
- Plans de salut
- Agència distribuïdora d'informació mèdica

- Receptes mèdiques i patrocinadors de targetes de medicaments

A la taula següent es detallen les diverses seccions de la normativa de seguretat HIPAA i cada secció inclou diverses normatives i especificacions d'implementació.

Nota: Tots els fitxers d'scripts personalitzats que es proporcionen per mantenir la conformitat HIPAA es troben al directori `/etc/security/pscexpert/bin`.

Taula 7. Detalls sobre les normatives HIPAA i la seva implementació

Seccions de la normativa de seguretat HIPAA	**Especificació de la implementació**	**La implementació d'aixpert**	**Ordres i valors de retorn**
164.308 (a) (1) (ii) (D) 164.308 (a) (5) (ii) (C) 164.312 (b)	Implementa els procediments per revisar regularment els registres de l'activitat del sistema d'informació com, per exemple, registres d'auditoria, informes d'accés i informes d'incidents de seguretat.	Determina si s'ha habilitat l'auditoria al sistema.	**Ordre**: **#audit query**. **Valor de retorn**: si és correcte, aquesta ordre surt amb un valor de 0. Si no és correcte, l'ordre surt amb un valor d'1.
164.308 (a) (1) (ii) (D) 164.308 (a) (5) (ii) (C) 166.312 (b)	Implementa els procediments per revisar regularment els registres de l'activitat del sistema d'informació com, per exemple, registres d'auditoria, informes d'accés i informes d'incidents de seguretat.	Habilita l'auditoria al sistema. A més, configura els esdeveniments que s'han de capturar.	**Ordre**: **# audit start >/dev/null 2>&1**. **Valor de retorn**: si és correcte, aquesta ordre surt amb un valor de 0. Si no és correcte, l'ordre surt amb un valor d'1. Es realitza auditoria dels esdeveniments següents: **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)	Xifratges i desxifratge (A):Implementa un mecanisme per xifrar i desxifrar l'EPHI.	Determina si el sistema de fitxers encriptats (EFS) s'ha habilitat al sistema.	**Ordre**: **# efskeymgr -V >/dev/null 2>&1**. **Valor de retorn**: Si ja s'ha habilitat l'EFS, aquesta ordre existeix amb un valor de 0. Si l'EFS no s'ha habilitat, aquesta ordre existeix amb un valor d'1.
164.312 (a) (2) (iii)	Finalització de sessió automàtica (A): Implementa els procediments electrònics per finalitzar una sessió electrònica després d'un interval d'inactivitat predefinit.	Configura el sistema per finalitzar sessió des dels processos interactius passats 15 minuts d'inactivitat.	**Ordre**: **grep TMOUT= /etc/security /.profile > /dev/null 2>&1** **echo "TMOUT=900 ; TIMEOUT=900; export TMOUT TIMEOUT**. **Valor de retorn**: Si l'ordre no aconsegueix trobar el valor **TMOUT=15**, s'abandona l'script amb un valor d'1. Si no, se surt de l'ordre amb un valor de 0.

Taula 7. Detalls sobre les normatives HIPAA i la seva implementació (continuació)

Seccions de la normativa de seguretat HIPAA	Especificació de la implementació	La implementació d'aixpert	Ordres i valors de retorn
164.308 (a) (5) (ii) (D) 164.312 (a) (2) (i)	Gestió de contrasenyes (A):Implementa els procediments per crear, canviar i protegir contrasenyes.	Garanteix que totes les contrasenyes continguin, com a mínim 14 caràcters.	**Ordre**: **chsec -f /etc/security/user -s user -a minlen=8**. **Valor de retorn**: Si és correcte, s'abandona l'script amb un valor de 0. Si no és correcte, s'abandona l'script amb un codi d'error d'1.
164.308 (a) (5) (ii) (D) 164.312 (a) (2) (i)	Gestió de contrasenyes (A):Implementa els procediments per crear, canviar i protegir contrasenyes.	Garanteix que totes les contrasenyes incloguin com a mínim dos caràcters alfabètics, un dels quals ha de ser una majúscula.	**Ordre**: **chsec -f /etc/security/user -s user –a minalpha=4**. **Valor de retorn**: Si és correcte, s'abandona l'script amb un valor de 0. Si no és correcte, s'abandona l'ordre amb un codi d'error d'1.
164.308 (a) (5) (ii) (D) 164.312 (a) (2) (i)	Gestió de contrasenyes (A):Implementa els procediments per crear, canviar i protegir contrasenyes.	Especifica en 2 el número mínim de caràcters no alfabètics en una contrasenya.	**Ordre**: **#chsec –f /etc/security/user –s user –a minother=2**. **Valor de retorn**: Si és correcte, s'abandona l'script amb un valor de 0. Si no és correcte, s'abandona l'ordre amb un codi d'error d'1.
164.308 (a) (5) (ii) (D) 164.312 (a) (2) (i)	Gestió de contrasenyes (A):Implementa els procediments per crear, canviar i protegir contrasenyes.	Garanteix que cap contrasenya contingui caràcters repetitius.	**Ordre**: **#chsec –f /etc/security/user –s user –a maxrepeats=1**. **Valor de retorn**: Si és correcte, s'abandona l'script amb un valor de 0. Si no és correcte, s'abandona l'ordre amb un codi d'error d'1.
164.308 (a) (5) (ii) (D) 164.312 (a) (2) (i)	Gestió de contrasenyes (A):Implementa els procediments per crear, canviar i protegir contrasenyes.	Garanteix que no es torna a utilitzar una de les últimes cinc contrasenyes canviades.	**Ordre**: **#chsec –f /etc/security/user –s user –a histsize=5**. **Valor de retorn**: Si és correcte, s'abandona l'script amb un valor de 0. Si no és correcte, s'abandona l'ordre amb un codi d'error d'1.
164.308 (a) (5) (ii) (D) 164.312 (a) (2) (i)	Gestió de contrasenyes (A):Implementa els procediments per crear, canviar i protegir contrasenyes.	Especifica el número màxim de setmanes perquè sigui vàlida una contrasenya en 13 setmanes.	**Ordre**: **#chsec –f /etc/security/user –s user –a maxage=8**. **Valor de retorn**: Si és correcte, s'abandona l'script amb un valor de 0. Si no és correcte, s'abandona l'ordre amb un codi d'error d'1.
164.308 (a) (5) (ii) (D) 164.312 (a) (2) (i)	Gestió de contrasenyes (A):Implementa els procediments per crear, canviar i protegir contrasenyes.	Elimina el nombre mínim de requeriments de setmanes abans de canviar una contrasenya.	**Ordre**: **#chsec –f /etc/security/user –s user –a minage=2**. **Valor de retorn**: Si és correcte, s'abandona l'script amb un valor de 0. Si no és correcte, s'abandona l'ordre amb un codi d'error d'1.

Taula 7. Detalls sobre les normatives HIPAA i la seva implementació (continuació)

Seccions de la normativa de seguretat HIPAA	Especificació de la implementació	La implementació d'aixpert	Ordres i valors de retorn
164.308 (a) (5) (ii) (D) 164.312 (a) (2) (i)	Gestió de contrasenyes (A):Implementa els procediments per crear, canviar i protegir contrasenyes.	Especifica el nombre màxim de setmanes en 4 setmanes, per canviar una contrasenya caducada, després que hagi caducat el valor del paràmetre **maxage** establert per l'usuari.	**Ordre**: **#chsec –f /etc/security/user –s user –a maxexpired=4**. **Valor de retorn**: Si és correcte, s'abandona l'script amb un valor de 0. Si no és correcte, s'abandona l'ordre amb un codi d'error d'1.
164.308 (a) (5) (ii) (D) 164.312 (a) (2) (i)	Gestió de contrasenyes (A):Implementa els procediments per crear, canviar i protegir contrasenyes.	Especifica que el nombre mínim de caràcters que no es poden repetir de la contrasenya anterior és de 4 caràcters.	**Ordre**: **#chsec –f /etc/security/user –s user –a mindiff=4**. **Valor de retorn**: Si és correcte, s'abandona l'script amb un valor de 0. Si no és correcte, s'abandona l'ordre amb un codi d'error d'1.
164.308 (a) (5) (ii) (D) 164.312 (a) (2) (i)	Gestió de contrasenyes (A):Implementa els procediments per crear, canviar i protegir contrasenyes.	Especifica que 5 és el nombre de dies que s'esperarà abans que el sistema enviï un advertiment indicant que cal un canvi de contrasenya.	**Ordre**: **#chsec –f /etc/security/user –s user –a pwdwarntime = 5**. **Valor de retorn**: Si és correcte, s'abandona l'script amb un valor de 0. Si no és correcte, s'abandona l'ordre amb un codi d'error d'1.
164.308 (a) (5) (ii) (D) 164.312 (a) (2) (i)	Gestió de contrasenyes (A):Implementa els procediments per crear, canviar i protegir contrasenyes.	Verifica que les definicions d'usuari siguin correctes i arregla els errors.	**Ordre**: **/usr/bin/usrck -y ALL** **/usr/bin/usrck –n ALL**. **Valor de retorn**: L'ordre no torna cap valor. L'ordre comprova i corregeix els errors, si n'hi ha.
164.308 (a) (5) (ii) (D) 164.312 (a) (2) (i)	Gestió de contrasenyes (A):Implementa els procediments per crear, canviar i protegir contrasenyes.	Bloqueja el compte després de tres intents d'inici de sessió fallits consecutius.	**Ordre**: **#chsec –f /etc/security/user –s user –a loginretries=3**. **Valor de retorn**: Si és correcte, s'abandona l'script amb un valor de 0. Si no és correcte, s'abandona l'ordre amb un codi d'error d'1.
164.308 (a) (5) (ii) (D) 164.312 (a) (2) (i)	Gestió de contrasenyes (A):Implementa els procediments per crear, canviar i protegir contrasenyes.	Especifica el retard entre un inici de sessió no satisfactori i el següent en 5 segons.	**Ordre**: **chsec -f /etc/security/login.cfg -s default -a logindelay=5**. **Valor de retorn**: Si és correcte, s'abandona l'script amb un valor de 0. Si no és correcte, s'abandona l'ordre amb un codi d'error d'1.
164.308 (a) (5) (ii) (D) 164.312 (a) (2) (i)	Gestió de contrasenyes (A):Implementa els procediments per crear, canviar i protegir contrasenyes.	Especifica en 10 el nombre d'intents d'inici de sessió no satisfactoris en un port, abans que el port es bloquegi.	**Ordre**: **chsec -f /etc/security/lastlog -s username -a \ unsuccessful_login_count=10**. **Valor de retorn**: Si és correcte, s'abandona l'script amb un valor de 0. Si no és correcte, s'abandona l'ordre amb un codi d'error d'1.

Taula 7. Detalls sobre les normatives HIPAA i la seva implementació (continuació)

Seccions de la normativa de seguretat HIPAA	Especificació de la implementació	La implementació d'aixpert	Ordres i valors de retorn
164.308 (a) (5) (ii) (D) 164.312 (a) (2) (i)	Gestió de contrasenyes (A):Implementa els procediments per crear, canviar i protegir contrasenyes.	Especifica en 60 segons l'interval de temps en un port pels intents d'inici de sessió satisfactoris abans que s'inhabiliti el port.	**Ordre**: **#chsec -f /etc/security/lastlog -s user –a time_last_unsuccessful_ login=60**. **Valor de retorn**: Si és correcte, s'abandona l'script amb un valor de 0. Si no és correcte, s'abandona l'ordre amb un codi d'error d'1.
164.308 (a) (5) (ii) (D) 164.312 (a) (2) (i)	Gestió de contrasenyes (A):Implementa els procediments per crear, canviar i protegir contrasenyes.	Especifica en 30 minuts l'interval de temps després del qual es desbloqueja un port i després d'haver-lo inhabilitat.	**Ordre**: **#chsec -f /etc/security/login.cfg -s default -a loginreenable = 30**. **Valor de retorn**: Si és correcte, s'abandona l'script amb un valor de 0. Si no és correcte, s'abandona l'ordre amb un codi d'error d'1.
164.308 (a) (5) (ii) (D) 164.312 (a) (2) (i)	Gestió de contrasenyes (A):Implementa els procediments per crear, canviar i protegir contrasenyes.	Especifica en 30 segons l'interval de temps per escriure una contrasenya.	**Ordre**: **chsec -f /etc/security/login.cfg -s usw -a logintimeout=30**. **Valor de retorn**: Si és correcte, s'abandona l'script amb un valor de 0. Si no és correcte, s'abandona l'ordre amb un codi d'error d'1.
164.308 (a) (5) (ii) (D) 164.312 (a) (2) (i)	Gestió de contrasenyes (A):Implementa els procediments per crear, canviar i protegir contrasenyes.	Garanteix que els comptes es bloquegin passats 35 dies d'inactivitat.	**Ordre**: **grep TMOUT= /etc/security /.profile > /dev/null 2>&1if TMOUT = (35x24x60x60){#chsec -f /etc/security/user -s user -aaccount_locked = true}**. **Valor de retorn**: Si falla l'ordre a l'hora d'establir el valor de **account_locked** en **true**, s'abandona l'script amb un valor d'1. Si no, s'abandona l'ordre amb un valor de 0.
164.312 (c) (1)	Implementa les polítiques i els procediments per protegir l'EPHI de l'alteració o destrucció incorrecta.	Estableix les polítiques d'execució fiable (TE) en ON (activat).	**Ordre**: Activa **CHKEXEC, CHKSHLIB, CHKSCRIPT, CHKKERNEXT, STOP_ON_CHKFAIL,TE=ON Per exemple, trustchk –p TE=ON CHKEXEC = ON, CHKSHLIB,=ON, CHKSCRIPT=ON, CHKKERNEXT = ON**. **Valor de retorn**: Si es produeix un error, s'abandona l'script amb un valor d'1.
164.312 (e) (1)	Implementa les mesures de seguretat tècniques per evitar l'accés no autoritzat a l'EPHI que s'està transmetent a través d'una xarxa de comunicació electrònica.	Determina si els conjunts de fitxers **ssh** s'han instal•lat. En cas negatiu, apareix un missatge d'error.	**Ordre**: **# lslpp –l | grep openssh > /dev/null 2>&1**. **Valor de retorn**: Si el codi de retorn per aquesta ordre és de 0, s'abandona l'script amb un valor de 0. Si els conjunts de fitxers SSH no s'han instal•lat, s'abandona l'script amb un valor d'1 i es mostra el missatge d'error `Instal•la els conjunts de fitxers SSH per a la transmissió segura`.

A la taula següent es detallen les diverses funcions de la normativa de seguretat HIPAA i cada funció inclou diverses normatives i especificacions d'implementació.

Taula 8. Detalls sobre les funcions de l'HIPAA i la seva implementació

Funcions de l'HIPAA	Especificació de la implementació	La implementació d'aixpert	Ordres i valors de retorn
Enregistrament d'errors	Consolida els errors procedents de diferents registres i envia correus electrònics a l'administrador.	Determina si hi ha errors de maquinari. Determina si hi ha errors no recuperables procedents del fitxer **trcfile** en la ubicació `/var/adm/ras/trcfile`. Envia els errors a **arrel@<nom_amfitrió>**.	**Ordre**: **errpt -d H**. **Valor de retorn**: si és correcte, aquesta ordre surt amb un valor de 0. Si no és correcte, l'ordre surt amb un valor d'1.
Habilitació d'FPM	Canvia els permisos dels fitxers.	Canvia el permís dels fitxers d'una llista de permisos i fitxers utilitzant l'ordre **fpm**.	**Ordre**: **# fpm -1 <level> -f <fitxer d'ordres>**. **Valor de retorn**: si és correcte, aquesta ordre surt amb un valor de 0. Si no és correcte, l'ordre surt amb un valor d'1.
Habilitació de RBAC	Crea usuaris **isso**, **so** i **sa** i els assigna els rols corresponents.	Suggereix que creeu els usuaris **isso**, **so** i **sa**. Assigna els rols adients als usuaris.	**Ordre**: **/etc/security/pscexpert/bin/RbacEnablement**.

Informació relacionada:

Llei de responsabilitat i portabilitat de l'assegurança mèdica (HIPAA)

Conformitat amb la North American Electric Reliability Corporation

La North American Electric Reliability Corporation (NERC) és una corporació sense ànim de lucre que desenvolupa normatives per al sector de sistemes elèctrics. El PowerSC Standard Edition conté el perfil preconfigurat de la NERC que proporciona les normatives de seguretat que podeu utilitzar per protegir els sistemes elèctric amb risc.

El perfil NERC compleix la normativa de la Critical Infrastructure Protection (CIP).

El perfil NERC es troba a `/etc/security/aixpert/custom/NERC.xml`. Podeu restablir els requeriments de CIP que s'apliquen al perfil de la NERC a l'estat per defecte aplicant el perfil NERC_to_AIXDefault.xml que es troba al directori `/etc/security/aixpert/custom`. Aquest procés no és el mateix que el de desfer una operació del perfil NERC.

A la taula següent es proporciona informació sobre les normatives de la CIP que s'apliquen al sistema operatiu AIX i sobre la manera en que el PowerSC Standard Edition gestiona la normativa de la CIP:

Taula 9. Normatives de la CIP per al producte PowerSC Standard Edition

Normativa de la CIP	Implementació de l'AIX Security Expert	Ubicació de l'script que modifica el valor
CIP-003-3 R5.1	Configura els paràmetres de seguretat del sistema per evitar problemes eliminant els atributs SUID (Set-User Identification) i SGID (Set-Group Identification) dels fitxers binaris.	• `/etc/security/pscexpert/bin/filepermgr` • `/etc/security/pscexpert/bin/rmsuidfrmrcmds`

Taula 9. Normatives de la CIP per al producte PowerSC Standard Edition (continuació)

Normativa de la CIP	Implementació de l'AIX Security Expert	Ubicació de l'script que modifica el valor
CIP-003-3 R5.1.1	Habilita el control d'accés basat en rols (RBAC) creant els rols d'usuari operador del sistema, administrador del sistema i */*oficial de seguretat del sistema amb els permisos necessaris.	`/etc/security/pscexpert/bin/EnableRbac`
CIP-005-3a R2.1-R2.4	Habilita l'intèrpret d'ordres segur (SSH - Secure Shell) per a accés de seguretat.	`/etc/security/pscexpert/bin/sshstart`
CIP-005-3a R2.5 CIP-007-5 R1.1	Inhabilita els serveis innecessaris i no segurs següents: • Daemon **lpd** • Entorn d'escriptori comú (CDE - Common Desktop Environment)	`/etc/security/pscexpert/bin/comntrows`
CIP-005-3a R2.5 CIP-007-5 R1.1	Inhabilita els serveis innecessaris i no segurs següents: • Daemon **timed** • Daemon **NTP** • Daemon **rwhod** • Daemon **DPID2** • Agent DHCP	`/etc/security/pscexpert/bin/rctcpip`

Taula 9. Normatives de la CIP per al producte PowerSC Standard Edition (continuació)

Normativa de la CIP	Implementació de l'AIX Security Expert	Ubicació de l'script que modifica el valor
CIP-005-3a R2.5 CIP-007-5 R1.1	Inhabilita els serveis innecessaris i no segurs següents: • Daemon **comsat** • Daemon **dtspcd** • Daemon **fingerd** • Daemon **ftpd** • Daemon **rshd** • Daemon **rlogind** • Daemon **rexecd** • Daemon **systat** • Daemon **tfptd** • Daemon **talkd** • Daemon **rquotad** • Daemon **rstatd** • Daemon **rusersd** • Daemon **rwalld** • Daemon **sprayd** • Daemon **pcnfsd** • Daemon **telnet** • Servei cmsd • Servei ttdbserver • Servei TCP echo • Servei TCP discard • Servei TCP chargen • Servei TCP daytime • Servei TCP time • Servei UDP echo • Servei UDP discard • Servei UDP chargen • Servei UDP daytime • Servei UDP time	`/etc/security/pscexpert/bin/cominetdconf`
CIP-005-3a R2.5 CIP-007-5 R1.1	Aplica la de denegació de la sol•licitud de servei pels ports de mitigació.	`/etc/security/pscexpert/bin/tcptr_aixpert`
CIP-005-3a R3 CIP-007-3a R5, R6.5 CIP-007-5 R4.4	Habilita l'auditoria dels fitxers binaris al sistema.	`/etc/security/pscexpert/bin/pciaudit`
CIP-007-3a R3 CIP-007-5 R2.1	Mostra un missatge per habilitar Trusted Network Connect (TNC).	`/etc/security/pscexpert/bin/GeneralMsg`
CIP-007-3a R4 CIP-007-5 R3.3	Conserva la integritat del sistema gràcies la detecció, l'eliminació i la protecció de tipus coneguts de programari malintencionat.	`/etc/security/pscexpert/bin/manageITsecurity`
CIP-007-3a R5.2.1	Permet canviar la contrasenya la primera vegada que s'inicia sessió per a tots els comptes d'usuaris per defecte que no estiguin bloquejats.	`/etc/security/pscexpert/bin/pwdchg`
CIP-007-3a R5.2.2-R5.2.3	Bloqueja tots els comptes d'usuari per defecte.	`/etc/security/pscexpert/dodv2/lockacc_rlogin`

Taula 9. Normatives de la CIP per al producte PowerSC Standard Edition (continuació)

Normativa de la CIP	Implementació de l'AIX Security Expert	Ubicació de l'script que modifica el valor
CIP-007-3a R5.3.1	Defineix cada contrasenya en un mínim de 6 caràcters.	`/etc/security/pscexpert/bin/chusrattr`
CIP-007-5 R5.5.1	Defineix cada contrasenya en un mínim de 8 caràcters.	`/etc/security/pscexpert/bin/chusrattr`
CIP-007-3a R5.3.2 CIP-007-5 R5.5.2	Defineix cada contrasenya en una combinació de caràcters alfabètics, numèrics i especials.	`/etc/security/pscexpert/bin/chusrattr`
CIP-007-3a R5.3.3 CIP-007-5 R5.6	Canvia cada contrasenya anualment.	`/etc/security/pscexpert/bin/chusrattr`
CIP-007-3a R7	Mostra un missatge per habilitar el sistema de fitxers encriptats (EFS).	`/etc/security/pscexpert/bin/GeneralMsg`
CIP-007-5 R5.7	Limita el nombre d'intents d'autenticació incorrectes.	`/etc/security/pscexpert/bin/chusrattr`
CIP-010-1 CIP-010-2 R2.1	Mostra un missatge per habilitar Real Time Compliance (RTC).	`/etc/security/pscexpert/bin/GeneralMsg`

Informació relacionada:

Conformitat amb la North American Electric Reliability Corporation

Gestió de l'automatització de la seguretat i de la conformitat

Informació sobre el procés de planificació i desplegament dels perfils d'automatització de seguretat i de conformitat del PowerSC en un grup de sistemes segons els procediments acceptats de conformitat i de governament de TI.

Com a part del governament de sistema i de TI, els sistemes que executin una càrrega de treball similar i classes de seguretat de dades similars s-han de gestionar i configurar de forma coherent. Per planificar i desplegar el nivell de conformitat en els sistemes, dueu a terme les tasques següents:

Identificació dels grups de treball del sistema

Les instruccions de governament de conformitat i TI indiquen que els sistemes que executin un càrrega de treball similar i classes de seguretat de dades han de gestionar-se i configurar-se de forma coherent. Per tant, heu d'identificar tots es sistemes en un grup de treball similar.

Utilització d'un sistema de proves de no producció per a la configuració inicial

Apliqueu el perfil de conformitat corresponent del PowerSC al sistema de proves.

Tingueu en compte els exemples següents per aplicar els perfils de conformitat al sistema operatiu AIX.

Exemple 1: Aplicació del fitxer `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
```

en aquest exemple, no hi ha cap regla que falli, és a dir, `Failedrules=0`. Això significa que totes les regles s'han aplicat correctament i que es pot iniciar la fase de proves. Si hi ha errors, es genera una sortida detallada.

Exemple 2: Aplicació del fitxer PCI.xml amb un error

```
# 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
```

Cal resoldre l'error de la regla pci_grpck. Entre les causes possibles de l'error trobem els motius següents:

- La regla no s'aplica a l'entorn i s'ha d'eliminar.
- Hi ha un problema al sistema que cal corregir.

Investigació d'una regla que ha fallat

En la majoria de casos, no es produeix cap error quan s'aplica un perfil de seguretat i conformitat del PowerSC. Això no obstant, pot ser que al sistema li faltin prerequisits relacionats amb la instal•lació o que tingui altres problemes que requereixin l'atenció per part de l'administrador.

La causa de l'error es pot investigar utilitzant l'exemple següent:

Consulteu el fitxer /etc/security/aixpert/custom/PCI.xml i localitzeu la regal que falla. En aquest exemple, la regla és pci_grpck. Executeu l'ordre **fgrep**, busqueu la regla que falla pci_grpck i consulteu la regla XML associada.

```
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
```

Des de la regla pci_grpck, es pot consultar l'ordre /usr/sbin/grpck.

Actualització de la regla que ha fallat

Quan s'aplica un perfil de seguretat i de conformitat del PowerSC, podeu detectar errors.

Pot ser que al sistema li faltin prerequisits d'instal•lació o que tingui altres problemes que requereixin l'atenció per part de l'administrador. Després de determinar l'ordre subjacent de la regla que ha fallat, examineu el sistema per comprendre l'ordre de configuració que està fallant. El sistema pot tenir un problema de seguretat. També pot donar-se el cas que una regla en particular no s'apliqui a l'entorn del sistema. A continuació, caldrà crear un perfil de seguretat.

Creació d'un perfil de configuració de seguretat personalitzada

Si no es pot aplicar cap regla a l'entorn específic del sistema, la majoria d'organitzacions de conformitat permeten excepcions documentades.

Per eliminar una regla i crear un fitxer de conjuració i de polítiques de seguretat personalitzat, seguiu aquests passos:

1. Copieu el contingut dels següents fitxers en un únic fitxer anomenat /etc/security/aixpert/custom/<*la_meva_política_seguretat*>.xml:

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

2. Editeu el fitxer <*la_meva_política_seguretat*>.xml traient la regla que no s'aplica del codi XML d'obertura <AIXPertEntry name... i posant-la al codi XML d'acabament </AIXPertEntry.

Podeu inserir les regles de configuració addicionals per obtenir seguretat. Inseriu les regles addicionals a l'esquema XML AIXPertSecurityHardening. No podeu canviar els perfils del PowerSC directament però podeu personalitzar els perfils.

Per a la majoria d'entorns, heu de crear una política XML personalitzada. Per distribuir un perfil personalitzat a altres sistemes, heu de copiar de forma segura la política XML personalitzada al sistema que requereix la mateixa configuració. S'utilitza un protocol segur com, per exemple, el protocol de transferència de fitxers segura (SFTP) per distribuir una política XML personalitzada a altres sistemes i el perfil s'emmagatzema en una ubicació segura /etc/security/aixpert/custom/ <*la_meva_política_seguretat.xml*>/etc/security/aixpert/custom/

Inicieu sessió al sistema on s'ha de crear un perfil personalitzat i executeu l'ordre següent:

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

Comprovació de les aplicacions amb l'AIX Profile Manager

Les configuracions de seguretat poden afectar a les aplicacions i la forma en què s'accedeix i es gestiona el sistema. És important comprovar les aplicacions i els mètodes de gestió esperats del sistema abans de desplegar el sistema en un entorn de producció.

Els estàndards de conformitat reguladors imposen una configuració de seguretat que és més estricta que una configuració a punt de fer servir. Per comprovar el sistema, seguiu aquests passos:

1. Seleccioneu **Visualitza i gestiona perfils** del panell de la dreta de la pàgina de benvinguda de l'AIX Profile Manager.
2. Seleccioneu el perfil que ha utilitzat la plantilla per desplegar-lo als sistemes que cal supervisar.
3. Feu clic a **Compara**.
4. Seleccioneu el grup gestionat o seleccioneu sistemes individuals dins el grup i feu clic a **Afegeix** per afegir-los al requadre seleccionat.
5. Feu clic a **D'acord**.

S'inicia l'operació de comparació.

Supervisió de sistemes per a aconseguir una conformitat continuada amb l'AIX Profile Manager

Les configuracions de seguretat poden afectar a les aplicacions i la forma en què s'accedeix i es gestiona el sistema. És important supervisar les aplicacions i els mètodes de gestió esperats del sistema a l'hora de desplegar el sistema en un entorn de producció.

Per utilitzar l'AIX Profile Manager amb la finalitat de supervisar un sistema AIX, seguiu aquests passos:

1. Seleccioneu **Visualitza i gestiona perfils** del panell de la dreta de la pàgina de benvinguda de l'AIX Profile Manager.
2. Seleccioneu el perfil que ha utilitzat la plantilla per desplegar-lo als sistemes que cal supervisar.
3. Feu clic a **Compara**.
4. Seleccioneu un grup gestionat o seleccioneu sistemes individuals dins el grup i afegiu-los al requadre seleccionat.
5. Feu clic a **D'acord**.

S'inicia l'operació de comparació.

Configuració de l'automatització de la seguretat i de la conformitat del PowerSC

Informació sobre el procediment per configurar el PowerSC pel que fa a l'automatització de la seguretat i a de la conformitat des de la línia d'ordres i utilitzant l'AIX Profile Manager.

Configuració dels paràmetres de les opcions de conformitat del PowerSC

Informació sobre els aspectes bàsics de seguretat del PowerSC així com de la funció d'automatització de conformitat, de la prova de configuració en sistemes de prova de no producció i de la planificació i el desplegament dels paràmetres. Quan s'aplica una configuració de conformitat, els paràmetres canvien diversos paràmetres de configuració al sistema operatiu.

Nota: Algunes normatives de conformitat i certs perfils inhabiliten Telnet perquè Telnet utilitza contrasenyes de text simple. Per tant, heu de tenir instal•lat, configurat i en funcionament l'Open SSH. Podeu utilitzar qualsevol altre mitjà de comunicació segur amb el sistema que s'està configurant. Aquestes normatives de conformitat requereixen que l'inici de sessió com a `root` estigui inhabilitat. Configureu un usuari no root, o més d'un, abans de continuar aplicant canvis de configuració. Aquesta configuració no inhabilita l'arrel i podeu iniciar sessió com a usuari no root i executar l'ordre **su** a l'arrel. Proveu si podeu establir la connexió SSH al sistema, inicieu sessió com a usuari no root i executeu l'ordre a l'`arrel`.

Per accedir als perfils de configuració DoD, PCI, SOX o COBIT, utilitzeu el directori següent:

- Els perfils del sistema operatiu AIX es troben al directori `/etc/security/aixpert/custom`.
- Els perfils del servidor d'E/S virtual (VIOS) es troben al directori `/etc/security/aixpert/core`.

Configuració de la conformitat del PowerSC des de la línia d'ordres

Implementeu o comproveu el perfil de conformitat utilitzant l'ordre **pscxpert** al sistema AIX i l'ordre **viosecure** al servidor d'E/S virtual (VIOS).

Per aplicar els perfils de conformitat del PowerSC en un sistema AIX, escriviu una de les ordres següents, que depèn del nivell de conformitat de seguretat que vulgueu aplicar.

Taula 10. Ordres del PowerSC per a l'AIX

Ordre	Estàndard de conformitat
% pscxpert -f /etc/security/aixpert/custom/DoD.xml	*Guia per a la implementació tècnica de seguretat de l'UNIX del departament de defensa dels Estats Units*
% pscxpert -f /etc/security/aixpert/custom/Hipaa.xml	*Llei de responsabilitat i portabilitat de l'assegurança mèdica*
% pscxpert -f /etc/security/aixpert/custom/PCI.xml	*Normativa de seguretat de la informació en la indústria de mitjans de pagament*
% pscxpert -f /etc/security/aixpert/custom/SOX-COBIT.xml	*Sarbanes-Oxley Act of 2002 – COBIT IT Governance*

Per aplicar els perfils de conformitat del PowerSC en un sistema VIOS, escriviu una de les ordres següents per al nivell de conformitat de seguretat que vulgueu aplicar.

Taula 11. Ordres del PowerSC per al servidor d'E/S virtual

Ordre	Estàndard de conformitat
% viosecure -file /etc/security/aixpert/custom/DoD.xml	*Guia per a la implementació tècnica de seguretat de l'UNIX del departament de defensa dels Estats Units*
% viosecure -file /etc/security/aixpert/custom/Hipaa.xml	*Llei de responsabilitat i portabilitat de l'assegurança mèdica*
% viosecure -file /etc/security/aixpert/custom/PCI.xml	*Normativa de seguretat de la informació en la indústria de mitjans de pagament*
% viosecure -file /etc/security/aixpert/custom/SOX-COBIT.xml	*Sarbanes-Oxley Act of 2002 – COBIT IT Governance*

L'ordre **pscxpert** del sistema AIX i l'ordre **viosecure** del VIOS poden trigar en executar-se perquè comproven o defineixen tot el sistema i duen a terme canvis de configuració relacionats amb la seguretat. La sortida és similar a l'exemple següent:

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

Això no obstant, algunes regles fallen en funció de l'entorn de l'AIX, del conjunt d'instal•lació i de la configuració anterior.

Per exemple, una regla de prerequisit pot fallar perquè el sistema no disposa del conjunt de fiters d'instal•lació necessaris. Cal comprendre cadascun dels errors per resoldre'ls abans de desplegar els perfils de conformitat mitjançant el centre de dades.

Conceptes relacionats:

"Gestió de l'automatització de la seguretat i de la conformitat" a la pàgina 106
Informació sobre el procés de planificació i desplegament dels perfils d'automatització de seguretat i de conformitat del PowerSC en un grup de sistemes segons els procediments acceptats de conformitat i de governament de TI.

Configuració de la conformitat del PowerSC amb l'AIX Profile Manager

Informació sobre el procediment per configurar els perfils de seguretat i de conformitat del PowerSC i per desplegar la configuració en un sistema gestionat AIX utilitzant l'AIX Profile Manager.

Per configurar els perfils de seguretat i de conformitat del PowerSC mitjançant l'AIX Profile Manager, seguiu aquests passos:

1. Inicieu sessió a l'IBM Systems Director i seleccioneu l'AIX Profile Manager.
2. Creeu una plantilla que es basi en un dels perfils de seguretat i conformitat del PowerSC duent a terme aquests passos:
   a. Feu clic a **Visualitza i gestiona plantilles** del panell de la dreta de la pàgina de benvinguda de l'AIX Profile Manager.
   b. Feu clic a **Crea**.
   c. Feu clic a **Sistema operatiu** des de la llista **Tipus de plantilla**.
   d. Proporcioneu un nom a la plantilla al camp **Nom de la plantilla de configuració**.
   e. Feu clic a **Continua** > **Desa**.
3. Seleccioneu el perfil que s'utilitzarà amb la plantilla seleccionant **Examina** a l'opció **Selecciona quin perfil s'ha d'utilitzar per aquesta plantilla**. Els perfils mostren els elements següents:
   - `ice_DLS.xml` és el nivell de seguretat per defecte del sistema operatiu AIX.
   - `ice_DoD.xml` són els paràmetres del departament de seguretat de defensa i la guia d'implementació per a l'UNIX.
   - `ice_HLS.xml` són els paràmetres de la seguretat genèrica de nivell elevat per a l'AIX.
   - `ice_LLS.xml` són els paràmetres de la seguretat de baix nivell per a l'AIX.
   - `ice_MLS.xml` són els paràmetres de la seguretat de nivell mitjà per a l'AIX.

- `ice_PCI.xml` és el paràmetre de la industria de targetes de pagament (Payment Card Industry) per al sistema operatiu AIX.
- `ice_SOX.xml` són els paràmetres de SOX o COBIT per al sistema operatiu AIX.

4. Elimineu els perfils del requadre seleccionat.
5. Seleccioneu **Afegeix** per moure el perfil necessari al requadre seleccionat.
6. Feu clic a **Desa**.

Per desplegar la configuració en un sistema gestionat AIX, seguiu aquests passos:

1. Seleccioneu **Visualitza i gestiona plantilles** del panell de la dreta de la pàgina de benvinguda de l'AIX Profile Manager.
2. Seleccioneu la plantilla que calgui desplegar.
3. Feu clic a **Desplega**.
4. Seleccioneu els sistemes dels que se n'hagi de desplegar el perfil i feu clic a **Afegeix** per moure el perfil necessari al requadre seleccionat.
5. Feu clic a **D'acord** per desplegar la plantilla de configuració. El sistema es configura en funció de la plantilla seleccionada del perfil.

Perquè el desplegament sigui satisfactori per a DoD, PCI o SOX, cal haver instal•lat el PowerSC Standard Edition al punt final del sistema AIX. Si el sistema que s'està desplegant no té instal•lat el PowerSC, el desplegament fallarà. L'IBM Systems Director desplega la plantilla de configuració als punts finals seleccionats del sistema AIX i els configura segons els requisits de conformitat.

Informació relacionada:

AIX Profile Manager

IBM Systems Director

PowerSC Real Time Compliance

La funció del PowerSC Real Time Compliance supervisa constantment els sistemes AIX habilitats per garantir que s'hagin configurat de forma coherent i segura.

La funció del PowerSC Real Time Compliance funciona amb les polítiques Automatització de conformitat del PowerSC i AIX Security Expert per oferir una notificació quan es produeixin violacions de conformitat o quan es canviï un fitxer supervisat. Quan es viola la política de configuració de seguretat d'un sistema, la funció del PowerSC Real Time Compliance envia un correu electrònic o un missatge de text per avisar l'administrador del sistema.

La funció del PowerSC Real Time Compliance és una funció de seguretat passiva que admet perfils de conformitat predefinits o modificats entre el quals hi trobem: Department of Defense Security Technical Implementation Guide (guia per a la implementació tècnica de seguretat del departament de defensa), la Payment Card Industry Data Security Standard (normativa de seguretat de la informació en la indústria de mitjans de pagament, la llei Sarbanes-Oxley i el COBIT. Es proporciona una llista per defecte dels fitxers per supervisar-ne els canvis però podeu afegir fitxers a la llista.

Instal•lació del PowerSC Real Time Compliance

La funció del PowerSC Real Time Compliance s'instal•la amb la versió 1.1.4, o posterior, del PowerSC Standard Edition i no forma part del sistema operatiu AIX bàsic.

Per instal•lar el PowerSC Standard Edition, seguiu aquests passos:

1. Assegureu-vos que esteu executant un dels sistemes operatius AIX següents als sistema on s'instal•la la funció del PowerSC Standard Edition:
   - IBM AIX 6 amb el nivell tecnològic 7, o posterior, amb AIX Event Infrastructure for AIX i AIX Clusters (bos.ahafs 6.1.7.0), o posterior
   - IBM AIX 7 amb el nivell tecnològic 1, o posterior, amb AIX Event Infrastructure for AIX i AIX Clusters (bos.ahafs 7.1.1.0), o posterior
   - AIX versió 7.2, o posterior, amb AIX Event Infrastructure for AIX i AIX Clusters (bos.ahafs 7.2.0.0), o posterior
2. Per actualitzar o instal•lar el conjunt de fitxers de funcions del PowerSC Standard Edition, instal•leu el conjunt de fitxers `powerscStd.rtc` des del paquet d'instal•lació de la versió 1.1.4, o posterior, del PowerSC Standard Edition.

Configuració del PowerSC Real Time Compliance

Podeu configurar el PowerSC Real Time Compliance per enviar alertes quan es produeixen violacions d'un perfil de conformitat o canvi en un fitxer supervisat. Entre els exemples dels perfils hi trobem: Department of Defense Security Technical Implementation Guide (guia per a la implementació tècnica de seguretat del departament de defensa), la Payment Card Industry Data Security Standard (normativa de seguretat de la informació en la indústria de mitjans de pagament, la llei Sarbanes-Oxley i el COBIT.

Podeu configurar el PowerSC Real Time Compliance mitjançant un dels mètodes següents:

- Escriviu l'ordre **mkrtc**.
- Executeu l'eina SMIT escrivint l'ordre següent:

  ```
  smit RTC
  ```

Identificació dels fitxers supervisats mitjançant la funció del PowerSC Real Time Compliance

La funció del PowerSC Real Time Compliance supervisa els canvis d'una llista per defecte de fitxers des dels paràmetres de seguretat d'alt nivell, que es poden personalitzar afegint o eliminant fitxers d'una llista de fitxers al fitxer `/etc/security/rtc/rtcd_policy.conf`.

Hi ha dos mètodes d'identificar la plantilla de conformitat que s'aplica en un sistema. Un mètode és utilitzar l'ordre **pscxpert** i l'altre és utilitzar l'AIX Profile Manager amb l'IBM Systems Director.

Quan s'identifica el perfil de conformitat, es poden afegir més fitxers a la llista de fitxers que cal supervisar incloent els fitxers addicionals al fitxer `/etc/security/rtc/rtcd_policy.conf`. Després de desar el fitxer, s'utilitza immediatament la llista nova com a línia base i se'n supervisen els canvis sense reiniciar el sistema.

Definició d'alertes per al PowerSC Real Time Compliance

Heu de configurar la notificació de la funció del PowerSC Real Time Compliance indicant el tipus de les alertes i els destinataris de les alertes.

El daemon rtcd, que és el component principal de la funció del PowerSC Real Time Compliance, obté la informació sobre els tipus d'alertes i els destinataris del fitxer de configuració `/etc/security/rtc/rtcd.conf`. Podeu editar aquest fitxer per actualitzar-ne la informació utilitzant un editor de text.

Informació relacionada:

Format de fitxer /etc/security/rtc/rtcd.conf per a la conformitat en temps real

Engegada fiable

La funció d'engegada fiable utilitza mòdul de plataforma fiable virtual (VTPM), que és una instància virtual de TPM de Trusted Computing Group. El VTPM s'utilitza per emmagatzemar de forma segura mesures de l'engegada del sistema per a una futura verificació.

Conceptes de l'engegada fiable

És important entendre la integritat del procés d'engegada i com classificar l'engegada segons sigui una engegada fiable o no fiable.

Podeu configurar un màxim de 60 particions lògiques habilitades per a VTPM (LPAR) per a cada sistema físic utilitzant la consola de gestió de maquinari (HMC). Si s'ha configurat, el VTPM és exclusiu per a cada LPAR. Quan es fa servir amb la tecnologia Execució fiable (Trusted Execution) de l'AIX, el VTPM proporciona protecció i seguretat en les particions següents:

- La imatge d'engegada al disc
- El sistema operatiu sencer
- Les capes de l'aplicació

Un administrador por veure sistemes fiables i no fiables des d'una consola central que estigui instal•lada amb el verificador **openpts**, que hi ha disponible al paquet d'expansió de l'AIX. La consola **openpts** gestiona un servidor Power Systems, o més d'un, i supervisa o testifica l'estat fiable dels sistemes AIX Profile Manager mitjançant el centre de dades. La testificació és el procés en què el verificador determina (o testifica) si un col•lector ha dut a terme una engegada fiable.

Estat de l'engegada fiable

Es diu que una partició és fiable si el verificador testifica correctament la integritat del col•lector. El verificador és la partició remota que determina si un col•lector ha dut a terme una engegada fiable. El col•lector és la partició AIX que té connectat un Virtual Trusted Platform Module (VTPM) i té instal•lada la Trusted Software Stack (TSS). Indica que les mesures que s'han enregistrat dins del VTPM coincideixen amb un conjunt de referències que conserva el verificador. Un estat d'engegada fiable indica si la partició s'ha engegat de forma fiable. Aquesta afirmació és sobre la integritat del procés d'engegada del sistema i no indica el nivell actual o en curs de la seguretat del sistema.

Estat de l'engegada no fiable

Una partició es troba en un estat no fiable si el verificador no pot testificar correctament la integritat del procés d'engegada. L'estat no fiable indica que algun aspecte del procés d'engegada no és coherent amb la informació de referència que conserva el verificador. Entre les causes possibles d'una testificació anòmala s'hi troba l'engegada des d'un dispositiu d'arrencada diferent, l'engegada d'una imatge de kernel diferent i el canvi de la imatge d'arrencada existent.

Conceptes relacionats:

"Resolució de problemes amb l'engegada fiable" a la pàgina 119
Hi ha certs escenaris i passos de recuperació comuns necessaris a l'hora d'identificar el motiu de l'error en la testificació mitjançant l'engegada fiable.

Planificació de l'engegada fiable

Informació sobre les configuracions de maquinari i de programari necessàries per instal•lar l'engegada fiable.

Prerequisits de l'engegada fiable

La instal•lació de l'engegada fiable implica configurar el col•lector i el verificador.

Quan us prepareu per instal•lar el sistema operatiu AIX en un sistema que ja tingui instal•lada l'engegada fiable, heu de copiar el fitxer `/var/tss/lib/tpm/system.data` i utilitzar-lo per sobreescriure el fiter a la mateixa ubicació després d'acabar la reinstal•lació. Si no copieu aquest fitxer, heu d'eliminar el mòdul de plataforma fiable virtualitzat de la consola de gestió i tornar-lo a instal•lar a la partició.

Col•lector

Els requeriments de configuració per instal•lar un col•lector impliquen els següents prerequisits:

- Maquinari del POWER7 que s'està executant en un release de microprogramari 740.
- Instal•leu l'IBM AIX 6 amb el nivell tecnològic 7 o instal•leu l'IBM AIX 7 amb el nivell tecnològic 1.
- Instal•leu la versió 7.4 o posterior de la consola de gestió de maquinari (HMC).
- Configureu la partició amb el VTPM i un mínim d'un 1 GB de memòria.
- Instal•leu l'intèrpret d'ordres segur (SSH - Secure Shell), específicament l'OpenSSH o equivalent.

Verificador

Es pot accedir al verificador **openpts** des de la interfície de línia d'ordres i la interfície gràfica d'usuari que s'ha dissenyat per executar-lo en un interval de plataformes. La versió de l'AIX del verificador OpenPTS està disponible al paquet d'expansió de l'AIX. Hi ha disponibles versions del verificador OpenPTS per al Linux i altres plataformes mitjançant una descàrrega web. Els requeriments de configuració inclouen els prerequisits següents:

- Instal•leu l'SSH, específicament l'OpenSSH o equivalent.
- Estabiliu la connectivitat de xarxa (mitjançant l'SSH) al col•lector.
- Instal•leu la versió 1.6 o posterior de Java™ per accedir a la consola **openpts** des de la interfície gràfica.

Preparació per a la recuperació

La informació de l'engegada fiable que es descriu a continuació serveix de guia a l'hora d'identificar situacions que poden necessitar algun remei. El procés d'engegada no se'n veu afectat.

Hi ha certes circumstàncies en què una testificació pot fallar i és difícil predir la circumstància que es pot produir. Heu de decidir l'acció adient en funció de la circumstància. Això no obstant, és recomanable estar preparats per alguns casos greus i disposar d'una política o d'un flux de treball que us ajudi a gestionar aquest tipus d'incidents. La recuperació és l'acció de correcció que s'ha d'emprendre quan la testificació informa que un col•lector, o més d'un, no és fiable.

Per exemple, si s'ha produït un error de testificació perquè una imatge d'engegada difereix de la referència del verificador, penseu en tenir respostes a les preguntes següents:

- Com puc verificar que l'amenaça sigui creïble?
- Hi ha hagut algun manteniment planificat que s'hagi portat a terme, alguna actualització de l'AIX o maquinari nou que s'hagi instal•lat recentment?
- Podeu posar-vos en contacte amb l'administrador que accedeix a aquesta informació?
- Quan es va engegar el sistema per última vegada en un estat fiable?
- Si l'amenaça de seguretat sembla legítima, quina acció heu d'emprendre? (Els suggeriments inclouen la recopilació dels registres d'auditoria, la desconnexió del sistema de la xarxa, l'aturada del sistema i l'avís als usuaris).
- Hi havia algun altre sistema compromès que calgui comprovar?

Conceptes relacionats:

“Resolució de problemes amb l'engegada fiable” a la pàgina 119
Hi ha certs escenaris i passos de recuperació comuns necessaris a l'hora d'identificar el motiu de l'error en la testificació mitjançant l'engegada fiable.

Consideracions sobre la migració

Tingueu en compte aquests prerequisits abans de migrar una partició que s'hagi habilitat per al mòdul de plataforma fiable virtual (VTPM).

Un avantatge d'un VTPM sobre un TPM físic és que permet que la partició es desplaci entre sistemes mentre se'n conserva el VTPM. Per migrar de forma segura la partició lògica, el microprogramari xifra les dades del VTPM abans de la transmissió. Per tal de garantir una migració segura, s'ha d'haver implementat les següents mesures de seguretat abans de la migració:

- Habiliteu l'IPSEC entre el servidor d'E/S virtual (VIOS) que està duent a terme la migració.
- Definiu la clau del sistema fiable mitjançant la consola de gestió de maquinari (HMC) per controlar els sistemes gestionats capaços de desxifrar les dades VTPM després de la migració. El sistema de destinació de la migració ha de tenir la mateixa clau que la del sistema d'origen perquè les dades es migrin correctament.

Informació relacionada:

Utilització de l'HMC

Migració del VIOS

Instal•lació de l'engegada fiable

Hi ha certes configuracions de maquinari i programari necessàries per instal•lar l'engegada fiable.

Informació relacionada:

“Instal•lació del PowerSC Standard Edition” a la pàgina 7
Heu d'instal•lar un conjunt de fitxers per a cada funció específica del PowerSC Standard Edition.

Instal•lació del col•lector

Heu d'instal•lar el col•lector utilitzant el conjunt de fitxers des del CD bàsic de l'AIX.

Per tal d'instal•lar el col•lector, instal•leu els paquets `powerscStd.vtpm` i `openpts.collector` que es troben al CD bàsic, mitjançant l'ordre **smit** o **installp**.

Instal•lació del verificador

el component verificador OpenPTS s'executa al sistema operatiu AIX i en altres plataformes.

La versió de l'AIX del verificador es pot instal•lar des del conjunt de fitxers utilitzant el paquet d'expansió de l'AIX. Per instal•lar el verificador al sistema operatiu AIX, instal•leu el paquet `openpts.verifier` des del paquet d'expansió de l'AIX utilitzant l'ordre **smit** o **installp**. D'aquesta manera s'instal•len les versions de la interfície gràfica i de la línia d'ordres del verificador.

El verificador OpenPTS per a altres sistemes operatius es pot baixar de `Download Linux OpenPTS Verifier For Use With AIX Trusted Boot`.

Informació relacionada:

Baixada del verificador OpenPTS del Linux per a utilitzar-lo amb l'engegada fiable de l'AIX

Configuració de l'engegada fiable

Informació sobre el procediment per inscriure un sistema i testificar un sistema per a l'engegada fiable.

Inscripció d'un sistema

Informació sobre el procediment per inscriure un sistema amb el verificador.

La inscripció d'un sistema és el procés de proporcionar un conjunt inicial de mesures al verificador, que forma la base per a posteriors sol•licituds de testificació. Per inscriure un sistema des d'una línia d'ordres, utilitzeu l'ordre següent des del verificador:

```
openpts -i <nom d'amfitrió>
```

La informació sobre la partició inscrita es troba al directori `$HOME/.openpts`. Cada partició nova s'assigna a un únic identificador durant el procés d'inscripció i la informació relacionada amb les particions inscrites s'emmagatzema al directori corresponent a l'ID únic.

Per inscriure un sistema des de la interfície gràfica, seguiu aquests passos:

1. Inicieu la interfície gràfica utilitzant l'ordre **/opt/ibm/openpts_gui/openpts_GUI.sh**.
2. Seleccioneu **Inscriure** del menú de navegació.
3. Escriviu el nom d'amfitrió i les credencials SSH del sistema.
4. Feu clic a **Inscriure**.

Conceptes relacionats:

"Testificació d'un sistema"
Informació sobre el procediment per testificar un sistema des de la línia d'ordres i utilitzant la interfície gràfica.

Testificació d'un sistema

Informació sobre el procediment per testificar un sistema des de la línia d'ordres i utilitzant la interfície gràfica.

Per consultar la integritat de l'engegada d'un sistema, utilitzeu l'ordre següent des del verificador:

```
openpts <nom d'amfitrió>
```

Per testificar un sistema des d'una interfície gràfica, seguiu aquests passos:

1. Seleccioneu una categoria del menú de navegació.
2. Seleccioneu un sistema o més d'un per testificar-los.
3. Feu clic a **Testifica**.

Inscripció i testificació d'un sistema sense contrasenya

La sol•licitud de testificació s'envia a través de l'intèrpret d'ordres segur (SSH - Secure Shell). Instal•leu el certificat del verificador al col•lector per permetre connexions SSH sense contrasenya.

Per configurar el certificat del verificador al sistema del col•lector, seguiu aquests passos:

- Al verificador, executeu les ordres següents:

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

- Al col•lector, executeu l'ordre següent:

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

Gestió de l'engegada fiable

Informació sobre el procediment per gestionar resultats de testificació de l'engegada fiable.

Interpretació dels resultat de la testificació

Informació sobre el procediment per veure i comprendre els resultats de la testificació.

Una testificació pot donar com a resultat els estats següents:

1. Ha fallat la sol•licitud de testificació: la sol•licitud de testificació no s'ha completat correctament. Consulteu la secció Resolució de problemes per conèixer les possibles causes de l'error.
2. Integritat de sistema vàlida: la testificació s'ha completat correctament i l'engegada del sistema coincideix amb la informació de referència que conserva el verificador. Això indica una Engegada fiable correcta.
3. Integritat de sistema no vàlida: La sol•licitud de testificació s'ha completat però s'ha detectat una discrepància entre la informació que es recopila durant l'engegada del sistema i la informació de referència que conserva el verificador. Això indica una engegada no fiable.

La testificació també informa de si s'ha aplicat alguna actualització al recopilador mitjançant el missatge següent:

Actualització del sistema disponible: Aquest missatge indica que s'ha aplicat una actualització al recopilador i que hi ha disponible un conjunt d'informació de referència actualitzada que entrarà en vigor durant la propera engegada. A l'usuari se li demanarà quin verificador acceptarà o rebutjarà les actualitzacions. Per exemple, l'usuari pot decidir acceptar aquestes actualitzacions si l'usuari està assabentat del manteniment que s'efectua al col•lector.

Per tal d'investigar un error de testificació utilitzant la interfície gràfica, seguiu aquests passos:

1. Seleccioneu una categoria del menú de navegació.
2. Seleccioneu un sistema per investigar-lo.
3. Feu doble clic a l'entrada corresponent al sistema. Es visualitza una finestra de propietats. Aquesta finestra conté informació de registre sobre la testificació que ha fallat.

Supressió de sistemes

Informació sobre el procediment per suprimir un sistema des de la base de dates del verificador.

Per eliminar un sistema de la base de dades del verificador, executeu l'ordre següent:

```
openpts -r <nom d'amfitrió>
```

Resolució de problemes amb l'engegada fiable

Hi ha certs escenaris i passos de recuperació comuns necessaris a l'hora d'identificar el motiu de l'error en la testificació mitjançant l'engegada fiable.

L'ordre **openpts** declara un sistema com a no vàlid si l'estat de l'engegada fiable del sistema no coincideix amb la informació de referència que es conserva al verificador. L'ordre **openpts** determina el possible motiu pel qual la integritat no és vàlida. Hi ha diverses variables en una engegada de l'AIX completa i una testificació anòmala requereix un anàlisi per determinar la causa de l'error.

A la taula següent es llisten alguns escenaris i passos de recuperació comuns per identificar el motiu de l'error:

Taula 12. Resolució de problemes d'alguns escenaris comuns d'errors

Motiu de l'error	Possibles causes de l'error	Recuperació suggerida

No s'ha completat la testificació	• Nom d'amfitrió incorrecte.
	• No hi ha cap ruta de xarxa entre l'origen i la destinació.
	• Credencial de seguretat incorrectes.
		Comproveu la connexió del Secure Shell (SSH) utilitzant l'ordre següent:
		`ssh ptsc@hostname`
		
		Si la connexió de l'SSH és correcta, comproveu els motius següents de l'error en la testificació:
		• El sistema que s'està testificant no executa el daemon **tcsd**.
		• El sistema que s'està testificant no l'ha inicialitzat l'ordre **ptsc**. Aquest procés s'hauria de produir de forma automàtica durant l'inici del sistema però comproveu la presència d'un directori `/var/ptsc/` al col•lector. Si no existeix el directori `/var/ptsc/`, executeu l'ordre següent al col•lector:
		`ptsc -i`

S'ha modificat el microprogramari del complex electrònic central (CEC).	• S'ha aplicat una actualització de microprogramari. • L'LPAR s'ha migrat a un sistema que executava una versió diferent del microprogramari.	Comproveu el nivell de microprogramari del sistema que allotja l'LPAR.
Han canviat els recursos assignats a l'LPAR.	Ha canviat la CPU o la memòria assignada a l'LPAR.	Comproveu el fitxer de perfil de partició a l'HMC.
El microprogramari s'ha modificat pels adaptadors que hi ha disponibles a l'LPAR.	S'ha afegit o eliminat un dispositiu de maquinari de l'LPAR.	Comproveu el fitxer de perfil de partició a l'HMC.
S'ha canviat la llista de dispositius adjunta a l'LPAR.	S'ha afegit o eliminat un dispositiu de maquinari de l'LPAR.	Comproveu el fitxer de perfil de partició a l'HMC.
S'ha modificat la imatge d'engegada que inclou el kernel de sistema operatiu.	• S'ha aplicat una actualització de l'AIX i el verificador no era conscient de l'actualització. • S'ha executat l'ordre **bosboot**.	• Confirmeu amb l'administrador del col•lector si cal efectuar alguna acció de manteniment abans de la darrera operació de rearrencada. • Comproveu l'activitat de manteniment als registres del col•lector.
L'LPAR s'engega des d'un dispositiu diferent.	• La inscripció s'ha efectuat immediatament després de la instal•lació de la xarxa. • El sistema s'engega des d'un dispositiu de manteniment.	El dispositiu d'engegada i els senyalador es poden comprovar utilitzant l'ordre **bootinfo**. Si s'ha efectuat una inscripció immediatament després de la instal•lació del NIM (Network Installation Management - gestió d'instal•lació de xarxa) i abans de l'operació de rearrencada, els detalls d'inscripció pertanyen a la instal•lació de xarxa i no a la següent engegada de disc. Aquesta inscripció es pot reparar eliminant la inscripció i tornant a inscriure la partició lògica.
S'ha invocat al menú d'engegada dels serveis de gestió del sistema (SMS- System Management Services) interactius.		El procés d'engegada s'ha d'executar sense interrupcions ni cap interacció de l'usuari perquè el sistema sigui fiable. Si s'entra al menú d'engegada de l'SMS provoca que l'engegada no sigui vàlida.
S'ha modificat la base de dades de l'execució fiable (TE).	• S'han afegit o eliminat fitxers binaris de la base de dades de TE. • S'han actualitzat fitxers binaris a la base de dades.	Executeu l'ordre **trustchk** per verificar la base de dades.

Conceptes relacionats:

“Preparació per a la recuperació” a la pàgina 116
La informació de l'engegada fiable que es descriu a continuació serveix de guia a l'hora d'identificar situacions que poden necessitar algun remei. El procés d'engegada no se'n veu afectat.

“Conceptes de l'engegada fiable” a la pàgina 115
És important entendre la integritat del procés d'engegada i com classificar l'engegada segons sigui una engegada fiable o no fiable.

Informació relacionada:

Utilització de l'HMC

Tallafoc fiable

La funció Tallafoc fiable proporciona seguretat de capa de virtualització que millora el rendiment i els recursos de forma eficient quan s'estableix comunicació entre diferents zones de seguretat de la LAN virtual (VLAN) al mateix servidor de Power Systems. El tallafoc fiable redueix la càrrega a la xarxa externa desplaçant la capacitat de filtre dels paquets del tallafoc que compleixen determinades regles especials a la capa de virtualització. Aquesta capacitat de filtre es controla mitjançant normes de filtres de xarxa definides fàcilment, el que permet que el tràfic de xarxa fiable travessi zones de seguretat de la VLAN sense deixar l'entorn virtual. El tallafoc fiable protegeix i encamina el tràfic de xarxa intern entre els sistemes operatius AIX, IBM i i Linux.

Conceptes del tallafoc fiable

Hi ha alguns conceptes bàsics per entendre quan s'utilitza el tallafoc fiable.

El maquinari de Power Systems es pot configurar amb diverses zones de seguretat VLAN (LAN virtual). Una política configurada per l'usuari, creada com a norma de filtre del tallafoc fiable, permet que part del tràfic de xarxa fiable travessi les zones de seguretat VLAN i romangui a nivell intern de la capa de virtualització. Això és similar a introduir un tallafoc físic no connectat a l'entorn virtualitzat, que proporciona un mètode més eficient en quant al rendiment a l'hora d'implementar les prestacions del tallafoc per a centres virtualitzats.

Amb el Tallafoc fiable podeu configurar regles per permetre que cert tipus de transferència directament d'una VLAN d'un servidor d'E/S virtual (VIOS) en una altra VLAN del mateix VIOS, mentre encara es conserva un nivell elevat de seguretat limitant altres tipus de trànsit. És un tallafoc configurable en una capa de virtualització dels servidors Power Systems.

Utilitzant l'exemple de la Figura 1 a la pàgina 124, la finalitat és poder transferir informació de forma segura i eficient de l'LPAR1 de la VLAN 200 i de l'LPAR2 de la VLAN 100. Sense el Tallafoc fiable, la informació de destinació per a l'LPAR2 des de LPAR1 s'envia fora de la xarxa interna a l'encaminador, que encamina la informació altra vegada cap a l'LPAR2.

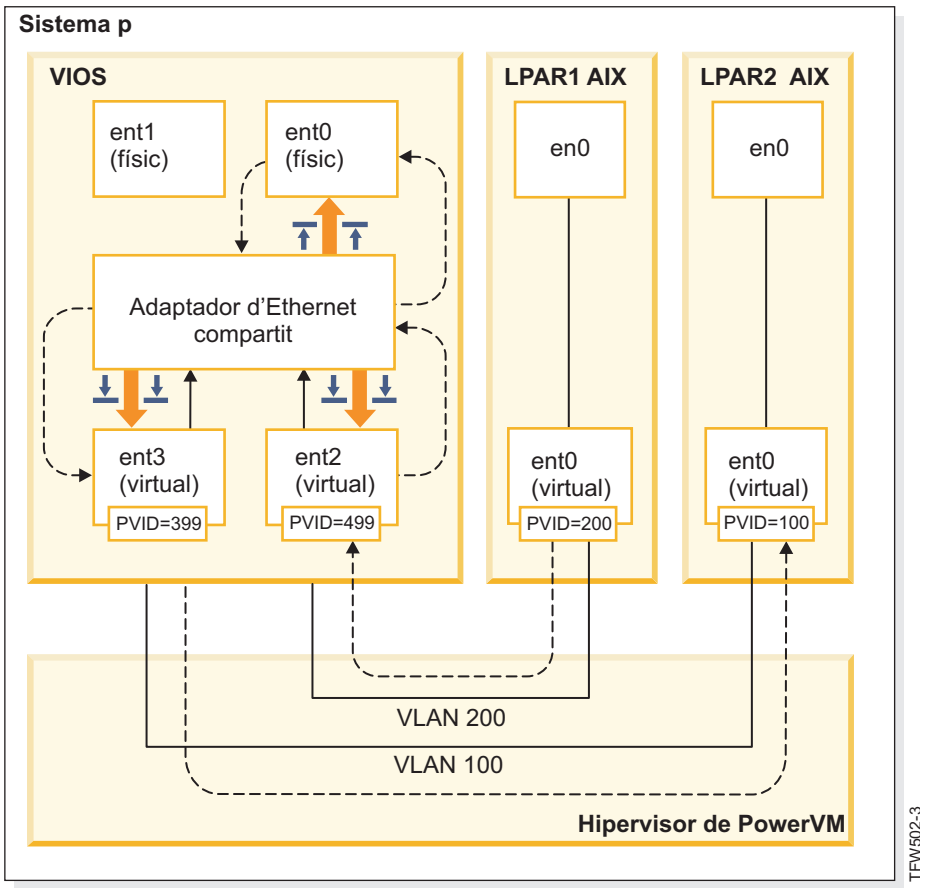

Figura 1. Exemple de transferència d'informació a través de la VLAN sense el tallafoc fiable

Mitjançant el tallafoc fiable podeu configurar regles per permetre que la informació passi de l'LPAR1 a l'LPAR2 sense deixar la xarxa interna. Aquest camí d'accés apareix a la Figura 2 a la pàgina 125.

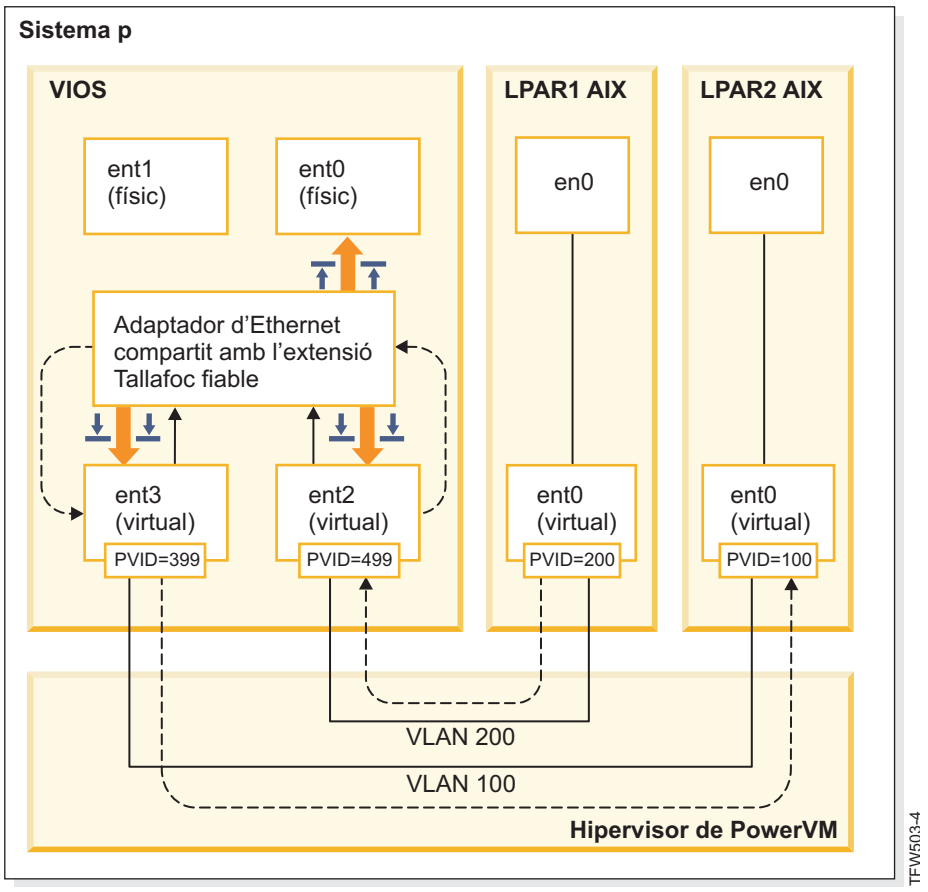

Figura 2. Exemple de la transferència d'informació a través de la VLAN amb el tallafoc fiable

Regles de configuració que pertanyen que determinada informació passi de forma segura a través de les VLAN retallen el camí d'accés a la destinació. El tallafoc fiable utilitza el SEA (adaptador d'Ethernet compartit) i l'extensió del kernel de la SVM (màquina virtual de seguretat) per permetre la comunicació.

Adaptador d'Ethernet compartit
El SEA és on comença i acaba l'encaminament. Quan es registre l'SVM, el SEA rep els paquets i els reenvia a l'SVM. Si l'SVM determina que el paquet és per a un LPAR del mateix servidor Power Systems, actualitza la capçalera de la capa 2 del paquet. El paquet es torna al SEA per reenviar-lo a la destinació final al sistema o a la xarxa externa.

Màquina virtual de seguretat
L'SVM és on s'apliquen les normes de filtre. Les normes de filtre són necessàries per mantenir la seguretat a la xarxa interna. Per registrar l'SVM amb el SEA, els paquets es reenvien a l'SVM abans d'enviar-los a la xarxa externa. En funció de les regles de filtre actives, l'SVM determina si un paquet roman a la xarxa interna o si es trasllada a la xarxa externa.

Instal•lació del tallafoc fiable

La instal•lació del tallafoc fiable del PowerSC és similar a instal•lar altres funcions del PowerSC.

Prerequisits:

- Les versions del PowerSC anteriors a la 1.1.1.0 no tenien el conjunt de fitxers necessari per instal•lar el tallafoc fiable. Assegureu-vos que disposeu del CD d'instal•lació del PowerSC de la versió 1.1.1.0 o posterior.
- Per aprofitar el tallafoc fiable, ja heu d'haver utilitzat la consola de gestió de maquinari (HMC) o el servidor d'E/S virtual (VIOS) per configurar les vostres LAN virtuals (VLAN).

El tallafoc fiable es proporciona com un conjunt de fitxers addicional en el CD d'instal•lació del PowerSC Standard Edition. El nom del fiter és `powerscStd.svm.rte`. Podeu afegir el tallafoc fiable a una instància existent de la versió 1.1.0.0, o posterior, del PowerSC, o instal•lar-lo com a part d'una nova instal•lació de la versió 1.1.1.0, o posterior, del PowerSC.

Per afegir la funció de tallafoc fiable en una instancia existent del PowerSC:

1. Assegureu-vos que executeu la versió 2.2.1.4, o posterior, del VIOS.
2. Inseriu el CD d'instal•lació de la versió 1.1.1.0 del PowerSC o baixeu la imatge del CD d'instal•lació.
3. Utilitzeu l'ordre **oem_setup_env** per l'accés a l'arrel.
4. Utilitzeu l'ordre **installp** o l'eina SMIT per instal•lar el conjunt de fitxers `PowerscStd.svm.rte`.

Informació relacionada:

"Instal•lació del PowerSC Standard Edition" a la pàgina 7
Heu d'instal•lar un conjunt de fitxers per a cada funció específica del PowerSC Standard Edition.

Configuració del tallafoc fiable

Calen paràmetres de configuració addicionals per a la funció de tallafoc fiable després d'instal•lar-la.

Advertiment de tallafoc fiable

L'Advertiment de tallafoc fiable analitza el trànsit del sistema des de diferents particions lògiques (LPAR) per proporcionar informació per determinar si mitjançant l'execució del tallafoc fiable es millora el rendiment del sistema.

Si la funció Advertiment de tallafoc fiable enregistra una quantitat significativa de trànsit des de diferents LAN virtuals (VLAN) que hi ha al mateix complex electrònic central, l'habilitació del tallafoc fiables hauria de beneficiar el vostre sistema.

Per habilitar l'advertiment de tallafoc fiable, escriviu l'ordre següent:

```
vlantfw -m
```

Per visualitzar l'advertiment de tallafoc fiable, escriviu l'ordre següent:

```
vlantfw -D
```

Per inhabilitar l'advertiment de tallafoc fiable, escriviu l'ordre següent:

```
vlantfw -M
```

Registre del tallafoc fiable

El registre del tallafoc fiable compila una llista de camins d'accés de tràfic de xarxa en el complex electrònic central. La llista mostra els filtres que utilitza el tallafoc fiable per encaminar el trànsit.

Quan l'advertiment de tallafoc fiable determina que l'encaminament del trànsit millora internament l'eficàcia, el registre del tallafoc fiable conserva una llista de camins d'accés al fitxer `svm.log`. La mida del fitxer `svm.log` està limitada a 16 MB. Si les entrades superen el límit de 16 MB, les entrades més antigues s'eliminaran del fitxer de registre.

Per iniciar el registre del tallafoc fiable, escriviu l'ordre següent:

```
vlantfw -l
```

Per aturar el registre del tallafoc fiable, escriviu l'ordre següent:

```
vlantfw -L
```

Podeu veure el fitxer de registre a la ubicació següent:`/home/padmin/svm/svm.log`.

Nota: Podeu executar les ordres per iniciar i aturar el registre de tallafoc fiable només quan estigueu autenticat com a usuari root.

Diversos adaptadors Ethernet compartits

Podeu configurar el tallafoc fiable en sistemes que utilitzen diversos adaptadors Ethernet compartits.

Algunes configuracions utilitzen diversos adaptadors Ethernet compartits (SEA) al mateix servidor d'E/S virtual (VIOS). Diversos SEA poden proporcionar avantatges de protecció en cas de migració després d'un error i de l'anivellament de recursos. El tallafoc fiable admet l'encaminament a través de diversos SEA, sempre que estiguin al mateix VIOS.

A la Figura 3 es mostra un entorn que utilitza diversos SEA.

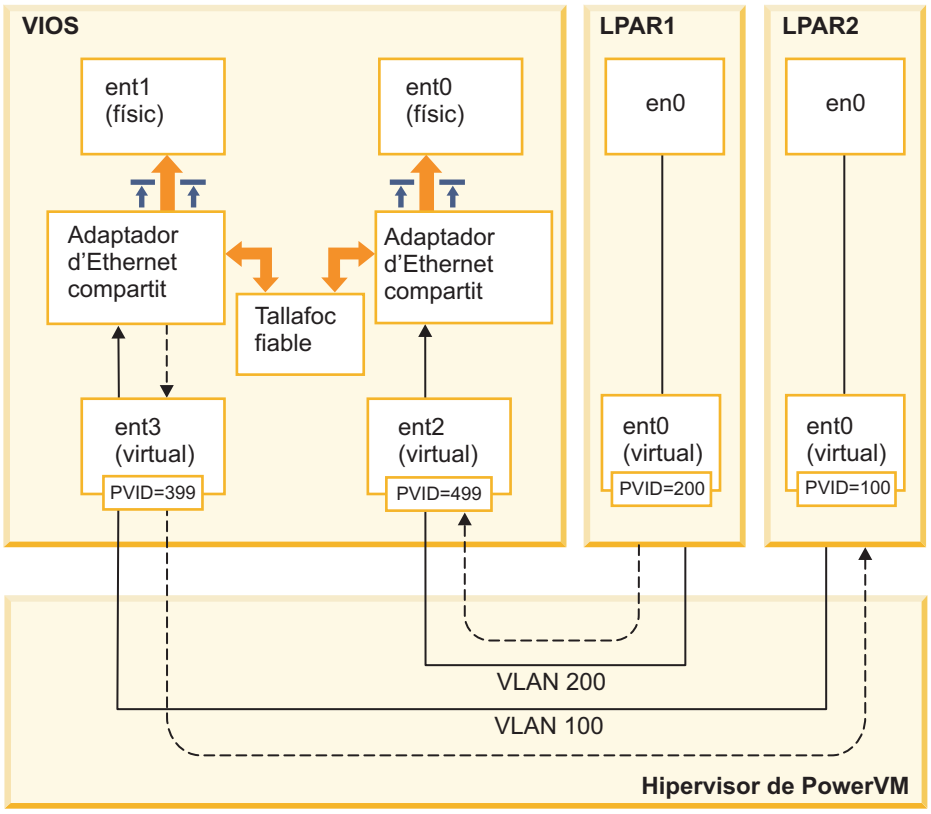

Figura 3. Configuració utilitzant diversos adaptadors Ethernet compartits en un únic VIOS

A continuació hi trobareu exemples de diverses configuracions de SEA que el tallafoc fiable admet:

- Els SEA es configuren amb adaptadors troncals al mateix commutador virtual d'hipervisor Power. Aquesta configuració s'admet perquè cada SEA rep tràfic de xarxa amb diferents ID de VLAN.
- Els SEA es configuren amb adaptadors troncals en diferents commutadors virtuals d'hipervisors Power i cada adaptador troncal es troba en un ID de VLAN diferent. En aquesta configuració, cada SEA continua rebent tràfic de xarxa utilitzant diferents ID de VLAN.
- Els SEA es configuren amb adaptadors troncals en diferents commutadors virtuals d'hipervisors Power i es tornen a utilitzar els mateixos ID de VLAN als commutadors virtuals. En aquest cas, el tràfic per a ambdós SEA té els mateixos ID de VLAN.

  Un exemple d'aquesta configuració és tenir la LPAR2 a VLAN200 amb el commutador virtual 10 i la LPAR3 a VLAN200 amb el commutador virtual 20. Com que totes dues LPAR i els seus corresponents SEA utilitzen el mateix ID de VLAN (VLAN200), tots dos SEA tenen accés als paquets amb aquest ID de VLAN.

No podeu habilitar el ponteig en més d'un VIOS. Per aquest motiu, el tallafoc fiable no admet les següents configuracions de diversos SEA:

- Diversos VIOS i diversos controladors de SEA.
- Compartició de càrrega de SEA redundant: els adaptadors troncals es configuren perquè l'encaminament entre VLAN no es pugui dividir entre servidors del VIOS.

Extracció d'adaptadors Ethernet compartits

Els passos per extreure l'adaptador Ethernet compartit del sistema s'han de dur a terme en un ordre concret.

Per extreure un adaptador Ethernet compartit (SEA) del sistema, seguiu aquests passos:

1. Extraieu la màquina virtual de seguretat associada al SEA escrivint l'ordre següent:
   ```
   rmdev -dev svm
   ```
2. Extraieu el SEA escrivint l'ordre següent:
   ```
   rmdev -dev ID adaptador ethernet compartit
   ```

Nota: L'extracció del SEA abans d'extreure la SVM pot provocar un error del sistema.

Creació de regles

Podeu crear regles per habilitar l'encaminament a través de la VLAN del tallafoc fiable.

Per habilitar les funcions d'encaminament del tallafoc fiable, heu de crear regles que especifiquin quines comunicacions es permeten. Per a la seguretat ampliada, no hi ha cap regla única que permeti la comunicació entre totes les VLAN del sistema. Cada connexió permesa requereix la seva pròpia regla, encara que cada regla estigui activada es permet la comunicació en ambdues direccions dels punts finals especificats.

Com que s'ha creat la creació de regles a la interfície del servidor d'E/S virtual (VIOS), hi ha disponible informació addicional sobre les ordres en la col•lecció de temes del VIOS al Centre d'informació de maquinari de Power Systems.

Per crear una regla, seguiu aquests passos:

1. Obriu la interfície de línia d'ordres del VIOS.
2. Inicialitzeu el controlador de l'SVM escrivint l'ordre següent:
   ```
   mksvm
   ```
3. Inicieu el tallafoc fiable escrivint l'ordre d'inici:
   ```
   vlantfw -s
   ```
4. Per visualitzar totes les adreces conegudes MAC i IP de l'LPAR, escriviu l'ordre següent:
   ```
   vlantfw -d
   ```

   Necessitareu les adreces IP i MAC de les particions lògiques (LPAR) de les que esteu creant les regles.
5. Creeu la norma de filtre per permetre la comunicació entre les dues LPAR (LPAR1 i LPAR2) escrivint una de les ordres següents (les ordres s'haurien d'escriure en una línia):
   ```
   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
   ```

   Nota: Una norma de filtre permet la comunicació en les dues direccions per defecte, depenent de les entrades de port i de protocol. Per exemple, podeu habilitat Telnet per a l'LPAR1 a l'LPAR2 executant l'ordre següent:

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

6. Activeu totes les normes de filtre del kernel escrivint l'ordre següent:

```
mkvfilt -u
```

Nota: Aquest procediment activa aquesta regla i les altres normes de filtre que existeixen al sistema.

Exemples addicionals

Als exemples següents es mostren algunes normes de filtres que podeu crear utilitzant el tallafoc fiable.

- Per permetre la comunicació de l'intèrpret d'ordres segur (SSH - Secure Shell) des de l'LPAR de la VLAN 100 a l'LPAR de la VLAN 200, escriviu l'ordre següent:

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

- Per permetre el trànsit entre tots els ports 0 a 499, escriviu l'ordre següent:

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

- Per permetre tot el trànsit del TCP entre les LPAR, escriviu l'ordre següent:

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

  Si no especifiqueu cap port ni cap altra operació de port, el trànsit pot utilitzar tots els ports.

- Per permetre l'enviament de missatges d'Internet Control Message Protocol entre les LPAR, escriviu l'ordre següent:

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

Conceptes relacionats:

"Desactivació de regles"
Podeu desactivar regles que permetin l'encaminament a través de VLAN en la funció Tallafoc fiable.

Referència relacionada:

"Ordre genvfilt" a la pàgina 172
"Ordre mkvfilt" a la pàgina 174
"Ordre vlantfw" a la pàgina 193

Informació relacionada:

Servidor virtual d'entrada i sortida (VIOS)

Desactivació de regles

Podeu desactivar regles que permetin l'encaminament a través de VLAN en la funció Tallafoc fiable.

Com que les regles s'han desactivat a la interfície del servidor d'E/S virtual (VIOS), hi ha disponible informació addicional sobre les ordres i els processos en la col•lecció de temes del VIOS al Centre d'informació de maquinari de Power Systems.

Per desactivar una regla, seguiu aquests passos:

1. Obriu la interfície de línia d'ordres del VIOS.
2. Per visualitzar totes les regles de filtre actives, escriviu l'ordre següent:

   ```
   lsvfilt -a
   ```

   Podeu ometre el senyalador **-a** per visualitzar totes les regles de filtre emmagatzemades a l'Object Data Manager.
3. Fixeu-vos en el nombre d'identificació de la regla de filtre que esteu desactivant. En aquest exemple, el nombre d'identificació de la regla de filtre és 23.
4. Desactiveu la regla de filtre 23 quan estigui activa al kernel escrivint l'ordre següent:

   ```
   rmvfilt -n 23
   ```

Per desactivar totes les regles de filtre del kernel, escriviu l'ordre següent:

```
rmvfilt -n all
```

Conceptes relacionats:

"Creació de regles" a la pàgina 128
Podeu crear regles per habilitar l'encaminament a través de la VLAN del tallafoc fiable.

Referència relacionada:

"Ordre lsvfilt" a la pàgina 173

"Ordre rmvfilt" a la pàgina 193

Registre fiable

El registre fiable del PowerVM permet que les particions lògiques (LPAR) de l'AIX escriguin informació als fitxers de registre que s'emmagatzemen en un servidor d'E/S virtual connectat (VIOS). Les dades es transmeten al VIOS directament a través de l'hipervisor, i la connectivitat de xarxa no és necessària entre la LPAR client i el VIOS.

Registres virtuals

L'administrador del servidor d'E/S virtual (VIOS) crea i gestiona els fitxers de registre i es presenten al sistema operatiu de l'AIX com a dispositius de registre virtuals al directori `/dev`, d'una forma similar als discs virtuals o als suports òptics virtuals.

Si s'emmagatzemen els fitxers de registre com a registres virtuals, augmenta el nivell de confiança als registres perquè un usuari amb privilegis d'usuari root no els pot canviar a la LPAR de client on s'han generat. Es poden connectar diversos dispositius de registres virtuals al mateix LPAR de client i cada registre es troba en un fitxer diferent dins del directori `/dev`.

El registre fiable permet consolidar les dades de registre procedents de diverses LPAR de client en un únic sistema de fitxers, al qual es pot accedir des del VIOS. Per tant, el VIOS proporciona una única ubicació al sistema per a l'anàlisi de registres i l'arxivat. L'administrador de la LPAR de client pot configurar aplicacions i el sistema operatiu AIX perquè les dades s'escriguin als dispositius de registres virtuals, de forma similar que s'escriuen les dades als fitxers locals. El subsistema d'auditoria de l'AIX es pot configurar per dirigir els registres d'auditoria a registres virtual i altres serveis de l'AIX com, per exemple, syslog, treballen amb la configuració existent per dirigir les dades als registres virtuals.

Per configurar el registre virtual, l'administrador del VIOS ha d'especificar un nom pel registre virtual que té els següents components independents:

- Nom de client
- Nom de registre

Els noms dels dos components els pot definir l'administrador del VIOS en qualsevol valor, però el nom de client sol ser el mateix per a tots els registres virtuals que s'han connectat a una LPAR determinada (per exemple, el nom d'amfitrió de la LPAR). El nom de registre s'utilitza per identificar la finalitat del registre (per exemple, auditoria o syslog).

En una LPAR de l'AIX, cada dispositiu de registre virtual està present com a dos fitxers funcionalment equivalents al sistema de fitxers `/dev`. El nom del primer fitxer apareix després del dispositiu, per exemple, `/dev/vlog0`, i el segon fitxer s'anomena concatenant un prefix `vl` amb el nom del registre i el número de dispositiu. Per exemple, si el dispositiu de registre virtual `vlog0` té `audit` com a nom de registre, es trobarà al sistema de fitxers `/dev` com a `vlog0` i `vlaudit0`.

Informació relacionada:

Creació de registres virtuals

Detecció de dispositius de registre virtuals

Una vegada l'administrador del VIOS hagi creat els dispositius de registre virtuals i els hagi connectat a una LPAR client, cal renovar la configuració del dispositiu de la LPAR client perquè els dispositius estiguin visibles.

L'administrador de la LPAR client renova els valors utilitzant un dels mètodes següents:

- Reiniciant la LPAR client
- Executant l'ordre **cfgmgr**

Executeu l'ordre **lsdev** per visualitzar els dispositius de registre virtuals. Els dispositius s'anteposen a `vlog`, de forma predeterminada. A continuació hi trobareu un exemple de la sortida de l'ordre **lsdev** en una LPAR de l'AIX en què hi ha dos dispositius de registres virtuals:

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

Examineu les propietats d'un dispositiu de registre virtual utilitzant l'ordre `lsattr –El <nom dispositiu>`, que genera una sortida similar a la següent:

```
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
```

Aquesta sortida mostra el nom de client, el nom de dispositiu i la quantitat de dates de registre que pot emmagatzemar al VIOS.

El registre virtual emmagatzema dos tipus de dades de registre, que són les següents:

- Dades de registre: les dades de registre sense format generades per aplicacions a la LPAR de l'AIX.
- Dades d'estat: informació sobre quan s'han configurat, s'han obert, s'han tancat els dispositius i altres operacions que s'utilitzen per analitzar l'activitat del registre.

L'administrador del VIOS especifica la quantitat de **dades de registre** i de **dades d'estat** que es poden emmagatzemar per a cada registre virtual, i la quantitat s'indica mitjançant els valors `max_log_size` i `max_state_size`. Quan la quantitat de les dades emmagatzemades supera el límit especificat, se sobreescriuen les dades de registre més antigues. L'administrador del VIOS ha d'assegurar que es recopilen les dades de registre i que s'arxiven amb freqüència per conservar els registres.

Instal•lació del registre fiable

Podeu instal•lar la funció Registre fiable del PowerSC utilitzant la interfície de línia d'ordres o l'eina SMIT.

Els prerequisits per instal•lar el registre fiable són la versió 2.2.1.0, o anterior, del VIOS i l'IBM AIX 6 amb el nivell tecnològic 7 o l'IBM AIX 7 amb el nivell tecnològic 1.

El nom de fitxer per instal•lar la funció de registre fiable és `powerscStd.vlog`, que s'inclou al CD d'instal•lació del PowerSC Standard Edition.

Per instal•lar la funció Registre fiable:

1. Assegureu-vos que executeu la versió 2.2.1.0, o posterior, del VIOS.
2. Inseriu el CD d'instal•lació del PowerSC o baixeu la imatge del CD d'instal•lació.
3. Utilitzeu l'ordre **installp** o l'eina SMIT per instal•lar el conjunt de fitxers `powerscStd.vlog`.

Informació relacionada:

“Instal•lació del PowerSC Standard Edition” a la pàgina 7
Heu d'instal•lar un conjunt de fitxers per a cada funció específica del PowerSC Standard Edition.

Configuració del registre fiable

Informació sobre el procediment per configurar el registre fiable al subsistema d'auditoria de l'AIX i al syslog.

Configuració del subsistema d'auditoria de l'AIX

El subsistema d'auditoria de l'AIX es pot configurar per escriure dades binàries en un dispositiu de registre virtual a més d'escriure registres al sistema de fitxers local.

Nota: Abans de configurar el subsistema d'auditoria de l'AIX, cal que dueu a terme el procediment de l'apartat "Detecció de dispositius de registre virtuals" a la pàgina 131.

Per configurar el subsistema d'auditoria de l'AIX, seguiu aquests passos:

1. Configureu el subsistema d'auditoria de l'AIX per registrar dades en mode binari (`auditbin`).
2. Activeu l'engegada fiable per a l'auditoria de l'AIX editant el fitxer de configuració `/etc/security/audit/config`.
3. Afegiu un paràmetre `virtual_log = /dev/vlog0` a l'stanza `bin:`.

   Nota: La instrucció és vàlida si l'administrador de l'LPAR vol que les dades `auditbin` s'escriguin al fitxer `/dev/vlog0`.
4. Reinicieu el subsistema d'auditoria de l'AIX en la seqüència el següent:

   ```
   audit shutdown
   audit start
   ```

Els registres d'auditoria s'escriuen al servidor d'E/S virtual (VIOS) a través del dispositiu de registre virtual especificat a més d'escriure registres al sistema de fitxers local. Els registres s'emmagatzemen sota control dels paràmetres `bin1` i `bin2` existents a l'stanza `bin:` del fitxer de configuració `/etc/security/audit/config`.

Informació relacionada:

Subsistema d'auditoria

Configuració del syslog

Es pot configurar el syslog perquè escrigui missatger en registres virtuals aplicant regles al fitxer `/etc/syslog.conf`.

Nota: Abans de configurar el fitxer `/etc/syslog.conf`, cal que dueu a terme el procediment de l'apartat "Detecció de dispositius de registre virtuals" a la pàgina 131.

Podeu editar el fitxer `/etc/syslog.conf` perquè coincideixi amb els missatges de registre, que es basen en els criteris següents:

- Recurs
- Nivell de prioritat

Per utilitzar els registres virtuals pels missatges del syslog, s'ha d'haver configurat el fitxer `/etc/syslog.conf` amb regles per escriure els missatges desitjats al registre virtual adient al directori `/dev`.

Per exemple, per enviar missatges de nivell de depuració generats per qualsevol recurs al registre virtual `vlog0`, afegiu la línia següent al fitxer `/etc/syslog.conf`:

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

Nota: No utilitzeu els recursos de rotació de registres que hi ha disponibles al daemon `syslogd` per a qualsevol ordre que escrigui dades en registres virtuals. Els fitxers del sistema de fitxers `/dev` no són fitxers normals i no es pot canviar el nom ni desplaçar. L'administrador del VIOS ha de configurar la rotació de registres virtuals al VIOS.

Cal reiniciar el daemon `syslogd` després de dur a terme la configuració utilitzant l'ordre següent:

```
refresh -s syslogd
```

Informació relacionada:

Daemon syslogd

Escriptura de dades en dispositius de registre virtuals

Les dades arbitràries s'escriuen en un dispositiu de registre virtual obrint el fitxer corresponent del directori `/dev` i escrivint les dades al fitxer. Un procés pot obrir un registre virtual cada vegada.

Per exemple:

Per escriure missatges als dispositius de registre virtuals mitjançant l'ordre **echo**, escriviu l'ordre següent:

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

Per emmagatzemar fitxers als dispositius de registre virtuals mitjançant l'ordre **cat**, escriviu l'ordre següent:

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

La mida màxima d'escriptura individual està limitada a 32 KB i els programes que intenten escriure més dades en una sola operació d'escriptura reben un error d'E/S (EIO). Les utilitats de la interfície de línia d'ordres (CLI), com ara l'ordre **cat**, interrompen automàticament les transferències en operacions d'escriptura de 32 KB.

Trusted Network Connect (TNC)

El Trusted Network Connect (TNC) forma part del grup d'informàtica fiable (TCG) que proporciona especificacions per verificar la integritat del punt final. El TNC té definida una arquitectura de solucions obertes que ajuda els administradors a aplicar polítiques per controlar de forma eficaç l'accés a la infraestructura de xarxa.

El Trusted Network Connect (TNC) té quatre components:

- Servidor de TNC
- Gestió de pedaços del TNC
- Servidor de TNC
- Remitidor d'IP de TNC

Conceptes de Trusted Network Connect

Informació sobre els components, la configuració de comunicació segura i el sistema de gestió de pedaços del Trusted Network Connect (TNC).

Components del Trusted Network Connect

Informació sobre els components de l'estructura del Trusted Network Connect (TNC).

El model de TNC consta dels components següents:

Servidor de Trusted Network Connect (TNC)

El servidor de Trusted Network Connect (TNC) identifica els clients que s'afegeixen a la xarxa i inicia una verificació en ells.

El client de TNC proporciona la informació de nivell de conjunt de fitxers necessària per a la verificació del servidor. El servidor determina si el client es troba al nivell que ha configurat l'administrador. Si el client no és compatible, el servidor de TNC avisa l'administrador indicant-li que cal posar-hi remei.

El servidor de TNC inicia la verificació als clients que intenten accedir a la xarxa. El servidor de TNC carrega un conjunt de verificadors de mesures d'integritat (IMV) que poden sol•licitar mesures d'integritat dels client i verificar-los. L'AIX té un IMV per defecte que verifica el conjunt de fitxers i el nivell de pedaços de seguretat dels sistemes. El servidor de TNC és una estructura que carrega i gestiona diversos mòduls de l'IMV. Per verificar un client, es parteix dels IMV per sol•licitar informació dels clients i es verifiquen els clients.

Gestió de pedaços del TNC

El servidor de Trusted Network Connect (TNC) s'integra amb el Service Update Management Assistant (SUMA) i cURL per proporcionar una solució de gestió de pedaços completa.

El gestor de pedaços descarrega els darrers paquets de servei i esmenes de seguretat que hi ha disponibles als llocs web d'IBM ECC i de Fix Central. El daemon de gestió de pedaços de TNC envia la informació actualitzada més recentment al servidor de TNC, que serveix de conjunt de fitxers de línia base per verificar els clients.

El daemon **tncpmd** s'ha de configurar per gestionar les baixades de SUMA i enviar la informació de conjunt de fitxers al servidor de TNC. Aquest daemon s'ha d'allotjar en un sistema que estigui connectat a Internet perquè baixi automàticament les actualitzacions. Per utilitzar el servidor de gestió de pedaços del TNC sense connectar-lo a Internet, podeu registrar un dipòsit d'esmenes definides per l'usuari amb el servidor de gestió de pedaços del TNC.

Nota: El servidor de TNC i el daemon **tncpmd** es pot allotjar al mateix sistema.

La gestió de pedaços es proporciona en un dels mètodes següents:

- Utilitzant la interfície de línia d'ordres (pmconf)
- Utilitzant el daemon (tncpmd2)

Utilització de la interfície de línia d'ordres (pmconf) per proporcionar gestió de pedaços:

SUMA i cURL s'invoquen quan es baixa un nivell de Service Pack (nivell d'SP) mitjançant l'ordre **pmconf add**.

Quan es baixa un nivell de Service Pack (nivell d'SP) mitjançant l'ordre **pmconf add**, s'invoca SUMA per baixar i registrar el nivell d'SP amb el TNC. A més, s'invoca cURL per baixar totes les esmenes de seguretat noves o que falten.

Els següents arguments de l'ordre **pmconf get** proporcionen més control sobre la gestió d'esmenes de seguretat:

- **display-only** permet que l'usuari examini les descripcions de vulnerabilitats que aborden les esmenes de seguretat que apliquen al nivell d'SP. Les esmenes de seguretat no es baixen fent servir aquesta ordre.
- **download-only** permet que l'usuari baixi, sense aplicar, esmenes de seguretat en un directori de baixada proporcionat per l'usuari. No s'apllica cap correcció.

Utilització del daemon (tncpmd2) per proporcionar gestió de pedaços:

El component planificador del daemon es pot configurar per comprovar automàticament les actualitzacions que afecten la seguretat dels clients de TNC.

Un interval de baixada controla la freqüència en que el planificador comprova els nivells de Service Pack nous. Si es detecta un nivell tecnològic (TL) per un nivell de Service Pack nou que està registrat actualment al TNC, es baixarà i s'afegirà al dipòsit tant el nivell de Service Pack nou com les correccions noves de seguretat o les que faltin. L'interval de baixada s'estableix utilitzant l'ordre **pmconf init**. El valor recomanat és com a mínim d'un per mes (43.200 minuts).

Un "ifix_download_interval" controla la freqüència en que el planificador comprova les correccions provisionals de seguretat noves que es puguin haver publicat. Totes les esmenes de seguretat noves es baixen i s'afegeixen al dipòsit. L'interval de baixada de correccions provisionals recomanat és d'un per dia (1440 minuts).

Client de Trusted Network Connect

El client de Trusted Network Connect (TNC) proporciona la informació necessària per a la verificació del servidor de TNC.

El servidor determina si el client es troba al nivell configurat per l'administrador. Si el client no és compatible, el servidor de TNC avisa l'administrador de les actualitzacions necessàries.

El client de TNC carrega els IMC durant l'engegada i els utilitza per recopilar la informació necessària.

Remitidor d'IP de Trusted Network Connect

El servidor de Trusted Network Connect (TNC) pot iniciar automàticament la verificació en clients que formin part de la xarxa. El remitidor d'IP que s'executa a la partició del servidor d'E/S virtual (VIOS) detecta els clients nous als quals el VIOS presta servei i envia les adreces IP al servidor de TNC. El servidor de TNC verifica el client segons la política que tingui definida.

Comunicació segura de Trusted Network Connect

Els daemons de Trusted Network Connect (TNC) es comuniquen entre els canals xifrats que s'han habilitat mitjançant Transport Layer Security (TLS) o Secure Sockets Layer (SSL).

La comunicació segura consisteix a garantir que les dades i les ordres que flueixen per la xarxa estiguin s'autentiquin i es protegeixin. Cada sistema ha de tenir la seva pròpia clau i el seu propi certificat que es generen quan s'executa l'ordre d'inicialització dels components. Aquest procés és totalment transparent per a l'administrador i requereix menys implicació per part seva.

Per verificar un client nou, cal importar el certificat del client a la base de dades del servidor. El certificat es marca com a no fiable d'entrada i, aleshores, l'administrador utilitza l'ordre **psconf** per veure i marcar els certificats com a fiables escrivint l'ordre:

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

Per utilitzar una clau i un certificat diferents, l'ordre **psconf** proporciona l'opció d'importar el certificat.

Per importar el certificat des del servidor, escriviu l'ordre següent:

```
psconf import  -S -k<nom de fitxer de claus> -f<nom de fitxer de claus>
```

Per importar el certificat des del client, escriviu l'ordre següent:

```
psconf import -C -k<nom de fitxer de claus> -f<nom de fitxer de claus>
```

Protocol de Trusted Network Connect

El protocol de Trusted Network Connect (TNC) s'utilitza amb l'estructura de TNC per conservar la integritat de la xarxa.

El TNC proporciona especificacions per verificar la integritat del punt final. S'accedeix als punts finals que sol•liciten accés en funció de les mesures d'integritat dels components crítics que poden afectar a l'entorn operatiu. L'estructura de TNC permet que els administradors supervisin la integritat dels sistemes a la xarxa. El TNC està integrat amb la infraestructura de distribució de pedaços de l'AIX per formar una solució de gestió de pedaços completa.

Les especificacions del TNC han de satisfer els requisits de l'arquitectura del sistema AIX i família de POWER. Els components del TNC s'han dissenyat per proporcionar una solució de gestió de pedaços completa al sistema operatiu AIX. Aquesta configuració permet que els administradors gestionin de forma eficient la configuració de programari als desplegaments d'AIX. Proporciona eines per verificar els nivells de pedaços dels sistemes i genera un informe dels clients que no són compatibles. A més, la gestió de pedaços simplifica el procés de baixada de pedaços i d'instal•lar-los.

Mòduls IMC i IMV

El servidor o el client de Trusted Network Connect (TNC) utilitzen internament els mòduls col•lector de mesures d'integritat (IMC) i el verificador de mesures d'integritat (IMV) per a la verificació del servidor.

Aquesta estructura permet carregar diversos mòduls IMC i IMV al servidor i als clients. El mòdul que du a terme la verificació del sistema operatiu (OS) i del nivell de conjunt de fitxers se subministra amb el sistema operatiu AIX per defecte. Per accedir als mòduls que se subministren amb el sistema operatiu AIX, utilitzeu un dels camins d'accés següents:

- `/usr/lib/security/tnc/libfileset_imc.a`: recopila el nivell de sistema operatiu i informació sobre el conjunt de fitxers que s'instal•la des del sistema client i l'envia a l'IMV (servidor de TNC) perquè la verifiqui.
- `/usr/lib/security/tnc/libfileset_imv.a`: sol•licita el nivell de sistema operatiu i informació sobre el conjunt de fiters del client i la compara amb la informació de la línia base. També actualitza l'estat del client a la base de dades del servidor de TNC. Per veure l'estat, introduïu l'ordre següent:

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

Referència relacionada:

"Ordre psconf" a la pàgina 179

Requeriments del TNC

Per utilitzar completament totes les funcions de cada component del TNC, heu de verificar que hi hagi disponibles els requeriments mínims al vostre entorn.

Gestió de pedaços del TNC

AIX	SUMA	OpenSSL	Notes
7.2 TL1	7.2.1.0	1.0.2	Se subministra amb el sistema operatiu
7.2 TL0	7.2.1.0	1.0.2	Pot ser que calgui instal•lar SUMA/Java per separat.
7.1 TL4	7.2.1.0	1.0.2	Pot ser que calgui instal•lar SUMA/Java per separat.
7.1 TL1, TL2, TL3			No s'admet la baixada dels nivells de Service Pack de l'AIX 7.2
7.1 TL0			Nivell de versió mínim admès per al TNCPM

Configuració dels components de TNC

Cadascun dels components de Trusted Network Connect (TNC) requereixen certa configuració per poder-lo executar al vostre entorn.

És necessari dur a terme tots els passos del procediment següent per configurar els components de TCN. Hi ha passos addicionals opcionals descrits a

1. Identifiqueu les adreces IP dels sistemes on es configurarà el servidor de TNC, el servidor de TNCPM (gestió de pedaços del TNC) i el remitidor d'IP de TNC pel servidor d'E/S virtual (VIOS).
2. Configureu el servidor de gestió d'instal•lació de xarxa (NIM). El sistema que s'ha configurat com a servidor de TNCPM és la NIM mestre. El conjunt de fitxers `sets:bos.sysmgt.nim.master` s'ha d'haver instal•lat en aquest sistema.
3. Heu d'habilitar l'AHA (Autonomic Health Advisor) per rebre notificacions automàtiques dels Service Pack nous i de les correccions de seguretat al servidor de TNC. Si no s'ha habilitat l'AHA, el planificador de TNC actualitzarà el servidor de TNC als intervals planificats. Per habilitar l'AHA perquè rebi notificacions automàtiques:

   ```
   mkdir /aha
    /usr/sbin/mount -v ahafs  /aha /aha
   ```

4. Per inicialitzar els dipòsits de correccions per a la gestió de pedaços del TNC, escriviu l'ordre següent (escriviu l'ordre en una sola línia):

   ```
   pmconf init -i <interval de descàrrega> -l <llista de Nt> [-A] [-P <camí d'accés de descàrrega>]
   [-x <interval de correccions provisionals>] [-K <clau de correcció provisional>]
   ```

   A continuació hi trobareu un exemple de l'ordre **pmconf**:

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

   L'ordre **init** baixa el Service Pack més recent per a cada nivell tecnològic i el deixa disponible per al servidor de TNC. Els Service Pack actualitzats permeten que el servidor de TNC executi una verificació del client de TNC de línia base i que el servidor de gestió de pedaços de TNC instal•li les actualitzacions del client de TNC. Especifiqueu el senyalador **-A** per acceptar tots els acords de llicència quan s'executin les actualitzacions del client. De forma predeterminada, els dipòsits de

correccions que baixa el servidor de gestió de pedaços de TNC es troben al fitxer /var/tnc/tncpm/fix_repository. Utilitzeu el senyalador **-P** per especificar un directori diferent.

5. Configureu el servidor de TNCPM. El servidor de TNCPM es pot configurar al sistema NIM. El servidor de TNCPM utilitza SUMA per descarregar els pedaços des dels llocs web de l'IBM Fix Central i de l'ECC. El servidor de TNCPM utilitza el cURL per baixar les correccions provisionals del lloc de seguretat d'IBM. Per baixar les actualitzacions, el sistema ha d'estar connectat a Internet. Escriviu l'ordre següent per configurar el servidor de TNCPM:

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

   Per exemple:

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

6. Configureu les polítiques al servidor de TNC. Per crear les polítiques per tal de verificar els clients, consulteu l'apartat "Creació de polítiques per al client de Trusted Network Connect" a la pàgina 143
7. Configureu els clients utilitzant l'ordre següent:

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

   Per exemple:

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

8. Completeu la configuració dels components de TNC duent a terme els passos opcionals per a cada component.

Referència relacionada:

"Ordre psconf" a la pàgina 179

Informació relacionada:

"Instal•lació del PowerSC Standard Edition" a la pàgina 7
Heu d'instal•lar un conjunt de fitxers per a cada funció específica del PowerSC Standard Edition.

Instal•lació amb la NIM

IBM Fix Central

Centre d'ajuda en línia del Passport Advantage

Configuració d'opcions per als components de TNC

Podeu configurar una o vàries opcions per a cadascun dels components de TNC.

Configuració d'opcions per al servidor de Trusted Network Connect (TNC)

Informació sobre els passos per configurar el servidor de TNC.

Per configurar el servidor de TNC, cal que el fitxer /etc/tnccs.conf tingui un valor similar al següent:

```
component = SERVER
```

Per configurar un sistema com a servidor, escriviu l'ordre següent:

```
psconf mkserver tncport=<port> pmserver=<ip|hostname[,ip2|hostname2..]:port>
[recheck_interval=<hora en minuts>]
```

Per exemple:

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

Nota: El port tncport i el port pmserver han de tenir definits valors diferents i, si no es proporciona el valor del paràmetre recheck_interval, s'utilitzarà un valor per defecte de 1440 minuts.

El valor de port per defecte de 42830 s'utilitza per al port `tncport` i el valor per defecte de 38240 s'utilitza per al port `pmserver`.

Referència relacionada:

"Ordre psconf" a la pàgina 179

Configuració de les opcions addicionals per al client de Trusted Network Connect

Informació sobre els passos per configurar el client de Trusted Network Connect (TNC) i els paràmetres de configuració necessaris per dur a terme la configuració.

Per configurar el client de TNC, cal que el fitxer `/etc/tnccs.conf` tingui un valor similar al següent:

```
component = CLIENT
```

Per configurar un sistema com a client, escriviu l'ordre següent:

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

Per exemple:

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

Nota: El valor del port del servidor i el valor de `tncport`, que és un port del client, han de coincidir.

Referència relacionada:

"Ordre psconf" a la pàgina 179

Configuració d'opcions per al servidor de gestió de pedaços del TNC

El servidor de Trusted Network Connect Patch Manager (TNCPM) s'integra amb SUMA i cURL per proporcionar una solució de gestió de pedaços completa.

S'ha d'haver configurat el servidor de TNCPM al servidor Network Installation Management (NIM) per tal de poder actualitzar els clients de TNC.

Per habilitar les descàrregues automàtiques de correccions provisionals i de l'IBM Security Advisory, podeu especificar un interval de correccions provisionals. Aquesta funció proporciona una notificació automàtica de les correccions de seguretat que s'acaben de publicar i dels identificadors CVE (Common Vulnerabilities and Exposures) associats. Es verifiquen tots els advertiment de seguretat i totes les correccions provisionals abans del registre amb el TNC. La clau pública de vulnerabilitat de l'IBM AIX, que és necessària per descarregar automàticament correccions provisionals, la trobareu disponible al seguretat de l'IBM AIX Security. Les descàrregues automàtiques de Service Pack i de correccions provisionals s'inhabiliten definint l'interval de descàrrega i l'interval de correcció provisional a 0.

També podeu actualitzar manualment el registre de Service Pack i de correccions provisionals. Per registrar manualment un advertiment de seguretat d'IBM juntament amb les corresponents correccions provisionals, escriviu l'ordre següent:

```
pmconf add -y <fitxer advertiment> -v <fitxer signatures>  -e <fitxer tar correccions provisionals>
```

Per registrar manualment una correcció provisional autònoma, escriviu l'ordre següent:

```
pmconf add -p <SP> -e <fitxer correccions provisionals>
```

Per registrar un nivell tecnològic nou i per descarregar el Service Pack més recent, escriviu l'ordre següent:

```
pmconf add -l <llista de NT>
```

Per descarregar un Service Pack que no sigui la versió més recent o per descarregar un nivell tecnològic que cal utilitzar per a la verificació i les actualitzacions de clients, escriviu l'ordre següent:

```
pmconf add -l <llista de NT> -d
pmconf add -s <llista de SP>
```

Per registrar un dipòsit de correccions de Service Pack o de nivells tecnològics que existeixi al sistema, escriviu l'ordre següent:

```
pmconf add -s <SP> -p <dipòsit_correccions_definit_usuari>
pmconf add -l <NT> -p <dipòsit_correccions_definit_usuari>
```

Per configurar un sistema perquè serveixi com a servidor de gestió de pedaços, escriviu l'ordre següent:

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

A continuació hi trobareu un exemple d'aquesta ordre:

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

El servidor de gestió de pedaços del TNC sempre admet la gestió dels APAR (Authorized Problem Analysis Reports - informes d'anàlisi de problemes autoritzats) de seguretat. Escriviu l'ordre següent per configurar la gestió de pedaços del TNC per tal que es puguin gestionar altres tipus d'APAR:

```
pmconf add -t <llista_tipus_APAR>
```

A l'exemple anterior, <llista_tipus_APAR> és una llista separada per comes que conté els tipus d'APAR següents:

- HIPER
- PE
- Millora

Per gestionar els dipòsits d'Open Packages (paquets oberts) del TNCPM escriviu una o més de les ordres següents:

```
pmconf add -o <nom paquet> -V <versió> -T [installp|rqm] -D <camí d'accés definit per l'usuari>
pmconf delete -o <nom paquet> -V <versió>
pmconf list -o <nom paquet> -V <versió>
pmconf list -O [-c] [-q]
```

Els Open Packages (paquets oberts) s'afegeixen en aquest directori predeterminat:

`/var/tnc/tncpm/dipòsit_correccions/packages`.

Camí d'accés definit per l'usuari = Ubicació del paquet al sistema

Per visualitzar la informació descriptiva adreçada a les correccions de seguretat d'un nivell de específic de Service Pack, sense aplicar les correccions al dipòsit, escriviu l'ordre següent:

```
 pmconf get -L -p <SP>
```

Per exemple:

```
pmconf get -L -p 7200-01-01
```

Per descarregar les correccions de seguretat d'un nivell específic de Service Pack, sense aplicar les correccions al dipòsit, escriviu l'ordre següent:

```
pmconf get -p <SP> -D <directori de baixades>
```

Nota: El *directori de baixades* ha d'existir abans d'executar aquesta ordre.

Per exemple:

```
pmconf get -p 7200-01-01 -D /tmp/ifixes_7200-01-01
```

El servidor de gestió de pedaços del TNC admet l'ordre **syslog** per descarregar actualitzacions de Service Pack, de nivell tecnològic i de client. El recurs és `user` i la prioritat és `info`. Un exemple seria `user.info`.

El servidor de gestió de pedaços del TNC també conserva un registre amb totes les actualitzacions de client al directori `/var/tnc/tncpm/log/update/<ip>/<marca horària>`.

Referència relacionada:

"Ordre psconf" a la pàgina 179

Informació relacionada:

Seguretat de l'AIX d'IBM

Configuració de la notificació per correu electrònic del servidor de Trusted Network Connect

Informació sobre el procediment per configurar la notificació per correu electrònic pel servidor de Trusted Network Connect (TNC).

El servidor de TNC visualitza el nivell de pedaç del client i si el servidor de TNC troba que el client no es compatible, envia un correu electrònic a l'administrador amb el resultat i el remei necessari.

Per configurar l'adreça de correu electrònic de l'administrador, escriviu l'ordre següent:

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

Per exemple:

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

A l'exemple anterior, el correu electrònic del grup d'IP *vayugrp1* i *vayugrp2* s'envia a l'adreça de correu electrònic abc@ibm.com.

Per enviar un correu electrònic a una adreça de correu electrònic global pel grup d'IP que no té assignada cap adreça de correu electrònic, escriviu l'ordre següent:

```
psconf add –e <adreça de correu>
```

Per exemple:

```
psconf add –e abc@ibm.com
```

A l'exemple anterior, si un grup d'IP no té assignada cap adreça de correu electrònic, el correu s'envia a l'adreça de correu electrònic abc@ibm.com. Funciona com a adreça de correu electrònic global.

Referència relacionada:

"Ordre psconf" a la pàgina 179

Configuració del remitidor d'IP al VIOS

Informació sobre com configurar el remitidor d'IP al servidor d'E/S virtual (VIOS) per iniciar la verificació de forma automàtica.

Nota: Heu de configurar l'extensió del kernel d'SVM al servidor d'E/S virtual (VIOS) abans de configurar el remitidor d'IP.

Per configurar el remitidor d'IP de TNC, el fitxer de configuració de `/etc/tnccs.conf` ha de tenir un paràmetre similar al següent `component = IPREF`.

Podeu configurar un sistema com a client escrivint l'ordre següent:

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

Per exemple:

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

El valor del port `tncserver` i el valor de `tncport`, que és un port del client, han de coincidir.

Configureu el remitidor d'IP del TNC al VIOS. Aquesta configuració al VIOS activa la verificació als clients que es connecten a la xarxa. Escriviu l'ordre següent per configurar el remitidor:

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

Per exemple:

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

Nota: El valor del port del servidor i el del port de TNC, que és un port del client, han de coincidir.

Referència relacionada:

"Ordre psconf" a la pàgina 179

Gestió dels components de Trusted Network Connect (TNC)

Informació sobre com gestionar Trusted Network Connect (TNC) per tal d'implementar tasques com ara l'addició de clients, polítiques, registres, resultats de verificacions, l'actualització de clients i certificats relacionats amb el TNC.

Visualització del registres del servidor de Trusted Network Connect

Informació sobre com veure els registres del servidor de Trusted Network Connect (TNC).

El servidor de TNC registra els resultats de verificació de tots els clients. Per veure el registre, executeu l'ordre **psconf**:

```
psconf list –H –i <ip |ALL>
```

Referència relacionada:

"Ordre psconf" a la pàgina 179

Creació de polítiques per al client de Trusted Network Connect

Informació sobre com definir polítiques relacionades amb el client de Trusted Network Connect (TNC).

La consola `psconf` proporciona la interfície que es necessita per gestionar les polítiques de TNC. Cada client o grup de clients es pot associar a una política.

Es poden crear les polítiques següents:

- Un grup d'IP (protocols d'Internet) conté diverses adreces d'IP de clients.
- Cada IP de client por pertànyer només a un grup.
- El grup d'IP està associat a un grup de polítiques.
- Un grup de polítiques conté diferents tipus de polítiques. Per exemple, la política del conjunt de fitxers que especifica quin ha de ser el nivell del sistema operatiu del client (es a dir, la versió, el nivell tecnològic i el Service Pack). Pot haver-hi diverses polítiques de conjunt de fitxers en un grup de polítiques i el client que fa referència a aquestes polítiques ha de tenir el nivell especificat mitjançant una de les polítiques de conjunt de fitxers.

Les ordres següents mostren com crear un grup d'IP, un grup de polítiques i polítiques de conjunts de fitxers.

Per crear un grup d'IP, escriviu l'ordre següent:

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

Per exemple:

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

Nota: Per un grup, com a mínim s'ha de proporcionar una IP. Les diverses IP s'han de separar amb comes.

Per crear una política de conjunt de fitxers, escriviu l'ordre següent:

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

Per exemple:

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

Nota: La informació de muntatge ha de tenir el format `<rel00-TL-sp>`.

Per crear una política i assignar un grup d'IP, escriviu l'ordre següent:

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

Per exemple:

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

Per assignar una política de conjunt de fitxers, escriviu l'ordre següent:

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

Per exemple:

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

Per afegir la política d'OpenPackage, escriviu l'ordre següent:

```
pconf add -O <grup_openpkg> <nom_openpkg:versió>
```

A continuació trobareu un exemple de com afegir una política d'OpenPackage:

```
psconf add –O opengrp2 openssl:1.0.1.516
```

Per assignar la política d'OpenPackage a Fspolicy, escriviu l'ordre següent:

```
psconf add -O opengrp2 fspolicy=fspolicy1
```

Nota: Si es proporcionen diverses polítiques de conjunt de fitxers, el sistema aplica la política que sigui més compatible amb el client. Per exemple, si el client té el nivell `6100-02-01` i indiqueu la política de conjunt de fitxers `7100-03-04` i `6100-02-03`, aleshores, s'aplicarà el nivell `6100-02-03` al client.

Referència relacionada:

"Ordre psconf" a la pàgina 179

Inici de la verificació del client de Trusted Network Connect

Informació sobre com verificar el client de Trusted Network Connect (TNC).

Utilitzeu un dels mètodes següents per a la verificació del client:

- Si el daemon del remitidor d'IP del servidor d'E/S virtual (VIOS) reenvia l'IP del client al servidor de TNC: el client de LPAR adquireix l'IP i intenta accedir a la xarxa. El daemon del remitidor d'IP del VIOS detecta l'adreça IP nova i la reenvia al servidor de TNC: el servidor de TNC inicia la verificació en rebre l'adreça IP nova.

- El servidor de TNC verifica periòdicament el client: l'administrador pot afegir les IP de client que s'han de verificar a la base de dades de polítiques de TNC. El servidor de TNC verifica els clients que hi ha a la base de dades. La reverificació es produeix automàticament a intervals regulars en referència al valor d'atribut `recheck_interval` que s'hagi especificat al fitxer de configuració `/etc/tnccs.conf`.
- L'administrador inicia la verificació del client manualment: l'administrador pot iniciar la verificació manualment per verificar si s'ha afegit un client a la xarxa executant l'ordre següent:

  ```
  pconf verify -i <ip>
  ```

Nota: Pels recursos que no estan connectats a un VIOS, els clients es poden verificar i actualitzar quan s'afegeixin manualment al servidor de TNC.

Referència relacionada:

"Ordre psconf" a la pàgina 179

Visualització dels resultats de verificació de Trusted Network Connect

Informació sobre el procediment per veure els resultats de verificació del client de Trusted Network Connect (TNC).

Per veure els resultats de verificació dels clients a la xarxa, escriviu l'ordre següent:

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

Aquesta ordre mostra tots els clients que tenen un estat **IGNORED**, **COMPLIANT** o **FAILED**.

- **IGNORED**: L'IP de client s'ignora a la llista d'IP (és a dir, el client pot estar exempt de verificació).
- **COMPLIANT**: El client ha passat la verificació (és a dir, el client és compatible amb la política).
- **FAILED**: El client no ha passat la verificació (és a dir, el client no és compatible amb la política i cal una acció d'administració).

Per determinar el motiu de l'error, executeu l'ordre **psconf** amb l'IP de client que ha fallat.

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

Referència relacionada:

"Ordre psconf" a la pàgina 179

Actualització del client de Trusted Network Connect

El servidor de Trusted Network Connect (TNC) verifica un client i actualitza la base de dades amb l'estat del client i el resultat de la verificació. L'administrador pot visualitzar els resultats i emprendre una acció per actualitzar el client.

Per actualitzar un client que es troba al nivell anterior, escriviu l'ordre següent:

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

Per exemple:

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

L'ordre **psconf** actualitza el client amb les instal•lacions de muntatge i dels APAR, si no s'han instal•lat.

Per actualitzar el client amb l'Open Packages:

```
psconf update -i <ip> -O opengrp2
```

Referència relacionada:

"Ordre psconf" a la pàgina 179

Gestió de les polítiques de gestió de pedaços

L'ordre **pmconf** s'utilitza per configurar les polítiques de gestió de pedaços.

Les polítiques de gestió de pedaços proporcionen informació com, per exemple, l'adreça IP del servidor de TNC i l'interval de temps per iniciar una actualització de SUMA.

Per gestionar la política de gestió de pedaços, escriviu l'ordre següent:

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

Per exemple:

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

Nota: Els ports `pmport` i `tncserver` han de ser diferents.

Referència relacionada:

"Ordre pmconf" a la pàgina 175

Importació de certificats de Trusted Network Connect

Informació sobre el procediment per importar un certificat i per transmetre dades de forma segura a la xarxa.

Els daemons de Trusted Network Connect (TNC) es comuniquen a través de canals xifrats habilitats mitjançant el protocol TLS (Transport Layer Security) o el protocol SSL (Secure Sockets Layer). Aquest daemon garanteix que les dades i les ordres que es transporten a la xarxa s'autentiquin i es protegeixin. Cada sistema té la seva pròpia clau i el seu propi certificat que es generen quan s'executa l'ordre d'inicialització dels components. Aquest procés és transparent per a l'administrador i requereix menys implicació per part seva. Quan es verifica un client per primera vegada, se n'importa el certificat a la base de dades del servidor. El certificat es marca com a no fiable d'entrada i l'administrador utilitza l'ordre **psconf** per veure i marcar els certificats com a fiables escrivint l'ordre:

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

Si l'administrador vol utilitzar una clau i un certificat diferents, l'ordre **psconf** proporciona la funció per importar la clau i el certificat.

Per importar el certificat des d'un servidor, escriviu l'ordre següent:

```
psconf import  -S -k <nom de fitxer de claus> -f <nom de fitxer>
```

Per importar el certificat des d'un client, escriviu l'ordre següent:

```
psconf import -C -k <nom de fitxer de claus> -f <nom de fitxer>
```

Referència relacionada:

"Ordre psconf" a la pàgina 179

Informes al servidor de TNC

El servidor de Trusted Network Connect (TNC) admet el format CSV (valors separats per comes) i el format de sortida de text per als informes sobre les vulnerabilitats i problemes comuns (CVE), l'IBM Security Advisory (advertiment de seguretat), les polítiques de seguretat del TNC, les esmenes de seguretat del client de TNC i els Service Pack i correccions provisionals que s'han registrat.

L'informe de CVE mostra tots els riscos i vulnerabilitats comuns per als Service Pack registrats. Per visualitzar els resultats d'aquest informe, escriviu l'ordre següent:

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

L'informe de l'IBM Security Advisory (advertiment de seguretat) mostra les vulnerabilitats de seguretat conegudes que hi ha al programari IBM instal•lat. Per visualitzar els resultats d'aquest informe, escriviu l'ordre següent:

```
psconf report -A <nom_advertiment>
```

L'informe de polítiques del servidor de TNC mostra les polítiques de seguretat que s'apliquen al servidor de TNC. Per visualitzar els resultats d'aquest informe, escriviu l'ordre següent:

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

L'informe d'esmenes del client de TNC mostra les correccions provisionals instal•lades i les que falten per al client de TNC. Per visualitzar els resultats d'aquest informe, escriviu l'ordre següent:

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

També podeu executar un informe que generi una llista de Service Pack registrats així com els APAR (informes d'anàlisi de programes autoritzats) i les correccions provisionals. Per visualitzar els resultats d'aquest informe, escriviu l'ordre següent:

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

Per visualitzar una llista dels paquets de codi obert registrats, escriviu l'ordre d'informe següent:

```
psconf report -O ALL -o TEXT
```

Referència relacionada:

"Ordre psconf" a la pàgina 179

Resolució de problemes amb Trusted Network Connect i la gestió de pedaços

Informació sobre les causes possibles de l'error i els passos per resoldre'l amb el TNC i el sistema de gestió de pedaços.

Per resoldre problemes amb el sistema TNC i el sistema de gestió de pedaços, verifiqueu els paràmetres de configuració que apareixen a la taula següent.

Taula 13. Resolució de problemes amb els paràmetres de configuració per als sistemes TNC i de gestió de pedaços

Problema	Solució
El servidor de TNC no s'inicia o no respon	Completeu el procediment següent: 1. Determineu si el daemon del servidor de TNC s'està executant escrivint l'ordre: `ps –eaf | grep tnccsd` 2. Si no s'està executant, suprimiu el fitxer `/var/tnc/.tncsock`. 3. Reinicieu el servidor. Si així no es resol el problema, comproveu al fitxer de configuració `/etc/tnccs.conf` l'entrada `component = SERVER` al servidor de TNC.
El servidor de gestió de pedaços del TNC no s'inicia o no respon	• Determineu si el daemon del servidor de gestió de pedaços del TNC s'està executant escrivint l'ordre següent: `ps –eaf | grep tncpmd` • Comproveu al fitxer de configuració `/etc/tnccs.conf` l'entrada `component = TNCPM` al servidor de gestió de pedaços del TNC.
El client de TNC no s'inicia o no respon	• Determineu si el daemon del client de TNC s'està executant escrivint l'ordre següent: `ps –eaf | grep tnccsd` • Comproveu al fitxer de configuració `/etc/tnccs.conf` l'entrada `component = CLIENT` al client de TNC.

Taula 13. Resolució de problemes amb els paràmetres de configuració per als sistemes TNC i de gestió de pedaços (continuació)

Problema	Solució
El remitidor d'IP de TNC no s'està executant al servidor d'E/S virtual (VIOS)	• Determineu si el daemon del remitidor de TNC s'està executant escrivint l'ordre següent: `ps –eaf | grep tnccsd` • Comproveu al fitxer de configuració `/etc/tnccs.conf` l'entrada `component = IPREF` al VIOS.
No es pot configurar cap sistema com a servidor i client de TNC	El servidor i el client de TNC no es poden executar simultàniament al mateix sistema.
Els daemons s'estan executant però no s'efectua la verificació	No es poden registrar els daemons dels missatges. Configureu el registre `level=info` al fitxer `/etc/tnccs.conf`. Podeu analitzar els missatges de registre.

Interfície gràfica d'usuari (GUI) del PowerSC

Aquesta secció descriu la Interfície gràfica d'usuari (GUI) del PowerSC d'IBM que inclou informació sobre com instal•lar, conservar i utilitzar la interfície.

La GUI del PowerSC d'IBM millora la usabilitat del producte PowerSC Standard Edition proporcionant una alternativa a la interacció de la línia d'ordres i del fitxer de registre. La GUI del PowerSC proporciona una consola de gestió centralitzada per a la visualització dels punts finals i dels seus estats; per a accions d'aplicar, desfer o comprovar els nivells de conformitat; agrupar sistemes per a l'aplicació de les accions de nivell de conformitat i visualitzar i personalitzar els perfils de configuració de conformitat.

La GUI del PowerSC també inclou la Supervisió de la integritat de fitxers (FIM - File Integrity Monitoring). La FIM inclou les funcions de Real Time Compliance (RTC) i d'execució fiable (TE). Mitjançant la GUI del PowerSC, podeu configurar la funció RTC i la TE, i veure esdeveniments en temps real. La GUI del PowerSC també proporciona prestacions d'edició i creació d'informes de perfils.

Conceptes del GUI del PowerSC

Abans d'utilitzar la GUI del PowerSC, hauríeu de conèixer els conceptes generals relacionats amb la seguretat i la detecció de punts finals.

Seguretat de la GUI del PowerSC

La GUI del PowerSC proporciona seguretat utilitzant la comunicació HTTPS bidireccional entre el servidor de la GUI del PowerSC i els agents de la GUI del PowerSC en cadascun dels punts finals de l'AIX.

El procés de conformitat de connexió TLS utilitza certificats disponibles tant en el servidor de la GUI del PowerSC com en els agents de la GUI del PowerSC. El procés de conformitat de connexió TLS admet l'autenticació única en ambdues direccions perquè tant l'agent de la GUI del PowerSC com el servidor de la GUI del PowerSC poden iniciar la comunicació. L'agent crea un nonce, que és un número aleatori, que s'envia al servidor de la GUI del PowerSC durant la primera connexió. El servidor de la GUI del PowerSC inclou aleshores aquest nonce en cada ordre que s'envia a aquest agent. El nonce en qüestió proporciona una altra capa de confirmació a l'agent del punt final que indica que s'està executant una ordre que s'ha originat des de l'autèntic servidor de la GUI del PowerSC. El punt final ha d'assegurar-se que l'origen de la trucada de servei web sigui fiable. El reconeixement inicial i el nonce en garanteixen la fiabilitat.

Tota comunicació entre els agents de la GUI del PowerSC i el servidor de la GUI del PowerSC es xifra mitjançant protocols i paquets de xifrat que són coherents amb els requisits de seguretat dels sistemes protegits. Actualment, el nivell de protocol és TLS 1.2. El servidor de la GUI del PowerSC interactua amb tots els agents de la GUI del PowerSC i amb tots els usuaris de la GUI del PowerSC. Per tant, el servidor de la GUI del PowerSC ha de tenir un certificat que sigui fiable per totes les connexions procedents de navegadors web de l'usuari. Per exemple, els certificats procedents d'una autoritat prou coneguda com ara Verisign o procedents d'una entitat certificadora de confiança interna.

Durant la instal•lació, el servidor de la GUI del PowerSC crea un certificat signat automàticament per al seu propi ús. Aquest certificat es pot utilitzar de forma indefinida però està destinada a l'ús temporal i es el pot substituir un certificat proporcionat per l'usuari amb un reconeixement ampli. La instal•lació del servidor de la GUI del PowerSC també crea un certificat de signatura que s'utilitza per signar tots els certificats de punt final.

El procés d'instal•lació crea automàticament un fitxer de magatzem de confiança per a cada punt final. El fitxer de magatzem de confiança és el mateix per a cada punt final i s'ha de copiar del servidor de la GUI del PowerSC en cada punt final. Aquesta combinació de certificats tant al servidor de la GUI del PowerSC com als punts finals proporciona un nivell elevat de seguretat de comunicació.

Es proporciona més control de seguretat si s'utilitza UNIX Groups. Qualsevol usuari com, per exemple, un usuari LDAP o un usuari local definit pel sistema operatiu, ha de ser membre d'un grup específic del UNIX per iniciar sessió a la GUI del PowerSC. L'administrador por canviar la pertinença a grup mitjançant l'ordre **pscuiserverctl**.

Després d'iniciar sessió, encara podeu patir restriccions al mode de només visualització. Podeu utilitzar la funció d'autorització d'usuari per dur a terme accions en punts finals que es controlen mitjançant la pertinença a grup UNIX. Per dur a terme qualsevol acció, heu de ser membre d'un grup UNIX que tingui permís per gestionar el punt final. Si us cal més informació, consulteu el tema Especificació dels grups que disposen d'accés.

Per defecte, qualsevol usuari que sigui membre del grup de seguretat pot gestionar cada punt final que estigui visible a la GUI del PowerSC. L'administrador del PowerSC por restringir l'accés de l'usuari al nivell de punt final individual mitjançant l'ordre **setGroups.sh**.

Hi ha un gran varietat d'ordres de configuració que només pot realitzar un usuari administratiu. En els exemples s'inclou la possibilitat de canviar els valors de correu electrònic globals o de crear un perfil nou. L'autoritat de l'usuari administratiu es defineix utilitzant grups UNIX i es pot configurar utilitzant l'ordre **pscuiserverctl**.

Com omplir el contingut del punt final en la pàgina de conformitat

El servidor de la GUI del PowerSC i l'agent de la GUI del PowerSC es comuniquen amb el punt final per tal de detectar-ne el nivell de conformitat.

En el moment de l'inici, i de forma intermitent fins que l'acció esdevingui satisfactòria, l'agent intenta iniciar el contacte amb el servidor de la GUI del PowerSC. Quan s'estableix el contacte, es du a terme un reconeixement de la seguretat de l'agent al servidor una vegada. Una vegada que s'ha negociat correctament el reconeixement de la seguretat de l'agent al servidor per primera vegada, el servidor crear un element de domini amb un identificador exclusiu (UID) per a la representació interna del punt final i passa l'UID al punt final. L'UID s'inclou després amb tota la comunicació de l'agent al servidor. Aquesta acció completa el procés de descobriment. El servidor de la GUI del PowerSC i el punt final poden comunicar-se de forma segura en qualsevol direcció.

Una vegada acabat el reconeixement del descobriment inicial, o després d'iniciar l'agent de la GUI del PowerSC, l'agent de la GUI del PowerSC intenta determinar la informació actual de l'estat de conformitat per a aquest punt final i actualitza el servidor de la GUI del PowerSC. L'existència del punt final i la informació actual de conformitat s'utilitza per omplir la pàgina d'estat de conformitat de la GUI del PowerSC. Si no es pot determinar la informació d'estat, l'entrada no està disponible a la pàgina d'estat de conformitat.

El servidor de la GUI del PowerSC conté una representació de tots els punts finals, que es creen automàticament com a resultat de la connexió i la comunicació inicials entre l'agent i el servidor. Com que els agents de punts finals realitzen un seguiment dels canvis en l'estat de conformitat del punt final, els canvis passen al servidor i es conserven. Tota la interacció d'usuari de la GUI del PowerSC amb un punt final es realitza a través del servidor de la GUI del PowerSC. La interfície d'usuari no interactua directament amb cap punt final ni cap agent de punt final.

Instal•lació del GUI del PowerSC

Els agents de la GUI del PowerSC i els components del servidor de la GUI del PowerSC s'instal•len durant la instal•lació del PowerSC Standard Edition. Cadascun s'instal•la des dels conjunts de fitxers `installp`.

Agent de la GUI del PowerSC

L'agent de la GUI del PowerSC s'instal•la en cada punt final de l'AIX. L'agent de la GUI del PowerSC fa un seguiment de l'activitat del punt final i proporciona aquesta informació al servidor de la GUI del PowerSC.

L'agent de la GUI del PowerSC també executa ordres que es poden activar des de la GUI del PowerSC. Tota comunicació entre els agents de la GUI del PowerSC i el servidor de la GUI del PowerSC es xifra.

L'ordre `installp` instal•la el nucli del producte PowerSC Standard Edition i l'agent de la GUI del PowerSC. El conjunt de fitxers `powerscStd.uiAgent.rte` `installp` s'utilitza per a la instal•lació de l'agent de la GUI del PowerSC. A l'exemple següent es mostra l'ordre `installp` que s'executa en cada punt final:

Nota: A l'exemple següent, les imatges de l'instal•lador s'expandeixen al directori `/tmp/inst.images/`.

```
#installp -agXYd /tmp/inst.images powerscStd.ice powerscStd.license powerscStd.uiAgent.rte
```

Servidor de la GUI del PowerSC

El servidor de la GUI del PowerSC es pot executar en qualsevol sistema AIX, es recomana que es crei una LPAR AIX dedicada en la que s'instal•li i s'executi el servidor de la GUI del PowerSC.

L'ordre **installp** instal•la el nucli del producte PowerSC Standard Edition i el servidor de la GUI del PowerSC. S'utilitza el conjunt de fitxers `powerscStd.uiServer.rte` **installp** per a la instal•lació del servidor de la GUI del PowerSC. L'exemple següent mostra l'ordre **installp** que s'executa en un punt final:

Nota: A l'exemple següent, les imatges de l'instal•lador s'expandeixen al directori `/tmp/inst.images/`.

```
#installp -agXYd /tmp/inst.images powerscStd.ice powerscStd.license powerscStd.uiServer.rte
```

Requeriments de la GUI del PowerSC

Infirmació sobre els requeriments del maquinari i del programari per la GUI del PowerSC.

Maquinari

- El servidor de la GUI del PowerSC hauria d'estar instal•lat en una LPAR o una VM independent que executi l'AIX 7.1 o posterior.
- Cal haver instal•lat els components de l'agent de la GUI del PowerSC en cada punt final de l'AIX.

Programari

- El servidor de la GUI del PowerSC requereix l'AIX 7.1 o posterior.
- El servidor de la GUI del PowerSC requereix que s'estigui executant el daemon sendmail.
- S'ha d'haver instal•lat el conjunt de fitxers `bos.loc.utf.<LANG>` perquè la GUI del PowerSC visualitzi correctament les descripcions de la regla de perfil en altres idiomes diferents de l'anglès.

Distribució del certificat de seguretat del magatzem de confiança als punts finals

Els administradors del sistema han de desplegar el certificat de seguretat del magatzem de confiança en tots els punts finals.

Durant la instal•lació, es crea un fitxer de magatzem de confiança i el poden utilitzar tots els punts finals. El nom del fiter és `endpointTruststore.jks`. El fiter es col•loca al directori `/etc/security/powersc/uiServer/`.

Després de la instal•lació, heu de col•locar el fitxer `endpointtruststore.jks` en cada punt final de l'agent de la GUI del PowerSC del mencionat punt final per posar-lo en contacte amb el servidor de la GUI del PowerSC i per iniciar el procés generat durant la creació del magatzem de claus al punt final.

Podeu distribuir el fitxer de magatzem de confiança d'una d'aquestes maneres:

- Copiant manualment el fiter `endpointTruststore.jks` en cada punt final.
- Si s'utilitza PowerVC (o un altre gestor de virtualització) al vostre entorn, el fitxer `endpointTruststore.jks` es pot posar a la imatge del PowerVC. Quan es desplega la imatge del PowerVC en un punt final, s'inclou l'agent de la GUI del PowerSC i el fitxer de magatzem de confiança.

Després de desplegar el fitxer `endpointTruststore.jks` utilitzant un dels mètodes següents, i quan es comença a executar un punt final, l'agent de la GUI del PowerSC utilitza el fitxer de magatzem de confiança per tal de determinar la ubicació en la que s'executa el servidor de la GUI del PowerSC. L'agent de la GUI del PowerSC envia aleshores un missatge al servidor de la GUI del PowerSC amb una sol•licitud per unir la llista de punts finals disponibles i supervisats.

Còpia manual del fitxer de magatzem de confiança en punts finals

Els administradors del sistema han de copiar manualment el fitxer de magatzem de confiança en cada punt final existent del seu entorn.

El fitxer de magatzem de confiança també s'ha de copiar en cada punt final nou que s'afegeixi.

Nota: Si disposeu d'un gestor de virtualització de dades com ara el PowerVC, podeu copiar el fitxer de magatzem de confiança en un punt final nou creant una imatge que conté tant l'agent de la GUI del PowerSC com el fitxer de magatzem de confiança. Consulteu "Còpia del fitxer de magatzem de confiança en punts finals utilitzant el gestor de virtualització".

1. Per copiar el magatzem de confiança de punt final `/etc/security/powersc/uiServer/endpointTruststore.jks` en el fitxer `/etc/security/powersc/uiAgent/endpointTruststore.jks` de cada punt final, executeu l'ordre **scp**:

   ```
   # scp endpointTruststore.jks user@endpoint-host-name:
                           /etc/security/powersc/uiAgent
   ```

2. Per reiniciar els agents de punt final després d'instal•lar el certificat de seguretat, executeu les ordres següents al punt final:

   ```
   stopsrc -s pscuiagent
   startsrc -s pscuiagent
   ```

3. Repetiu els passos 1 i 2 per a cada punt final existent i per cada punt final nou (si no disposeu de cap gestor de virtualització).

Còpia del fitxer de magatzem de confiança en punts finals utilitzant el gestor de virtualització

Els administradors del sistema poden utilitzar un gestor de virtualització com, per exemple, el PowerVC per copiar el fitxer de magatzem de confiança en cada punt final nou utilitzant una imatges que conté l'agent del PowerSC i el fitxer de magatzem de confiança.

1. Copieu el magatzem de confiança del punt final `/etc/security/powersc/uiServer/endpointTruststore.jks` en la imatge del PowerVC.
2. Desplegueu la imatge del PowerVC en cada punt final nou que s'afegeix al vostre sistema.

Configuració de comptes d'usuari

Per defecte, qualsevol usuari com, ja sigui un usuari LDAP o un usuari local definit pel sistema operatiu, ha de ser membre d'un grup per iniciar sessió a la GUI del PowerSC.

L'administrador pot canviar aquesta pertinença a grup necessària mitjançant l'ordre **pscuiserverctl**. Després d'iniciar sessió a la GUI del PowerSC, un usuari només pot veure l'estat dels punts finals si el compte d'usuari és un membre d'un grup UNIX que té permís per gestionar el punt final. L'administrador pot canviar els paràmetres del compte d'usuari per al nivell de punt final individual mitjançant l'ordre **setGroups.sh**.

Tingueu en compte els punts següents:

- Existeix una relació de molts a molts entre els punts finals i els grups AIX:
  - Un grup AIX es pot associar a molts punts finals.
  - Un punt final es pot associar a molts grups AIX.
- Una vegada l'usuari hagi iniciat sessió a la GUI del PowerSC, les associacions de grups s'utilitzen per determinar si un usuari té permís per executar ordres en punts finals específics o si l'usuari només pot veure l'estat dels punts finals.
  - Per executar ordres en un punt final específic mitjançant la GUI del PowerSC, l'usuari ha d'estar associat a un dels grups que estigui associat al punt final.
  - La pertinença de grup de l'usuari es compara amb el conjunt de grup que estan associats a cada punt final. Si la pertinença de grup de l'usuari coincideix amb els grups que estan associats a cada punt final, l'usuari podrà executar ordres com ara **Aplicar perfils**, **Desfer** i **Comprovar** en aquest punt final. Si la pertinença de grup de l'usuari no coincideix amb cap grup associat a cada punt final, l'usuari només pot veure l'estat d'aquest punt final.

Els següents scripts de l'intèrpret d'ordres estan disponibles al servidor de la GUI del PowerSC al directori `/opt/powersc/uiServer/bin/`.

Taula 14. Scripts de l'intèrpret d'ordres de grups

Script de l'intèrpret d'ordres	Descripció
`pscuiserverctl`	Especifica un grup d'inici de sessió AIX (UNIX) del qual l'usuari n'ha de ser membre per iniciar sessió a la GUI del PowerSC. L'usuari només ha de ser membre d'un dels grups.
`setGroups.sh`	Especifica un o diversos grups AIX del qual un usuari ha de ser membre per executar ordres en punts finals específics.

Execució de les ordres de configuració de grup i dels scripts

Els administradors del sistema han d'executar l'ordre **pscuiserverctl** i l'script **setGroups** per especificar quins grups del sistema operatiu es permeten per iniciar sessió a la GUI del PowerSC, han d'executar funcions d'administrador i han d'executar ordres en punts finals específics.

1. Al servidor de la GUI del PowerSC, canvieu el directori a `/opt/powersc/uiServer/bin/`.
2. Executeu l'ordre següent per especificar el grup de l'AIX al qual ha de pertànyer un usuari per iniciar sessió a la GUI del PowerSC. El grup que especifiqueu s'escriu al fitxer `/etc/security/powersc/uiServer/uiServer.conf`.

   ```
   pscuiserverctl set logonGroupList abp,security
   ```

   Consell: Abans d'executar l'ordre, podeu utilitzar l'ordre **groups** *username* per veure els grups dels quals l'usuari és membre.
3. Executeu l'ordre següent per especificar els grups del UNIX que disposen de permís per executar funcions d'administrador utilitzant la GUI del PowerSC.

   ```
   pscuiserverctl set administratorGroupList unixgrpadmin1,unixgrpadmin2
   ```

4. Executeu l'script següent per especificar els grups de l'AIX dels quals l'usuari n'ha de ser membre per executar ordres en punts finals específics. Heu de proporcionar noms d'amfitrions complets dels punts finals. Els grups que especifiqueu s'escriuen al fitxer `/etc/security/powersc/uiServer/groups.txt`.

   `./setGroups.sh` *`nom_grup "llista separada per comes de noms d'amfitrions de punt final"`*

   Nota: Els caràcters comodí limitats s'admeten quan es busquen punts finals. Per exemple, les especificacions següents són vàlides per especificar tots els punts finals que tenen un nom que comenci per "Boston_" o que acabi amb ".rs.com":

   - ./setGroups.sh groupname "Boston_*"
   - ./setGroups.sh groupname "*.rs.com"

   Consell: Un comodí (*) és l'únic caràcter comodí admès per aquesta ordre. Només es pot utilitzar al principi o al final d'una cadena.

Utilització de la GUI del PowerSC

Podeu utilitzar la GUI del PowerSC per veure els punts finals que s'han descobert al sistema, per crear grups personalitzats, per crear perfils personalitzats, per copiar perfils personalitzats en punts finals i per aplicar perfils. També podeu verificar la comunicació entre els punts finals i el servidor de la GUI del PowerSC i per aturar la comunicació entre un punt final i el servidor de la GUI del PowerSC.

La pàgina principal de la GUI del PowerSC conté les seccions següents:

- Safata de **Grups**: llista els grups que s'han definit al vostre entorn. Els grups són recopilació de punts finals que s'agrupen en funció dels punts en comú. El grup **Tots els sistemes** es crea automàticament quan es descobreixen els punts finals del vostre entorn. Podeu crear grups personalitzats. Per exemple, podeu crear un grup de punts finals que tinguin en comú el tipus HIPPA.
- La pàgina **Conformitat** inclou tres seccions:
  - El panell superior mostra informació estadística del grup que heu seleccionat de la safata **Grups**. La informació estadística mostra els resultats dels darrers nivells de conformitat que s'apliquen als punts finals del grup seleccionat. Pel grup seleccionat, podeu veure el percentatge d'aprovacions i d'errors del sistema, el nombre total de regles que s'han comprovat i les regles específiques que han fallat.
  - El panell central és una barra de tasques que es pot utilitzar per dur a terme accions en un punt final o més d'un. Podeu aplicar, desfer o comprovar un nivell de conformitat.
  - El panell inferior mostra una taula que inclou tots els punts finals o un grup de punts finals que estan disponibles al vostre entorn. La taula inclou la informació següent per a cada punt final:
    - Nom del sistema
    - Tipus de regla de conformitat
    - Hora i dia en què s'ha aplicat el nivell de conformitat al punt final
    - Hora i dia en què s'ha comprovat el nivell de conformitat al punt final
    - Estat de nivell de conformitat
    - Nombre de regles del punt final que han fallat
    - Nombre de regles del punt final que s'han aprovat correctament durant la comprovació del nivell de conformitat
- La pàgina **Seguretat** inclou dues seccions:
  - El panell superior mostra la informació de seguretat en temps real del grup de punts finals que heu seleccionat de la safata **Grups**. Pel grup seleccionat, podeu veure el nombre total d'esdeveniments en temps real (RTC), el nombre total d'esdeveniments d'execució fiable (TE), el percentatge de punts finals que estan actualitzats amb pedaços de TNC, el percentatge de punts finals que tenen instal•lada l'engegada fiable, el nombre de punts finals que tenen instal•lat el tallafoc fiable i el percentatge de punts finals que tenen instal•lat el registre fiable.

- El panell inferior mostra una taula que inclou els punts finals del sistema al grup. La taula inclou la informació següent per a cada punt final:
  - El nom del punt final del sistema
  - Els indicadors d'esdeveniments d'integritat
  - L'estat d'activació de l'RTC
  - L'estat d'activació del TE
  - L'estat dels pedaços de TNC actualitzats
- La pàgina **Informes** inclou informes d'integritat de conformitat i de fitxers. S'inclouen informes de visió general i de detalls.
- La pàgina **Editor de perfils** inclou tres seccions:
  - El panell superior té un menú desplegable que llista els perfils integrats i personalitzats que hi ha disponibles.
  - El panell central és una barra de tasques que es pot utilitzar per suprimir perfils, crear perfils nous i copiar perfils en punts finals que formen part d'un grup.
  - El panell inferior mostra una taula que inclou totes les regles que s'han inclòs al perfil seleccionat. Per a cada regla es mostra la informació següent:
    - Nom de regla de conformitat
    - Tipus de regla de conformitat
    - Descripció de la regla

Especificació de l'idioma de la GUI del PowerSC

La GUI del PowerSC es pot representar en diferents idiomes.

Per seleccionar l'idioma de la GUI del PowerSC, feu clic a la icona **Idiomes i paràmetres** de la barra de menú de la pàgina principal. Al menú es mostra l'idioma actual que s'utilitza per representar la interfície. Per canviar l'idioma, feu clic a la icona associada. Seleccioneu l'idioma de la vostra sessió de la llista d'idiomes disponibles.

Navegació per l'GUI del PowerSC

Des de la GUI del PowerSC podeu configurar i administrar la comunicació de punts finals i servidors, organitzar i agrupar punts finals, supervisar i aplicar nivells i perfils de conformitat integrats i personalitzats, supervisar i configurar la seguretat dels punts finals, i generar i distribuir informes en funció d'una planificació.

1. Obriu la GUI del PowerSC. La GUI del PowerSC mostra la pàgina d'inici.
2. Per administrar la comunicació de punts finals i servidors, feu clic a la icona **Idiomes i paràmetres** de la barra de menú de la pàgina principal. Feu clic a la icona **Administració de punt final** per verificar o per aturar la comunicació entre les punts finals i el servidor de la GUI del PowerSC. Per obtenir més informació, consulteu l'apartat “Administració de la comunicació de punts finals i servidors” a la pàgina 156.
3. Feu clic a l'el•lipsi de la línia horitzontal al panell de navegació de les pàgines de conformitat o de seguretat per obrir l'Editor de grups. Amb la utilització de l'Editor de grups podeu crear grups de punts finals personalitzats. Per obtenir més informació, consulteu l'apartat “Creació de grups personalitzats” a la pàgina 158.
4. Per crear perfils de conformitat personalitzats i copiar-los en punts finals, feu clic a la pestanya **Editor de perfils**. Per obtenir més informació, consulteu l'apartat “Com treballar amb perfils de conformitat” a la pàgina 159.
5. Per supervisar i aplicar els nivells i perfils de conformitat integrats i personalitzats, feu clic a la pestanya **Conformitat**. Per obtenir més informació, consulteu Aplicació dels nivells i perfils de conformitat.

6. Per supervisar i configurar la seguretat dels punts finals, feu clic a la pestanya **Seguretat**. Per obtenir més informació, consulteu Supervisió de la seguretat dels punts finals.
7. Per generar i distribuir informes sota petició basant-vos en una planificació, feu clic a la pestanya **Informes**. Per obtenir més informació, consulteu Com treballar amb informes.

Administració de la comunicació de punts finals i servidors

Des de la pàgina **Administració de punt final** podeu verificar o aturar la comunicació entre els punts finals i el servidor de la GUI del PowerSC. També podeu verificar i generar sol•licituds del magatzem de claus.

Verificació de la comunicació entre el punt final i el servidor

Podeu verificar la comunicació entre els punts finals descoberts i el servidor de la GUI del PowerSC.

1. Feu clic a la icona **Idiomes i paràmetres** de la barra de menú de la pàgina principal. Feu clic a **Administració de punt final**. S'obre la pàgina Administració de punt final.
2. Des de la safata **Grups**, seleccioneu el grup que inclogui els punts finals que vulgueu verificar. Els punts finals d'aquest grup es llistaran a la taula de punts finals.
3. Tots els punts finals del sistema d'un grup seleccionat es visualitzen a la taula de conformitat. Podeu filtrar els punts finals que es visualitzin mitjançant el camp **Filtrat per text**. Escriviu el text que voleu filtrar al camp i premeu Intro. La llista de punts finals del grup seleccionat es filtra de forma dinàmica per mostrar només les files que contenen el text que heu indicat.
4. Per renovar la informació d'estat visualitzada, feu clic a **Renova taula**.
5. Marqueu el quadre de selecció per a cada punt final que vulgueu verificar.
6. Feu clic a la icona **Verifica**.
7. Apareix un missatge de confirmació sobre la connexió vàlida a les columnes **Verificada** i **Diagnosi de connectivitat**.

Eliminació de punts finals de la supervisió de la GUI del PowerSC

Una vegada s'hagi detectat el punt final, se supervisa de forma continuada. Si s'elimina el punt final de l'entorn, també haureu d'eliminar-lo del servidor de la GUI del PowerSC.

Per eliminar els punts finals de la supervisió de la GUI del PowerSC perquè no se supervisin, seguiu aquests passos:

1. Feu clic a la icona **Idiomes i paràmetres** de la barra de menú de la pàgina principal. Feu clic a **Administració de punt final**. S'obre la pàgina Administració de punt final.
2. Des de la safata **Grups**, seleccioneu el grup que inclogui els punts finals que vulgueu eliminar. Els punts finals d'aquest grup es llistaran a la taula de punts finals.
3. Tots els punts finals del sistema d'un grup seleccionat es visualitzen a la taula de conformitat. Podeu filtrar els punts finals que es visualitzin mitjançant el camp **Filtrat per text**. Escriviu el text que voleu filtrar al camp i premeu Intro. La llista de punts finals del grup seleccionat es filtra de forma dinàmica per mostrar només les files que contenen el text que heu indicat.
4. Per renovar la informació d'estat visualitzada, feu clic a **Renova taula**.
5. Marqueu el quadre de selecció per a cada punt final que vulgueu deixar de supervisar.
6. Feu clic a la icona **Suprimeix**.
7. Es visualitza un missatge de confirmació sobre la supressió del punt final a les columnes **Marca horària verificada** i **Diagnosi de connectivitat**.

Verificació i generació de la sol•licitud del magatzem de claus

Per cada punt final heu de comprovar que la sol•licitud del magatzem de claus sigui vàlida i, si ho és, podeu generar un magatzem de claus pel punt final.

La primera vegada que es comença a executar un punt final, l'agent de la GUI del PowerSC utilitza el fitxer de magatzem de confiança per tal de determinar la ubicació on s'està executant el servidor de la GUI del PowerSC. L'agent de la GUI del PowerSC envia aleshores un missatges al servidor de la GUI del PowerSC amb una sol•licitud per unir la llista de punts finals supervisats i disponibles.

Mitjançant la pàgina **Administrador de punts finals Sol•licituds de magatzem de claus** podeu verificar que hi hagi una sol•licitud de magatzem de claus i si és vàlida, podeu generar un magatzem de claus pel punt final.

1. Feu clic a la icona **Idiomes i paràmetres** de la barra de menú de la pàgina principal. Feu clic a **Administració de punt final**. S'obre la pàgina d'administració **Punt final - Tots els sistemes**.
2. Tots els punts finals coneguts es llisten a la columna **Nom del sistema**. Feu clic a **Sol•licituds de magatzem de claus** per verificar si hi ha alguna sol•licitud de magatzem de claus pendent. S'obre la pàgina **Administrador de punts finals Sol•licituds de magatzem de claus**.
3. El magatzem de claus sol•licita que es faci un llistat de tots els servidors nous i afegits a la columna **Nom d'amfitrió**. Després de confirmar que voleu ampliar un magatzem de claus al punt final, marqueu el quadre de selecció del punt final i feu clic a **Verifica**.
4. El PowerVC du a terme la verificació. Especifiqueu l'ID d'usuari i la contrasenya a la finestra **Calen les credencials de PowerVC**. Feu clic a **D'acord**. Si no teniu cap PowerVC, salteu-vos aquest pas i aneu al següent.

   Nota: La verificació és el procés d'utilitzar les API d'Openstack per comprovar si el PowerVC està informat del punt final que s'acaba de declarar. Si no existeix el PowerVC a l'entorn d'usuari o si powervcKeystoneUrl no s'ha configurat correctament (mitjançant pscuiserverctl), aleshores, el PowerSC no podrà verificar el punt final.
5. Després de la verificació, es visualitza un missatge com a text contextual a la columna **Nom d'amfitrió**. El missatge confirma si el PowerVC reconeix el nou punt final. En funció de la informació del missatge, podeu triar generar el magatzem de claus.
6. Per generar el magatzem de claus, feu clic a **Genera magatzem de claus**. La fila del punt final a la taula parpelleja mentre es genera el magatzem de claus. Una vegada finalitzat, el valor de la columna **S'ha generat el magatzem de claus** canvia de **No** a **Sí**.

   Nota: Si no heu verificat el punt final utilitzant el PowerVC, es visualitzarà un missatge preguntant si voleu continuar amb la verificació. Feu clic a **Continua** si reconeixeu el punt final i si voleu generar el magatzem de claus.

   Pot ser que l'agent del PowerSC trigui uns quants minuts a descobrir que s'ha detectat el magatzem de claus. Després que l'agent instal•li el magatzem de claus, el nou punt final es llista com a punt final totalment gestionat a les pàgines **Administració de punt final - tots els sistemes**, **Conformitat**, **Seguretat** i **Informes** de la GUI del PowerSC.
7. Si no voleu generar cap magatzem de claus pel punt final, podeu eliminar la sol•licitud. Marqueu el punt final al quadre de selecció que vulgueu eliminar i polseu la icona **Suprimeix**.
8. Tots els punts finals que esperen la verificació del magatzem de claus es visualitzen a la taula de punts finals. Podeu filtrar els punts finals que es visualitzin mitjançant el camp **Filtrat per text**. Escriviu el tet que vulgueu filtrar al camp i premeu **Intro**. La llista de punts finals es filtra de forma dinàmica per mostrar només les files que contenen el text que heu indicat.
9. Per renovar la informació de la taula de punt final, feu clic a **Renova taula**.

Organització i agrupació de punts finals

Els administradors del sistema poden organitzar i agrupar punts finals basant-se en certes propietats comuns. Els grups personalitzats es poden definir i poden contenir un conjunt de punts finals seleccionats de forma explícita que es gestionen utilitzant la GUI del PowerSC.

Per exemple, si teniu 3 o 4 entorns, potser voleu crear grups que continguin punts finals de producció, punts finals de prova i punts finals de garantia de qualitat.

durant la instal•lació es crea un grup per defecte que s'anomena **Tots els sistemes**. Aquest grup conté tots els punts finals que s'han descobert al vostre entorn.

Creació de grups personalitzats

Podeu crear un grup personalitzat amb una llista de punts final enumerada i explícitament seleccionada.

1. Des de la safata **Grups** seleccioneu **Crea grup nou**. S'obre la safata **Creació d'un grup nou**. Si no s'ha ampliat la safata **Grups**, feu clic a l'el•lipsi de la línia horitzontal al panell de l'esquerra de la pàgina principal de la interfície.
2. Escriviu un nom únic pel nou grup i premeu Intro. El nou grup s'afegeix a la safata **Grups**.
3. Afegiu els sistemes que voleu incloure en aquest grup. Des de la llista **Tots els sistemes** dels punts finals disponibles, seleccioneu els sistemes que vulgueu incloure al grup. Feu clic a la fletxa de la dreta per moure tots els sistemes seleccionats al grup nou. Per eliminar sistemes de punts final del grup, ressalteu el punt final de la nova llista de grups i feu clic a la fletxa de l'esquerra.
4. Després d'afegir o eliminar membres de grups, deseu els canvis fent clic a la icona **Desa** a la barra de menú del panell de contingut.
5. Feu clic a l'el•lipsi de la línia horitzontal per tornar a la safata **Grups**. Es llista el nou grup.

Addició o eliminació de sistemes assignats a un grup existent

Podeu afegir o eliminar punts finals que s'hagin assignat a un grup existent.

1. Des de la safata **Grups**, feu clic a l'el•lipsi de la dreta del grup al qual vulgueu afegir un sistema de punts finals o del quan vulgueu eliminar un sistema de punts finals. Si no s'ha ampliat la safata **Grups**, feu clic a l'el•lipsi de la línia horitzontal al panell de l'esquerra de la pàgina principal de la interfície.
2. Feu clic a **Edita grup**.
3. Per afegir un sistema de punts finals al grup, seleccioneu el sistema de la llista **Tots els sistemes** i feu clic a la fletxa de la dreta. El sistema s'afegix a la llista *Nom de grup*.
4. Per eliminar un punt final del grup, seleccioneu el sistema de la llista **Sistemes de grups** i feu clic a la fletxa de l'esquerra. El sistema s'elimina de la llista *Nom de grup*.
5. Feu clic a la icona **Desa canvis de grup** per desar els canvis.
6. Per suprimir un sistema del grup, seleccioneu el sistema i feu clic a la fletxa de l'esquerra.
7. Per cancel•lar els canvis al grup, feu clic a **Cancel•la canvis de grup**
8. Feu clic a l'el•lipsi **Grups** per tornar a la safata **Grups**.

Supressió d'un grup

Podeu suprimir grups que ja no siguin aplicables.

1. Des de la safata **Grups**, feu clic a l'el•lipsi de la dreta del grup que voleu suprimir. Si la safata **Grups** no s'amplia, feu clic a l'el•lipsi de la línia horitzontal al panell de navegació de la pàgina principal de la interfície.
2. Feu clic a **Elimina grup**. El grup s'elimina i se suprimeix de la llista de grups de la safata **Grups**.

Canvi de nom d'un grup

Podeu canviar el nom d'un grup de punts finals.

1. Des de la safata **Grups**, feu clic a l'el•lipsi de la dreta del grup del qual voleu canviar el nom. Si la safata **Grups** no s'amplia, feu clic a l'el•lipsi de la línia horitzontal al panell de navegació de la pàgina principal de la interfície.
2. Feu clic a **Canvia el nom del grup**. Especifiqueu el nom nou del grup al camp **Nom del grup**.

Clonació d'un grup

Podeu clonar un grup per crear un duplicat amb els mateixos punts finals i un nom nou.

1. Des de la safata **Grups**, feu clic a l'el•lipsi de la dreta del grup que voleu suprimir. Si la safata **Grups** no s'amplia, feu clic a l'el•lipsi de la línia horitzontal al panell de navegació de la pàgina principal de la interfície.
2. Feu clic a **Clona grup**. El grup es copia i s'assigna un nom nou.

Com treballar amb perfils de conformitat

Mitjançant l'Editor de perfils de la GUI del PowerSC, podeu veure els perfils de conformitat integrats, crear perfils personalitzats i copiar perfils als punts finals del sistema.

El producte PowerSC Standard Edition se subministra amb un conjunt de perfils integrats que es poden utilitzar per configurar els punts finals del vostre sistema de forma que cada punt final compleixi els següents estàndards de seguretat:

- Normativa de seguretat de la informació en la indústria de mitjans de pagament (PCI)
- Conformitat amb la llei Sarbanes-Oxley i el COBIT (SOX/COBIT)
- Conformitat amb la STIG del departament de defensa dels Estats Units (DoD)
- Llei de responsabilitat i portabilitat de l'assegurança mèdica (HIPAA)
- Conformitat amb la North American Electric Reliability Corporation (NERC)

Si voleu més informació sobre els perfils integrats, consulteu el tema "Conceptes de l'automatització de seguretat i de conformitat" a la pàgina 9.

Cadascun dels perfils integrats inclou regles que s'han d'aplicar a un punt final per complir els requeriments de seguretat. Quan calgui aplicar només un subconjunt o una combinació diferent d'aquestes regles, o personalitzar els nivells de conformitat, podeu crear un perfil personalitzat.

En la majoria d'entorns, els administradors solen editar els fitxers de conformitat per eliminar les regles que presenten problemes. Després d'efectuar comprovacions de compatibilitat, es considera que els fitxers de regles de conformitat són estables i es despleguen en els servidors de producció.

La GUI del PowerSC es pot utilitzar per crear perfils personalitzats combinant regles a partir dels perfils incorporats (o altres de personalitzats).

Visualització dels perfils de conformitat

Podeu veure les regles que s'inclouen en cadascun dels perfils integrats i personalitzats.

1. Des de la pàgina principal, seleccioneu la pestanya **Editor de perfils**. S'obre la pàgina **Editor de perfils**.
2. Feu clic a la fletxa cap avall per obrir la llista de perfils. Al menú desplegable es llisten els **Perfils integrats** i els **Perfils personalitzats** que hi ha disponibles.
3. Seleccioneu el perfil que vulgueu veure. Cada regla inclosa al perfil es visualitza amb el nom, el tipus i una descripció. Si voleu més informació sobre les regles, consulteu el tema "Conceptes de l'automatització de seguretat i de conformitat" a la pàgina 9.
4. Totes les regles del perfil seleccionat es mostraran a la taula de perfils. Podeu filtrar els perfils que se mostren utilitzant el requadre **Filtrat per text**. Escriviu al quadre de text el text amb el que vulgueu filtrar. S'actualitza la llista de regles del perfil seleccionat.

Creació d'un perfil personalitzat

Podeu crear un perfil nou que es basi en un perfil existent i, aleshores, personalitzar el perfil nou perquè inclogui només un conjunt de regles específiques.

1. Des de la pàgina principal, seleccioneu la pestanya **Editor de perfils**. S'obre la pàgina **Editor de perfils**.
2. Feu clic a la fletxa cap avall per obrir la llista de perfils. Al menú desplegable es llisten els **Perfils integrats** i els **Perfils personalitzats** que hi ha disponibles.
3. Seleccioneu el perfil en el que voleu que es basi el perfil nou.
4. Feu clic a la icona **Crea perfil nou**. S'obre la finestra Nou nom i tipus de perfil.
5. Escriviu el nom del perfil nou al camp **Nom de perfil**.
6. Escriviu el tipus al camp **Tipus de perfil**. El tipus que escriviu sol indicar el tipus de política integrada en la que es basa el perfil nou a més d'un identificador exclusiu. Per exemple PCIxx, SOX-COBITxy, DoDxyz, HIPAAwxyz o NERCabc.
7. Feu clic a **Confirma**.
8. Per afegir una regla al perfil personalitzat, seleccioneu la regla del perfil original en el que es basa el perfil personalitzat i feu clic a la fletxa a la dreta. La regla s'afegeix al nou perfil personalitzat. Repetiu aquesta acció per a cada regla que vulgueu incloure.
9. Per eliminar una regla del perfil personalitzat, seleccioneu la regla del perfil personalitzat i feu clic a la fletxa a l'esquerra. La regla s'elimina del nou perfil personalitzat. Repetiu l'acció per a cada regla que vulgueu eliminar.
10. Feu clic a **Desa** quan hàgiu acabat d'afegir les regles.

Còpia de perfils en membres de grups

Podeu copiar els perfils personalitzats en un grup de punts finals. Després de copiar el perfil personalitzat al punt final, està disponible per l'aplicació al punt final. També està disponible per a comprovar si la verificació es pot aplicar al punt final sense errors.

1. Des de la pàgina principal, seleccioneu la pestanya **Editor de perfils**. S'obre la pàgina **Editor de perfils**.
2. Feu clic a la fletxa cap avall per obrir la llista de perfils. Al menú desplegable es llisten els **Perfils integrats** i els **Perfils personalitzats** que hi ha disponibles.
3. Seleccioneu el perfil que vulgueu copiar als membres d'un grup.
4. Feu clic a la icona **Copia perfil als membres del grup**. S'obre la finestra **Copia *nom de perfil* en**.
5. Cada grup que s'hagi creat per a l'organització apareixerà llistat amb un quadre de selecció associat. Marqueu el quadre de selecció per a cada grup on vulgueu copiar el perfil seleccionat.
6. Feu clic a **Copia**.
7. Per aplicar o comprovar el perfil, torneu a la pàgina **Conformitat** seleccionant la pestanya **Conformitat**.

Supressió d'un perfil personalitzat

Podeu suprimir els perfils personalitzats

1. Des de la pàgina principal, seleccioneu la pestanya **Editor de perfils**. S'obre la pàgina **Editor de perfils**.
2. Feu clic a la fletxa cap avall per obrir la llista de perfils. Al menú desplegable es llisten els **Perfils integrats** i els **Perfils personalitzats** que hi ha disponibles.
3. Expandiu la llista **Perfils personalitzats**.
4. Seleccioneu el perfil que vulgueu suprimir.
5. Feu clic a la icona **Suprimeix perfil**. Se suprimeix el perfil personalitzat que seleccioneu.

Administració dels nivells i perfils de conformitat

Els administradors del sistema poden aplica, comprovar o desfer els nivells i els perfils de conformitat integrats o personalitzats en diversos punts finals.

A la taula següent es llisten els perfils predefinits i els nivells de conformitat que admet el PowerSC Standard Edition.

Taula 15. Perfils predefinits i nivells de conformitat que admet el PowerSC Standard Edition

Perfils	**Nivells**
Base de dades	Baix
DoD	Mitjà
DoD_to_AIXDefault	Alt
DoDv2	Per defecte
DoDv2_to_AIXDefault	
HIPAA	
NERC	
NERC_to_AIXDefault	
NERCv5	
NERCv5_to_AIXDefault	
PCI	
PCI_to_AIXDefault	
PCIv3	
PCIv3_to_AIXDefault	
SOX-COBIT	

Des de la pàgina **Conformitat** de la GUI del PowerSC, podeu dur a terme les tasques següents:

- Seleccioneu i apliqueu un perfil o nivell definit a un dels diversos punts finals.
- Activeu una operació de desfer en un dels diversos punts finals.
- Comproveu un perfil o nivell definit respecte de l'estat actual d'un punt final o de diversos punts finals. L'operació de comprovació no provoca canvis en el punt final però defineix el valor **Marca horària comprovada** per indicar quan s'ha dut a terme la darrera comprovació.

Aplicació dels nivells i perfils de conformitat

Podeu aplicar un nivell o un perfil de conformitat a un o diversos punts finals d'un grup seleccionat.

1. Des de la pàgina principal, seleccioneu la pestanya **Conformitat**. S'obre la pàgina **Conformitat**.
2. Des de la safata **Grups**, seleccioneu el grup que inclogui els punts finals on voleu aplicar els nivells i els perfils de conformitat.
3. Tots els punts finals del sistema d'un grup seleccionat es visualitzen a la taula de conformitat. Podeu filtrar els punts finals que es visualitzin mitjançant el quadre de text **Filtrat per text**. Escriviu el text que voleu filtrar al quadre de text i premeu Intro. La llista de punts finals del grup seleccionat es filtra de forma dinàmica per mostrar només les files que contenen el text que heu indicat.
4. Per renovar la informació d'estat visualitzada, feu clic a **Renova taula**. Per definir la freqüència en que es renova la visualització de forma automàtica, feu clic a **Interval de renovació**.
5. Des de la columna **Tipus de regla de conformitat**, podeu veure els nivells i els perfils que s'han copiat al punt final associat. Seleccioneu el nivell o el perfil que vulgueu aplicar al punt final. Marqueu el quadre de selecció associat.
6. Repetiu el pas 5 per a cada punt final del grup en el que vulgueu aplicar els nivells i els perfils de conformitat.
7. Feu clic a la icona **Aplica perfils**.
8. Els nivells i perfils de conformitat seleccionats s'apliquen a cadascun dels punts finals seleccionats. Si hi ha una regla o més d'una que no es pot aplicar, es considera que ha fallat. Si falla una regla o més d'una, el punt final se senyala amb una barra vermella i es mostra el text **Error** a la columna **Nombre de regles fallides**.

9. Des de la columna **Nombre de regles fallides** de cada punt final senyalat podeu veure el motiu pel qual ha fallat la regla. Podeu ajustar les regles que s'apliquen creant un perfil personalitzat o editant un perfil personalitzat.

Com desfer els nivells de conformitat

Podeu desfer el nivell o el perfil de conformitat que s'ha aplicat en un punt final o diversos punts finals d'un grup seleccionat.

Per desfer els nivells de conformitat, seguiu aquests passos:

1. Des de la pàgina principal, seleccioneu la pestanya **Conformitat**. S'obre la pàgina **Conformitat**.
2. Des de la safata **Grups**, seleccioneu el grup que inclogui els punts finals dels que voleu desfer els nivells i els perfils de conformitat.
3. Tots els punts finals d'un grup seleccionat es visualitzen a la taula de conformitat. Podeu filtrar els punts finals que es visualitzin mitjançant el quadre de text **Filtrat per text**. Escriviu el text que voleu filtrar al quadre de text i premeu Intro. La llista de punts finals del grup seleccionat es filtra de forma dinàmica per mostrar només les files que contenen el text que heu indicat.
4. Per renovar la informació d'estat visualitzada, feu clic a **Renova taula**. Per definir la freqüència en que es renova la visualització de forma automàtica, feu clic a **Interval de renovació**.
5. Per desfer un nivell o un perfil que s'ha aplicat a un punt final:
   a. Marqueu el quadre de selecció del punt final.
   b. Feu clic a la icona **Desfés**.

Comprovació del nivell i del perfil de conformitat més recents

Podeu comprovar el nivell o el perfil de conformitat més recent que s'aplica a un punt final o diversos punts finals d'un grup seleccionat.

1. Des de la pàgina principal, seleccioneu la pestanya **Conformitat**. S'obre la pàgina **Conformitat**.
2. Des de la safata **Grups**, seleccioneu el grup que inclogui els punts finals dels que voleu comprovar els nivells i els perfils de conformitat.
3. Tots els punts finals d'un grup seleccionat es visualitzen a la taula de conformitat. Podeu filtrar els punts finals que es visualitzin mitjançant el quadre de text **Filtrat per text**. Escriviu el text que voleu filtrar al quadre de text i premeu Intro. La llista de punts finals del grup seleccionat es filtra de forma dinàmica per mostrar només les files que contenen el text que heu indicat.
4. Per renovar la informació d'estat visualitzada, feu clic a **Renova taula**. Per definir la freqüència en que es renova la visualització de forma automàtica, feu clic a **Interval de renovació**.
5. Marqueu al quadre de selecció associat el nom del sistema del punt final del que vulgueu comprovar el nivell o el perfil més recent que s'hagi aplicat.
6. Repetiu el pas 5 a la pàgina 161 per a cada punt final del grup del que vulgueu comprovar els nivells i els perfils de conformitat.
7. Feu clic a la icona **Comprova**.
8. El punt final es comprova per veure si s'han aplicat les regles que hi ha al nivell o al perfil de conformitat. Els punts finals no s'actualitzen. Si no es pot aplicar alguna regla, es considera que ha falla quan s'ha aplicat. Si falla una regla o més d'una, el punt final se senyala amb una barra vermella i es mostra el text **Error** a la columna **Nombre de regles fallides**.
9. Des de la llista **Nombre de regles fallides** de cada punt final senyalat, podeu veure el missatge que indica el motiu pel qual ha fallat la regla. Podeu ajustar les regles que s'apliquen creant un perfil personalitzat.

Comprovació que no s'ha aplicat un nivell o un perfil de conformitat

Podeu comprovar el nivell o el perfil de conformitat que no s'ha aplicat a un punt final o diversos punts finals d'un grup seleccionat.

1. Des de la pàgina principal, seleccioneu la pestanya **Conformitat**. S'obre la pàgina **Conformitat**.
2. Des de la safata **Grups**, seleccione el grup que inclou els punts finals dels quals voleu comprovar l'efecte d'un nivell o perfil de conformitat.
3. Tots els punts finals d'un grup seleccionat es visualitzen a la taula de conformitat. Podeu filtrar els punts finals que es visualitzin mitjançant el quadre de text **Filtrat per text**. Escriviu el text que voleu filtrar al quadre de text i premeu Intro. La llista de punts finals del grup seleccionat es filtra de forma dinàmica per mostrar només les files que contenen el text que heu indicat.
4. Per renovar la informació d'estat visualitzada, feu clic a **Renova taula**. Per definir la freqüència en que es renova la visualització de forma automàtica, feu clic a **Interval de renovació**.
5. Marqueu al quadre de selecció associat el nom del sistema del punt final del que vulgueu comprovar el nivell o el perfil més recent que s'hagi aplicat. Podeu seleccionar més d'un punt final.
6. Obriu la llista desplegable **Darrer tipus comprovat**. Seleccioneu una de les opcions següents:
   - **Tots els nivell disponibles** mostra una llista de tots els nivells disponibles que podeu comprovar en un punt final.
   - **Tots els perfils disponibles** mostra una llista de tots els perfils disponibles que podeu comprovar en un punt final.
7. Seleccioneu el nivell o el perfil que voleu comprovar respecte d'un punt final.
8. Feu clic a la icona **Comprova**. Els resultats de la comprovació es torne i apareixen sota el punt final.

Enviament de notificacions per correu electrònic quan es produeix un esdeveniment de conformitat

Des de la pàgina Conformitat, podeu enviar una notificació per correu electrònic a un destinatari, o a més d'un, quan es produeix un esdeveniment de conformitat.

1. Des de la pàgina principal, seleccioneu la pestanya **Conformitat**. S'obre la pàgina **Conformitat**.
2. Feu clic a la icona **Paràmetres de correu electrònic** a la part superior dreta de la barra de menú. S'obre la finestra **Paràmetres de correu electrònic**.
3. Marqueu el quadre de selecció **Envieu-me correus electrònics**.
4. Escriviu les adreces de correu electrònic de cada destinatari separades per comes al camp **Adreces (separades per comes)**.

Supervisió de la seguretat de punts finals

Des de la pàgina **Seguretat**, podeu supervisar la seguretat de punts finals en temps real.

A la pàgina Seguretat es visualitza l'estat dels punts finals que supervisa Real Time Compliance (RTC) i l'execució fiable (TE).

Tant l'RTC, un subcomponent del PowerSC, com la TE, un component de l'AIX, representen la supervisió de la integritat de fitxers (FIM - File Integrity Monitoring). La FIM supervisa els canvis en fitxers importats per tal de garantir que els esdeveniment que impacten als fitxers disposin d'autorització. Els esdeveniments que poden impactar en la seguretat inclouen informació si canvia el permís a un fitxer de forma inesperada, si s'actualitza el contingut d'un fitxer o si s'instal•la una aplicació no planificada. Heu de reconèixer aquests esdeveniment per protegir fitxers i aplicacions importants.

La pàgina **Seguretat** es la pàgina de supervisió en temps real de la GUI del PowerSC. Mostra els esdeveniments que es generen quan canvien els fitxers que supervisa l'RTE o la TE. Els esdeveniments inclouen els detalls sobre quan s'ha modificat el contingut del fitxer, quan s'ha accedit al punt final o quan s'han canviat la configuració.

Podeu utilitzar la pàgina **Seguretat** per realitzar les tasques següents:

- Visualitzar la informació de supervisió de l'RTC i la TE

- Configurar l'RTC i la TE per als punts finals
- Visualitzar l'estat d'altres productes i punts finals del PowerSC
- Commutar per activar i desactivar la TE

Configuració de Real Time Compliance (RTC)

Des de la pàgina **Seguretat** podeu configurar el producte Real Time Compliance (RTC) per a un punt final específic o un grup de punts finals específic.

1. Feu clic a l'el•lipsi de la dreta del punt final del qual voleu editar la configuració de l'RTC.
2. Feu clic a **Configura RTC**. S'obre la finestra Configuració de les polítiques d'RTC
3. Es llisten totes les opcions de configuració de l'RTC disponibles amb una explicació. Per canviar una o diverses opcions de configuració de l'RTC, marqueu o desmarqueu el quadre de selecció de l'esquerra de l'opció. En alguns casos, els canvis a les opcions no s'implementen fins que es reinicia el servidor.
4. Feu clic a **Desa**.

Restauració de les opcions de configuració de Real Time Compliance (RTC) en una data i hora anteriors

Podeu restaurar la configuració de l'RTC en una data i hora anteriors.

1. Feu clic a l'el•lipsi de la dreta del punt final del qual voleu retrocedir les opcions de configuració de l'RTC a una versió anterior.
2. Feu clic a **Desfés RTC**. Es llisten les marques horàries de cada versió de configuració de l'RTC.
3. Feu clic a la marca horària de la versió de configuració que vulgueu retrocedir. Es restauren les opcions de configuració de l'RTC que hi havia en lloc de la data i hora actuals.

Còpia de les opcions de configuració de Real Time Compliance (RTC) en altres grups

Podeu copiar les opcions de configuració de l'RTC en un altre grup de punts finals o en un conjunt específic de punts finals.

1. Feu clic a l'el•lipsi que hi ha a la dreta del punt final del qual en voleu copiar les opcions de configuració en un altre grup de punts finals o en un conjunt específic de punts finals.
2. Feu clic a **Còpia de la configuració de l'RTC**. Es mostra una llista de cada grup de punts finals inclosos al grup **Tots els sistemes**.
3. Seleccioneu el grup o els punts finals específics d'alguna d'aquestes maneres:
   - Marqueu el quadre de selecció del grup de punts finals de la llista de grups disponibles. Les opcions de configuració es copien en cada punt final del grup.
   - Utilitzeu la fletxa a la dreta per expandir un grup per tal de veure una llista de tots els punts finals del grup. Marqueu el quadre de selecció per a cada punt final del grup en el qual voleu copiar les opcions de configuració.
   - Expandiu la llista de punts finals al grup **Tots els sistemes**. Marqueu el quadre de selecció per a cada punt final del grup en el que voleu copiar els punts finals.
4. Feu clic a **D'acord**. Les opcions de configuració es copien en el grup seleccionat o en els punts finals seleccionats.

Edició de la llista de fitxers de Real Time Compliance (RTC)

Podeu veure i editar les opcions de supervisió de l'RTC per a cada fitxer en un punt final.

1. Feu clic a l'el•lipsi de la dreta del punt final que allotja els fitxers les opcions de supervisió de l'RTC dels quals voleu veure o editar.
2. Feu clic a **Edita la llista de fitxers d'RTC**. S'obre la pàgina **Configuració de la llista de fitxers d'RTC** i apareixen tots els directoris i fitxers que hi ha al punt final. Una marca de comprovació a la icona de la carpeta del directori indica que s'està supervisant un fitxer, o més d'un, d'aquest directori.

3. Si el fitxer, les opcions del qual voleu editar, està en un directori, feu doble clic al directori per llistar els fitxers. Es llisten tots els fitxers del directori.
4. Les opcions de supervisió de cada fitxer al punt final es llisten a les columnes **Contingut** i **Atributs**. Si es supervisen els canvis al fitxer, està marcada la columna **Contingut** del quadre de selecció. Si es supervisen els canvis d'atribut al fitxer, està marcada la columna **Atributs** del quadre de selecció. Per editar les opcions de supervisió, marqueu o desmarqueu els quadres de selecció d'un fitxer, o més d'un al punt final.
5. Feu clic a **Desa**.

Restauració de les opcions de supervisió de fitxers de Real Time Compliance (RTC) en una configuració anterior

Podeu retrocedir a una versió anterior dels fitxers que l'RTC està supervisant.

1. Feu clic a l'el•lipsi de la dreta del punt final del qual voleu retrocedir les opcions de supervisió de fitxers de l'RTC a una versió anterior.
2. Feu clic a **Desfés la llista de fitxers d'RTC**. Es llisten les marques horàries de cada versió de configuració dels fitxers supervisats.
3. Feu clic a la marca horària de la versió de configuració de les opcions de supervisió que vulgueu retrocedir. Es restauren les opcions de configuració que hi havia en lloc de la data i hora actuals.

Còpia de les opcions de supervisió de la llista de fitxers de Real Time Compliance (RTC) en altres grups

Podeu copiar les opcions de supervisió de fitxers de l'RTC en un altre grup de punts finals o en un conjunt específic de punts finals.

1. Feu clic a l'el•lipsi que hi ha a la dreta del punt final del qual voleu copiar les opcions de supervisió en un altre grup de punts finals o en un conjunt específic de punts finals.
2. Feu clic a **Copia la llista de fitxers d'RTC**. Es mostra una llista de cada grup de punts finals inclosos al grup **Tots els sistemes**.
3. Seleccioneu el grup o els punts finals específics d'alguna d'aquestes maneres:
   - Marqueu el quadre de selecció del grup de punts finals de la llista de grups disponibles. Les opcions de supervisió de la llista de fitxers es copien en cada punt final que hi hagi al grup.
   - Utilitzeu la fletxa a la dreta per expandir un grup per tal de veure una llista de tots els punts finals del grup. Marqueu el quadre de selecció per a cada punt final del grup en el qual voleu copiar les opcions de supervisió de fitxers.
   - Expandiu la llista de punts finals al grup **Tots els sistemes**. Marqueu el quadre de selecció per a cada punt final del grup en el que voleu copiar els punts finals.
4. Feu clic a **D'acord**. Les opcions de supervisió de fitxers es copien en el grup seleccionat o en els punts finals seleccionats.

Execució d'una comprovació de Real Time Compliance (RTC)

Des de la pàgina Seguretat, podeu executar una comprovació de conformitat en temps real per verificar si un punt final encara mostra conformitat.

1. Feu clic a l'el•lipsi de la dreta del punt final al qual voleu executar una comprovació de Real Time Compliance (RTC).
2. Feu clic a **Executa la comprovació de conformitat**. S'obre la pàgina **Conformitat** amb la fila del punt final fent pampallugues per indicar que s'està executant la comprovació.
3. Si no s'ha pogut aplicar alguna regla, apareix un missatge que indica l'error a la columna **Nombre de regles fallides**. Utilitzeu la fletxa avall a l'esquerra del punt final per veure la regla que ha fallat.

Configuració de l'execució fiable (TE)

Des de la pàgina **Seguretat** podeu configurar el producte Execució fiable (TE) per a un punt final específic o un grup de punts finals específic.

1. Feu clic a l'el•lipsi de la dreta del punt final del qual voleu editar les opcions de configuració de la TE.
2. Feu clic a **Configura TE**. S'obre la finestra Configuració de les polítiques de TE.
3. Es llisten totes les opcions de configuració de la TE amb una explicació. Per canviar una o diverses opcions de configuració de la TE, seleccioneu o esborreu el quadre de selecció associat. En alguns casos, els canvis a les opcions no s'implementen fins que es reinicia el servidor.
4. Feu clic a **Desa**.

Copia de les opcions d'Execució fiable (TE) en altres grups

Podeu copiar les opcions de configuració de la TE en un altre grup de punts finals o en un conjunt específic de punts finals.

1. Feu clic a l'el•lipsi que hi ha a la dreta del punt final del qual en voleu copiar les opcions de configuració en un altre grup de punts finals o en un conjunt específic de punts finals.
2. Feu clic a **Copia la configuració de TE**. Es mostra una llista de cada grup de punts finals inclosos al grup **Tots els sistemes**.
3. Seleccioneu el grup o els punts finals específics d'alguna d'aquestes maneres:
   - Marqueu el quadre de selecció del grup de punts finals de la llista de grups disponibles. Les opcions de configuració es copien en cada punt final del grup.
   - Expandiu un grup per veure una llista de tots els punts finals del grup. Marqueu el quadre de selecció per a cada punt final del grup en el qual voleu copiar les opcions de configuració.
   - Expandiu la llista de punts finals al grup **Tots els sistemes**. Marqueu el quadre de selecció per a cada punt final del grup en el que voleu copiar els punts finals.
4. Feu clic a **D'acord**. Les opcions de configuració es copien en el grup seleccionat o en els punts finals seleccionats.

Edició de la llista de fitxers d'Execució fiable (TE)

Podeu veure i editar les opcions de supervisió de la TE per a cada fitxer en un punt final.

1. Feu clic a l'el•lipsi de la dreta del punt final que allotja els fitxers les opcions de supervisió de la TE dels quals voleu veure o editar.
2. Feu clic a **Edita la llista de fitxers de TE**. S'obre la pàgina **Configuració de la llista de fitxers de TE** per llistar tots els directoris i fitxers que hi ha al punt final. Una marca de comprovació a la icona de la carpeta del directori indica que s'està supervisant un fitxer, o més d'un, d'aquest directori.
3. Si el fitxer, les opcions del qual voleu veure o editar, està en un directori, feu doble clic al directori per llistar els fitxers. Es llisten tots els fitxers del directori.
4. Les opcions de supervisió de cada fitxer al punt final es llisten a les columnes **TE** i **Volàtil**. Es mostra el quadre de selecció a la columna **TE** si se supervisa el fitxer pels canvis de contingut. Es marca el quadre de selecció a la columna **Volàtil** si el fitxer se supervisa només pels canvis de permís. Per canviar les opcions de supervisió, marqueu o desmarqueu els quadres de selecció d'un fitxer, o més d'un al punt final.
5. Feu clic a **Desa**.

Còpia de les opcions de supervisió de la llista de fitxers d'Execució fiable en altres grups

Podeu copiar les opcions de configuració de fitxers de la TE en un altre grup de punts finals o en un conjunt específic de punts finals.

1. Feu clic a l'el•lipsi que hi ha a la dreta del punt final del qual voleu copiar les opcions de supervisió en un altre grup de punts finals o en un conjunt específic de punts finals.
2. Feu clic a **Copia la llista de fitxers de TE**. Es mostra una llista de cada grup de punts finals inclosos al grup **Tots els sistemes**.
3. Seleccioneu el grup o els punts finals específics d'alguna d'aquestes maneres:
   - Marqueu el quadre de selecció del grup de punts finals de la llista de grups disponibles. Les opcions de supervisió de la llista de fitxers es copien en cada punt final que hi hagi al grup.
   - Expandiu un grup per veure una llista de tots els punts finals del grup. Marqueu el quadre de selecció per a cada punt final del grup en el qual voleu copiar les opcions de supervisió de fitxers.
   - Expandiu la llista de punts finals al grup **Tots els sistemes**. Marqueu el quadre de selecció per a cada punt final del grup en el que voleu copiar els punts finals.
4. Feu clic a **D'acord**. Les opcions de supervisió de fitxers es copien en el grup seleccionat o en els punts finals seleccionats.

Visualització de l'estat d'altres funcions del PowerSC

Des de la pàgina Seguretat podeu veure l'estat de les funcions Engegada fiable, Tallafoc fiable i Registre fiable del PowerSC. També podeu veure l'estat de les actualitzacions del Trusted Network Connect (TNC) en un punt final.

1. Des de la pàgina principal, seleccioneu la pestanya **Seguretat**. S'obre la pàgina **Seguretat**.
2. El component TNC del PowerSC s'utilitza per comprovar i actualitzar els pedaços de seguretat en cada punt final. La columna **Actualització mitjançant TNC** de la taula de punts finals indica si un punt final està o no actualitzat respecte la perspectiva del servidor de TNC. La secció **Actualització mitjançant TNC** del bàner del panell d'eines mostra el percentatge de punts finals al grup que estan actualitzats. Per treure la visualització de la informació d'actualització del TNC de la pàgina **Seguretat**, seguiu aquests passos:
   a. Feu clic a la icona **Idiomes i paràmetres** de la barra de menú de la pàgina principal.
   b. Feu clic a **Ús de subproducte**.
   c. Establiu **Actualització mitjançant TNC** en desactivat.
   d. Per restaurar la visualització, activeu **Actualització mitjançant TNC**.
3. La columna **TB** de la taula de punts finals indica si l'engegada fiable del PowerSC està disponible al punt final. La secció **Engegada fiable** del bàner del panell d'eines mostra el percentatge de punts finals del grup seleccionat actualment que tenen activada l'engegada fiable del PowerSC. Per treure la visualització de la informació de l'engegada fiable del PowerSC de la pàgina **Seguretat**, seguiu aquests passos:
   a. Feu clic a la icona **Idiomes i paràmetres** de la barra de menú de la pàgina principal.
   b. Feu clic a **Ús de subproducte**.
   c. Feu lliscar el commutador associat amb **Engegada fiable** a la posició desactivada.
   d. Per restaurar la visualització, feu lliscar el commutador en la posició activada.
4. La columna **TF** de la taula de punts finals indica si el tallafoc fiable del PowerSC està disponible al punt final. La secció **Tallafoc fiable** del bàner del panell d'eines mostra el percentatge de punts finals del grup seleccionat actualment que tenen activat el tallafoc fiable del PowerSC. Per treure la visualització de la informació del tallafoc fiable de la pàgina **Seguretat**, seguiu aquests passos:
   a. Feu clic a la icona **Idiomes i paràmetres** de la barra de menú de la pàgina principal.
   b. Feu clic a **Ús de subproducte**.
   c. Feu lliscar el commutador associat amb **Tallafoc fiable** a la posició desactivada.
   d. Per restaurar la visualització, feu lliscar el commutador en la posició activada.
5. La columna **TL** de la taula de punts finals indica si el registre fiable del PowerSC està disponible al punt final. La secció **Registre fiable** del bàner del panell d'eines mostra el percentatge de punts finals del grup seleccionat actualment que tenen activat el registre fiable del PowerSC. Per treure la visualització de la informació del registre fiable de la pàgina **Seguretat**, seguiu aquests passos:

a. Feu clic a la icona **Idiomes i paràmetres** de la barra de menú de la pàgina principal.
b. Feu clic a **Ús de subproducte**.
c. Feu lliscar el commutador associat amb **Registre fiable** a la posició desactivada.
d. Per restaurar la visualització, feu lliscar el commutador en la posició activada.

Commutació de la supervisió d'execució fiable

Podeu activar i desactivar la supervisió de l'execució fiable (TE). També podeu desactivar la supervisió de la TE i planificar-ne l'activació en funció d'un interval de temps especificat.

1. Feu clic a la icona **Commutació de l'execució fiable**.
2. Des de la safata desplegable, seleccioneu una de les opcions següents:
   - **Activa per a TOTS els punts finals** per activar la supervisió de la TE en cada punt final.
   - **Desactiva per a TOTS els punts finals** per desactivar la supervisió de la TE en cada punt final.
3. Si la supervisió de la TE està desactivada, estaran disponibles les opcions per establir una hora quan s'iniciï la supervisió de la TE. Podeu seleccionar una de les següents hores de reinici:
   - **1 hora**
   - **5 hores**
   - **1 dia**
   - **1 setmana**
   - **Mai**
4. Feu clic a **Desa**.

Enviament de notificacions per correu electrònic quan es produeix un esdeveniment de seguretat

Des de la pàgina Seguretat, podeu enviar una notificació per correu electrònic a un destinatari, o a més d'un, quan es produeix un esdeveniment de seguretat.

1. Des de la pàgina principal, seleccioneu la pestanya **Seguretat**. S'obre la pàgina **Seguretat**.
2. Feu clic a la icona **Paràmetres de correu electrònic** de la cantonada dreta de la barra de menú. S'obre la finestra **Paràmetres de correu electrònic**.
3. Marqueu el quadre de selecció **Envieu-me correus electrònics**.
4. Escriviu les adreces de correu electrònic de cada destinatari separades per comes al camp **Adreces (separades per comes)**.

Com treballar amb informes

Podeu accedir a diversos informes des de la pàgina Informes de la GUI de PowerSC.

Hi ha disponibles els informes següents:

- L'informe **Visió general de conformitat** és una instantània de la informació d'alt nivell que es visualitza a la pàgina **Conformitat** de la interfície.
- L'informe **Detall de conformitat** és una instantània de la informació de nivell elevat i detallada que es visualitza a la pàgina **Conformitat**.
- L'informe **Visió general de la integritat de fitxers** és una instantània de la informació d'alt nivell que es visualitza a la pàgina **Seguretat** de la interfície.
- L'informe **Detall de la integritat de fitxers** és una instantània de la informació de nivell elevat i detallada que es visualitza a la pàgina **Seguretat**.
- **Conformitat i FIM combinats**

Per defecte, la pàgina **Informes** mostra els informes **Visió general de conformitat** i **Visió general de la integritat de fitxers** per al grup **Tots els sistemes**. No hi ha grups especificats per defecte per als informes **Detall de conformitat**, **Detall de la integritat de fitxers** o **Conformitat i FIM combinats**.

Podeu generar tots els tipus d'informe per al grup **Tots els sistemes** i cada grup que hàgiu definit. Podeu generar l'informe per a tots els punts finals d'un grup o un subconjunt de punts finals del grup. Després de generar un informe, podeu planificar la distribució de l'informe en format HTML i com a fitxer CSV a un dels destinataris de correu electrònic, o a més d'un, segons demanda o cada dia.

La llista d'informes que es visualitzen a la pàgina **Informes** varia en funció de l'ID d'inici de sessió d'usuari. Podeu generar informes només per a aquests punts finals que gestioneu en funció del vostre ID d'inici de sessió. Cada informe que genereu en una determinada sessió es llista quan obriu la sessió següent.

Selecció del grup d'informes

Podeu executar cada informe per al grup **Tots els sistemes** i per a cada grup que hagueu definit. Podeu decidir executar un informe per a tots els punts finals que s'hagin inclòs en un grup o per a un subconjunt de punts finals del grup.

1. Des de la pàgina principal, feu clic a la pestanya **Informes**. S'obre la pàgina **Informes**.
2. Feu clic a l'el•lipsi de la dreta del tipus d'informe que vulgueu executar.
3. Feu clic a **Canvia de grup**.
4. S'obre un quadre de selecció en què apareix una llista de tots els grups disponibles. Seleccioneu el botó d'opció que hi ha al costat del grup del qual vulgueu executar l'informe. Feu clic a **Confirma**. L'informe s'executa i es renova el contingut del panel principal amb la informació del grup seleccionat.
5. Per executar un informe per un subconjunt de punts finals, expandiu el grup **Tots els sistemes**. Es visualitza una llista de tots els punts finals disponibles. Marqueu el quadre de selecció que hi ha al costat de cada punt final que vulgueu incloure a l'informe. Feu clic a **Confirma** per executar l'informe.

   Nota: Si voleu executar un informe en un grup específic de punts finals, podeu crear un grup que contingui aquests punts finals. La creació del grup estalvia temps i el poden utilitzar tots els usuaris perquè els grups són globals (els poden veure tots els usuaris de la interfície).
6. Podeu cercar un punt final específic escrivint el nom del punt final al quadre de text de cerca. Feu clic a **Confirma** per executar l'informe per aquest punt final.

Distribució d'informes a través del correu electrònic

Després de definir el grup per un informe, podeu planificar-ne la distribució en forma de correu electrònic amb format HTML i un fitxer CSV. Podeu planificar que el correu electrònic s'enviï a un destinatari de correu electrònic (o més d'un) immediatament o cada dia.

Inclosa la versió CSV de l'informe, es permet que els destinataris carreguin les dades de l'informe en un full de càlcul o que les importin en alguna altra aplicació de programari que consumeix fitxers CSV. Els fitxers CSV no tenen conceptes de gràfics o panells d'eines. Un fitxer CSV generat a partir d'un informe de visió general conté totes les capçaleres de columna separades per comes a la primera fila. A les files posteriors apareixen el punt final i els valors de cada columna.

Es generen diversos fitxers CSV a partir dels informes detallats. El primer fitxer CSV es formata de forma similar a l'informe de visió general. Es genera un fitxer CSV independent per a cada nivell de detall de l'informe. Per exemple, a l'informe de detalls d'integritat de fitxers es generaran els següents nivells de detall en un fitxer CSV independent:

- **Configuració de TE**
- **Configuració d'RTC**
- **Estat de subproducte**

1. Des de la pàgina principal, feu clic a la pestanya **Informes**. S'obre la pàgina **Informes**.
2. Des de la llista d'informes disponibles, seleccioneu l'informe que vulgueu distribuir. S'executa l'informe i es renova el contingut de la pàgina principal.
3. Feu clic a l'el•lipsi de la dreta de l'informe que vulgueu distribuir.
4. Feu clic a **Opcions de correu electrònic**. S'obre la finestra Envia informe per correu electrònic.
5. Especifiqueu l'adreça de correu electrònic per a cada destinatari al camp **Adreces**. Separeu les diverses adreces de destinataris amb un punt i coma (;).
6. Especifiqueu una descripció del correu electrònic al camp **Assumpte**.
7. Trieu una de les opcions següents:
   - Marqueu el quadre de selecció **Enviar cada dia a les** per enviar l'informe als destinataris cada dia. Especifiqueu l'hora local i envieu l'informe seleccionant l'hora en hores i minuts. Feu clic a **Desa i tanca**. L'informe s'envia cada dia a l'hora especificada.
   - Feu clic a **ENVIA IMMEDIATAMENT** per enviar l'informe. L'informe s'envia i es tanca la finestra.

Ordres del PowerSC Standard Edition

El PowerSC Standard Edition proporciona ordres que permeten que hi hagi comunicació amb el component Tallafoc fiable i el component Trusted Network Connect mitjançant la línia d'ordres.

Odre chvfilt

Finalitat

Canvia els valors de la norma de filtre d'encreuament de LAN virtual existent.

Sintaxi

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>]

Descripció

L'ordre **chvfilt** es fa servir per canviar la definició d'una norma de filtre d'encreuament de LAN virtual a la taula de normes de filtre.

Senyaladors

-a Especifica l'acció. Els valors vàlids són els següents:
- D (Denegar): bloqueja el trànsit
- P (Permetre): permet el trànsit

-c Especifica diferents protocols als quals s'aplica la norma de filtre. Els valors vàlids són els següents:
- udp
- icmp
- icmpv6
- tcp
- qualsevol

-d Especifica l'adreça de destinació en format IPv4 o IPv6.

-m Especifica la màscara d'adreces d'origen.

-M Especifica la màscara d'adreces de destinació.

-n Especifica l'ID de filtre de la norma de filtres que s'ha de modificar.

-o Especifica el port d'origen o l'operació de tipus Internet Control Message Protocol (ICMP). Els valors vàlids són els següents:
- lt
- gt
- eq
- qualsevol

-O Especifica el port de destinació o l'operació de codi ICMP. Els valors vàlids són els següents:
- lt
- gt
- eq

- qualsevol

-p Especifica el port d'origen o el tipus d'ICMP.

-P Especifica el port de destinació o el codi ICMP.

-s Especifica l'adreça d'origen en format v4 o v6.

-v Especifica la versió IP de la taula de normes de filtre. Els valors vàlids són 4 i 6.

-z Especifica l'ID de la LAN virtual de la partició lògica d'origen.

-Z Especifica l'ID de la LAN virtual de la partició lògica de destinació.

Estat de sortida

Aquesta ordre torna els valors de sortida següents:

0 S'ha executat correctament.

>0 S'ha produït un error.

Exemples

1. Per canviar una norma de filtre vàlida que existeixi al kernel, escriviu l'ordre tal com s'indica a continuació:

   ```
   chvfilt -n 1 -v4 -a P -z 100 -Z 300 -o eq -p 23 -O lt -P 345 -c tcp
   ```

2. Quan no existeix una norma de filtre (n=2) al kernel, la sortida és com la que figura a continuació:

   ```
   chvfilt -n 2 -v4 -a P -z 100 -Z 300 -o eq -p 23 -O lt -P 345 -c tcp
   ```

   El sistema mostra la següent sortida:

   ```
   ioctl(QUERY_FILTER) failed no filter rule err=2
   No es pot canviar la norma de filtre.
   ```

Ordre genvfilt

Finalitat

Afegeix una norma de filtre per a l'encreuament de LAN virtuals (VLAN) entre particions lògiques al mateix servidor IBM Power Systems.

Sintaxi

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**>]

Descripció

L'ordre **genvfilt** afegeix una norma de filtre per a l'encreuament de LAN virtual (VLAN) entre particions lògiques (LPAR) al mateix servidor IBM Power Systems.

Senyaladors

-a Especifica l'acció. Els valors vàlids són els següents:

- D (Denegar): bloqueja el trànsit
- P (Permetre): permet el trànsit

-c Especifica diferents protocols als quals s'aplica la norma de filtre. Els valors vàlids són els següents:

- udp
- icmp

- icmpv6
- tcp
- qualsevol

-d Especifica l'adreça de destinació en format v4 o v6.

-m Especifica la màscara d'adreces d'origen.

-M Especifica la màscara d'adreces de destinació.

-o Especifica el port d'origen o l'operació de tipus Internet Control Message Protocol (ICMP). Els valors vàlids són els següents:
- lt
- gt
- eq
- qualsevol

-O Especifica el port de destinació o l'operació de codi ICMP. Els valors vàlids són els següents:
- lt
- gt
- eq
- qualsevol

-p Especifica el port d'origen o el tipus d'ICMP.

-P Especifica el port de destinació o el codi ICMP.

-s Especifica l'adreça d'origen en format IPv4 o IPv6.

-v Especifica la versió IP de la taula de normes de filtre. Els valors vàlids són 4 i 6.

-z Especifica l'ID de la LAN virtual de l'LPAR d'origen. L'ID de LAN virtual ha d'estar en l'interval d'1 a 4096.

-Z Especifica l'ID de la LAN virtual de l'LPAR de destinació. L'ID de LAN virtual ha d'estar en l'interval d'1 a 4096.

Estat de sortida

Aquesta ordre torna els valors de sortida següents:

0 S'ha executat correctament.

>0 S'ha produït un error.

Exemples

1. Per executar una norma de filtre que permeti dades TCP d'un ID VLAN d'origen de 100 en un ID VLAN de destinació de 200 en ports específics, escriviu l'ordre tal com s'indica a continuació:
   ```
   genvfilt -v4 -a P -z 100 -Z 200  -o lt -p 345 -O lt -P 345 -c tcp
   ```

Referència relacionada:

"Ordre mkvfilt" a la pàgina 174

"Ordre vlantfw" a la pàgina 193

Ordre lsvfilt

Finalitat

Llista les normes de filtre d'encreuament LAN virtual de la taula de filtres.

Sintaxi

lsvfilt [**-a**]

Descripció

L'ordre **lsvfilt** es fa servir per llistar les normes de filtre d'encreuament LAN virtual i els estats.

Senyaladors

-a Llista només les normes de filtre actives.

Estat de sortida

Aquesta ordre torna els valors de sortida següents:

0 S'ha executat correctament.

>0 S'ha produït un error.

Exemples

1. Per llistar totes les normes de filtre actives al kernel, escriviu l'ordre tal com s'indica a continuació:

   ```
   lsvfilt -a
   ```

Conceptes relacionats:

"Desactivació de regles" a la pàgina 129
Podeu desactivar regles que permetin l'encaminament a través de VLAN en la funció Tallafoc fiable.

Ordre mkvfilt

Finalitat

Activa les normes de filtre d'encreuament de LAN virtual que defineix l'ordre **genvfilt**.

Sintaxi

mkvfilt -u

Descripció

L'ordre **mkvfilt** activa les normes de filtre d'encreuament de LAN virtual que defineix l'ordre **genvfilt**.

Senyaladors

-u Activa les normes de filtre de la taula de normes de filtre.

Estat de sortida

Aquesta ordre torna els valors de sortida següents:

0 S'ha executat correctament.

>0 S'ha produït un error.

Exemples

1. Per activar les normes de filtre al kernel, escriviu l'ordre tal com s'indica a continuació:

   ```
   mkvfilt -u
   ```

Referència relacionada:

"Ordre genvfilt" a la pàgina 172

Ordre pmconf

Finalitat

Crea informes i duu a terme la gestió del servidor de gestió de pedaços de connexió a xarxa segura (TNCPM) mitjançant el registre de nivells tecnològics i servidors TNC per obtenir les correccions més recents i generar informes sobre l'estat de TNCPM.

| **Nota:** El servidor de TNCPM s'ha d'executar només en la versió 7.2 de l'AIX amb el nivell tecnològic
| 7100-02 per permetre descarregar metadades del Service Pack.

Sintaxi

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

pmconf rmtncpm

pmconf start

pmconf stop

pmconf init -i <*interval baixada*> **-l** <*llista NT*> **-A** [**-P** <*camí accés baixades*>] [**-x** <*interval correccions provisional*>] [**-K** <*clau de correcció provisional*>]

pmconf add -l *llista_NT*

pmconf add -o <*nom de paquet*> -V <*versió*> -T [installp|rqm] -D <*camí d'accés definit per l'usuari*>

pmconf add -p <*llista_SP*> [**-U** <*camí_d'accés_SP_definit_usuari*>]

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

pmconf add -y <*fitxer d'advertiments*> **-v** <*fitxer de signatures*> **-e**

pmconf chtncpm attribute = *value*

pmconf delete -l <*llista_TL*>

pmconf delete -o <*nom paquet*> -V <*versió*>

pmconf delete -p <*llista_SP*>

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

pmconf export -f *nom_fitxer*

| **pmconf get** -o <paquet> -V <versió> -T <installp | rpm> -D <directori baixades>

| **pmconf get** -L -o <paquet> -V <versió | tot> -T <installp | rpm>

| **pmconf get** -L -p <SP>

| **pmconf get** -p <SP> -D <directori baixades>

pmconf hist -d

pmconf hist -u

pmconf import -f *nom_fitxer_cert* **-k** *nom_fitxer_clau*

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

pmconf list -a *SP*

pmconf list -C

pmconf list -l *SP*

pmconf list -o <*nom paquet*> -V <*versió*>

pmconf list -o [-c] [-q]

pmconf log loglevel = info | error | none

pmconf modify -i < *interval baixada*>

pmconf modify -P <*camí_accés_baixada*>

pmconf modify -g <*yes o no per acceptar totes les llicències*>

pmconf modify -t <*llista_tipus_APAR*>

pmconf modify -x <*interval de correccions provisionals*>

pmconf modify -K <*clau de correcció provisional*>

| **pmconf proxy** display

| **pmconf proxy** [enable=yes | no] [host=<nom d'amfitrió>] [port=<número de port>]

pmconf restart

pmconf status

Descripció

Les funcions de l'ordre **pmconf** són els següents:

Gestió de dipòsits de gestió
Registra o suprimeix el registre dels nivells tecnològics; suprimeix el registre de servidors TNC. TNCPM crea un dipòsit de correccions per a cada nivell tecnològic que conté les correccions més recents, informació **lslpp** (per exemple, informació sobre els conjunts de fitxers instal•lats o actualitzacions dels conjunts de fitxers), i la informació de correcció de seguretat per al nivell tecnològic.

Creació d'informes
Genera informa sobre l'estat de TNCPM.

El operacions següents es poden dur a terme mitjançant l'ordre **pmconf**:

Element	Descripció
add	Registra un nou nivell tecnològic utilitzant TNCPM.
chtncpm	Canvia els atributs al fitxer tnccs.conf. Una ordre **start** explícita és necessària perquè els canvis entrin en vigor al servidor de TNCPM.
delete	Suprimeix el registre d'un nivell tecnològic mitjançant TNCPM.
get	Mostra o baixa informació sobre les correccions de seguretat disponibles i els paquets de l'Open Source disponibles.
history	Mostra l'historial d'actualitzacions i baixades.
list	Mostra informació sobre TNCPM.
log	Estableix el nivell de registre per a components de TNC.
mktncpm	Crea el servidor de TNCPM.
modify	Modifica els atributs de tncpm.conf.
proxy	Gestiona la configuració dels paràmetres del servidor intermediari.
rmtncpm	Elimina el servidor de TNCPM.
start	Inicia el servidor de TNCPM.
stop	Atura el servidor de TNCPM.

Senyaladors

Element	Descripció
-A	Accepta tots els acords de llicència a l'hora de dur a terme les actualitzacions del client.
-a <fitxer_advertiment>	Especifica el fitxer d'advertiment que correspon al paràmetre **ifix**. Si el fitxer d'advertiment no es proporciona, el paràmetre **ifix** no es visualitza com una adreça comuna de vulnerabilitats i riscos (CVE) de la correcció provisional.
-a *SP*	Genera un informe amb informació d'informe autoritzat d'anàlisi de programa de seguretat (APAR) per al paquet de servei. *SP* té el format: REL00-TL-SP (per exemple, `6100-01-04` representa el paquet de servei 04 per al nivell tecnològic 01 i la versió 6.1).
-e <fitxer_correcció_provisional>	Especifica les correccions provisionals que s'afegeixen a TNCPM.
-i *interval_baixada*	Especifica l'interval amb què TNCPM comprova si hi ha un nou paquet de serveis per a nivells tecnològics registrats. L'interval e´s un valor sencer que representa minuts i representa el format següent: **d** (número de dies): **h** (hores): **m** (minuts). L'interval admès per *interval_baixada* és entre 30 i 525600 minuts.
-K <clau_correcció_provisional>	Especifica una clau pública de l'IBM AIX Product Security Incident Response Tool (PSIRT) que s'utilitza per autenticar els advertiments i les correccions provisionals que s'han baixat. Aquesta clau pública es pot baixar des d'un servidor de claus públiques PGP utilitzant l'ID **0x28BFAA12**.
-L	Especifica el mode Lliste o Només cerca.
o *nom de paquet*	El nom del paquet Open Source en el que cal cercar o que s'ha de baixar.
-P *camí_accés_dipòsit_correccions*	Especifica el directori de baixada dels dipòsits de correccions que TNCPM baixarà. El directori per defecte és **/var/tnc/tncpm/fix_repository**.
-p *llista_SP*	Especifica una llista de paquets de servei per baixar-se. La llista està separada per comes i té el format: REL00-TL-SP (per exemple, `6100-01-04` representa el paquet de servei 04 per al nivell tecnològic 01 i la versió 6.1). Quan utilitzeu el senyalador -U, especifiqueu només un SP.
-t *tipus_llista_APAR*	Especifica els tipus d'APAR que admet el TNCPM per a l'actualització del client i el llistat de servidors TNC. Els APAR de seguretat sempre s'admeten. La llista de tipus d'APAR és una llista separada per comes dels tipus següents: HIPER, FileNet Process Engine, Enhancement.
T *tipus de paquet*	Especifica el tipus de paquet Open Source en el que cal cercar o que s'ha de baixar
-U *dipòsit_correccions_definit_usuari*	Especifica el camí d'accés al dipòsit de correccions definit per l'usuari. Especifiqueu la versió, el nivell tecnològic i el paquet de servei associats al dipòsit de correccions que s'utilitza per a la verificació i les actualitzacions de clients.
-s	Genera un informe de paquets de servei registrats.
-l *SP*	Genera un informe d'informació **lslpp** sobre el paquet de servei. *SP* té el format: REL00-TL-SP (per exemple, `6100-01-04` representa el paquet de servei 04 per al nivell tecnològic 01 i la versió 6.1).
-u	Genera un informe de l'historial d'actualitzacions del client.
V *versió*	La versió del paquet Open Source en el que cal cercar o que s'ha de baixar. El mode de carca (-L) es pot especificar un valor “all” per cercar totes les versions disponibles del paquet especificat.
-d	Genera un informe de l'historial de baixades de paquets de servei.
-C	Genera un informe sobre el certificat de servidor.
-f *nom_fitxer*	Especifica el nom del fitxer de certificat.
-k	Especifica el fitxer des del qual cal llegir la clau del certificat en el cas d'una operació d'importació.

-c	Mostra els atributs d'usuari en registres separats per dos punts, tal com s'indica a continuació:
	`# name: atribut1: atribut2: ...`
	`policy: valor1: valor2: ...`

Element	Descripció
-v<*fitxer_signatures*>	Especifica el fitxer de signatures per l'advertiment de vulnerabilitat de l'IBM AIX.
-y <*fitxer advertiment*>	Especifica un fitxer d'advertiment de vulnerabilitat de l'IBM AIX.
-q	Suprimeix la informació de capçalera.
-x <*interval_correcció_provisional*>	Especifica l'interval, en minuts, en que es comprova i es baixen noves correccions provisionals. Si aquest valor s'estableix en 0, s'inhabilita la baixada i la notificació automàtiques de correccions provisionals. L'interval per defecte és cada 24 hores. L'interval admès per a <*interval de correccions provisionals*> és entre 30 i 525600 minuts.

Estat de sortida

Aquesta ordre torna els valors de sortida següents:

Element	Descripció
0	L'ordre s'ha executat correctament i s'han realitzat tots els canvis sol•licitats.
>0	S'ha produït un error. El missatge d'error imprès inclou més detalls sobre el tipus de fallada.

Exemples

1. Per inicialitzar TNCPM, introduïu l'ordre següent:
   ```
   pmconf init -f 10080 -l 5300-11,6100-00
   ```
2. Per crear el daemon TNCPM, introduïu l'ordre següent:
   ```
   mktncpm pmport=55777 tncserver=11.11.11.11:77555
   ```
3. Per iniciar el servidor, introduïu l'ordre següent:
   ```
   pmconf start
   ```
4. Per aturar el servidor, introduïu l'ordre següent:
   ```
   pmconf stop
   ```
5. Per registrar un nou nivell tecnològic utilitzant TNCPM, introduïu l'ordre següent:
   ```
   pmconf add -l 6100-01
   ```
6. Per suprimir el registre d'un nivell tecnològic de TNCPM, introduïu l'ordre següent:
   ```
   pmconf delete -l 6100-01
   ```
7. Per suprimir el registre d'un servidor de TNC d'un servidor que té l'adreça IP 11.11.11.11 de TNCPM, introduïu l'ordre següent:
   ```
   pmconf delete -t 11.11.11.11
   ```
8. Per registrar una versió més recent d'un paquet de servei anterior a TNCPM, introduïu l'ordre següent:
   ```
   pmconf add -s 6100-01-04
   ```
9. Per suprimir el registre d'un paquet de servei anterior de TNCPM, introduïu l'ordre següent:
   ```
   pmconf delete -s 6100-01-04
   ```
10. Per generar un informe de dipòsits de correcció per a cada nivell tecnològic registrat, introduïu l'ordre següent:
    ```
    pmconf list -s
    ```
11. Per generar un informe d'informació **lslpp** de nivell tecnològic, introduïu l'ordre següent:
    ```
    pmconf list -l 6100-01-02
    ```
12. Per generar un informe de l'historial d'actualitzacions, introduïu l'ordre següent:
    ```
    pmconf hist -u
    ```
13. Per generar un informe de l'historial de baixades, introduïu l'ordre següent:
    ```
    pmconf hist -d
    ```
14. Per generar un informe del certificat de servidor, introduïu l'ordre següent:
    ```
    pmconf list -C
    ```

15. Per generar un informe d'informació d'APAR de seguretat d'un paquet de servei, introduïu l'ordre següent:
    ```
    pmconf list -a 6100-01-02
    ```
16. Per importar un certificat de servidor, introduïu l'ordre següent:
    ```
    pmconf import -f /tmp/server.txt -k /tmp/server-cert-key.txt
    ```
17. Per exportar el certificat de servidor, introduïu l'ordre següent:
    ```
    pmconf export -f /tmp/server.txt
    ```
18. Per visualitzar totes les versions disponibles en format rpm dels paquets de codi obert "emacs", escriviu l'ordre següent:
    ```
    pmconf get -L -o emacs -V all -T rpm
    ```
19. Per baixar la versió 4.5.1 del paquet de codi obert "lsof", en format rpm, al directori /tmp/new_lsof, escriviu les ordres següents:
    ```
    mkdir /tmp/new_lsof
    pmconf get -o lsof -V 4.5.1 -T rpm -D /tmp/new_lsof
    ```
20. Per visualitzar totes les versions disponibles de l'OpenSSH en format installp, escriviu l'ordre següent:
    ```
    pmconf get -o openssh -T installp -L -V all
    ```
21. Per visualitzar els paràmetres de configuració de l'intermediari actual que utilitzarà cURL quan baixi els paquets Open Source per les correccions de seguretat, escriviu l'ordre següent:
    ```
    pmconf proxy display
    ```
22. Per establir la configuració de l'intermediari de manera que estigui inhabilitada, escriviu l'ordre següent:
    ```
    pmconf proxy enable=no
    ```
23. Per habilitar intermediari i establir l'amfitrió en "myProxyServer" al port 9876, escriviu l'ordre següent:
    ```
    pmconf proxy enable=yes host=myProxyServer port=9876
    ```
24. Per canviar el port del servidor intermediari que s'ha d'utilitzar, escriviu l'ordre següent:
    ```
    pmconf proxy port=1234
    ```
25. Per visualitzar les vulnerabilitats conegudes mitjançant correccions de seguretat per al nivell de Service Pack Level 7100-03-02, escriviu l'ordre següent:
    ```
     pmconf get -L -p 7100-03-02
    ```
26. Per baixar, però sense aplicar, les correccions de seguretat del nivell de Service Pack 7200-00-01, al directori /tmp/ifixes_for_7.2.0.1, escriviu les ordres següents:
    ```
    mkdir /tmp/ifixes_for_7.2.0.1
    pmconf get -p 7200-00-01 -D /tmp/ifixes_for_7.2.0.1
    ```

Ordre psconf

Finalitat

Genera informes i duu a terme la gestió del servidor del Trusted Network Connect (TNC) el client de TNC, el remitidor IP de TNC (IPRef) i l'assistent de gestió d'actualitzacions de servei (SUMA). Gestiona polítiques de gestió de pedaços i conjunts de fitxers en relació amb la integritat del punt final (servidor i client) a durant o després de la connexió de xarxa per protegir la xarxa d'amenaces i atacs.

Sintaxi

Operacions del servidor de TNC:

psconf mkserver [**tncport=**<*port*>] **pmserver=**<*amfitrió:port*> [tsserver=<amfitrió>] [**recheck_interval=**<*hora_en_minuts*> | **d** (dies) : **h** (hores) : **m** (minuts)] [**dbpath** =

<*directori_definit_per_usuari*>] [**default_policy=**<*yes* | *no* >] [**clientData_interval=**<*hora_en_minuts*> | **d** (dies) : **h** (hores) : **m** (minuts)] [**clientDataPath=**<*camí_accés_complet*>]

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

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

psconf chserver attribute = *value*

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

psconf add -F <*nom_política_FS*> -r <*info_muntatge*> [**apargrp= [±]**<*grup_apar1, grup_apar2.. >*] [*ifixgrp*=[+|-]<*grup_correcció_provisional1,grup_correció_provisional2...>*]

psconf add { **-G** <*nom_grup_IP*> **ip=[±]**<*amfitrió1, amfitrió2...*> | {**-A**<*grup_apar*> [**aparlist**=[**±**]*apar1, apar2...* | {**-V** <*grup_correcions_provisionals*> [*ifixlist*=[+|-]*ifix1,ifix2...*]}

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

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

psconf add -I ip= [±]<*amfitrió1, amfitrió2...*>

psconf delete { **-F** <*nom_política_sistema_fitxers*> | **-G** <*nom_grup_ip*> | **-P** <*nom_política*> | **-A** <*grup_apar*> | **-V** <*grup_corr_prov*>}

psconf delete -H -i <*amfitrió* | **ALL**> **-D** <*aaaa-mm-dd*>

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

psconf certdel -i <*amfitrió*>

psconf verify -i <*amfitrió*> | **-G** <*grup_ip*>

psconf update [-p] {-i<*amfitrió*>| **-G** <*grup_IP*>[**-r** <*info_muntatge*> | **-a** <*apar1, apar2...*> | **[-u] -v** <*correcció_provisional1, correcció_provisional2,...*> | **-O** <*grup_openpkg1, grup_openkg2,...*>}

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

psconf import -C -i <*amfitrió*> **-f** <*nom_fitxer*> | **–d** <*nom_fitxer_importació_base_dades*>

psconf { **import -k** <*nom_fitxer_clau*> | **export**} **-S -f** <*nom_fitxer*>

psconf list { **-S** | **-G** < *nom_grup_IP* | **ALL** > | **-F** < *nom_política_FS* | **ALL** > | **-P** < *nom_política* | **ALL** > | **-r** < *info_muntatge* | **ALL** > | **-I -i** < *ip* | **ALL** > | **-A** < *grup_apar* | **ALL** > | **-V** <*grup_correcions_provisionals*> | -O <*grup_openpkg*|*ALL*>} **[-c] [-q]**

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

psconf export -d <camí_accés_directori_exportació>

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

psconf report -A <nom_advertiment>

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

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

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

psconf clientData {-l | -g} -i <*ip|amfitrió***>**

psconf add -O <*grup_openpkg***> <***nom_openpkg:versió***>**

psconf delete -O <*grup_openpkg***> <***nom_openpkg:versió***>**

psconf delete -O <*grup_openpkg***>**

psconf delete -O ALL

psconf add -O <*grup_openpkg***> fspolicy=<***nom_política_fs***>**

psconf report -O ALL -o TEXT

| **psconf add -V <***grup_corr_prov***> autoupdate=<yes|no>**

| **psconf reboot -i <***amfitrió***> last one**

Operacions de client de TNC:

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

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

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

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

psconf chclient attribute = *value*

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

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

psconf import { **-S** | **-C -k** <*nom_fitxer_clau*> } **-f** <*nom_fitxer*>

Operacions d'IPRef de TNC:

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

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

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

psconf chipref attribute = *value*

psconf { **import -k** <*nom_fitxer_clau*> | **export** } **-R -f** <*nom_fitxer*>

psconf list -R

Descripció

La tecnologia TNC és una arquitectura basada en estàndard obert per a l'autenticació de punts finals, el mesurament de la integritat de la plataforma i la integració dels sistemes de seguretat. L'arquitectura TNC inspecciona la conformitat dels punts finals (clients i servidors de xarxa) amb polítiques de seguretat abans de permetre'ls l'accés a la xarxa protegida. L'IPRef de TNC notifica al servidor sobre qualsevol IP nova que es detecti al servidor d'E/S virtual (VIOS).

SUMA ajuda que els administradors del sistema prescindeixin de recuperar manualment les actualitzacions de manteniment del web. Ofereix opcions flexibles que permeten a l'administrador del sistema configurar una interfície automatitzada per baixar correccions des d'un lloc web de distribució de correccions als seus sistemes.

L'ordre **psconf** gestiona el servidor i els clients de la xarxa afegint o suprimint polítiques de seguretat, confirmant que els clients són fiables o no fiables, generant informes i actualitzant el servidor i el client.

Les operacions següents es poden dur a terme mitjançant l'ordre **psconf**:

Element	Descripció
add	Afegeix una política, un client o la informació de correu electrònic al servidor de TNC.
apargrp	Especifica els noms de grup d'APAR com a part de la política de conjunts de fitxers emprada per a la verificació de clients TNC
aparlist	Especifica la llista d'APAR que formen part del grup d'APAR.
certadd	Marca el certificat com a fiable o no fiable.
certdel	Suprimeix la informació de client.
chclient	Canvia els atributs al fitxer `tnccs.conf`. Una ordre **start** explícita és necessària perquè els canvis entrin en vigor al client de TNC. La sintaxi d'atribut=valor serà la mateixa que a **mkclient**.
chipref	Canvia els atributs al fitxer `tnccs.conf`. Una ordre **start** explícita és necessària perquè els canvis entrin en vigor a IPRef. La sintaxi d'atribut=valor és la mateixa que la de **mkipref**.
chserver	Canvia els atributs al fitxer `tnccs.conf`. Una ordre **start** explícita és necessària perquè els canvis entrin en vigor al servidor de TNC. La sintaxi d'atribut=valor és la mateixa que la de **mkserver**. **Nota:** L'atribut **dbpath** no es pot canviar mitjançant l'ordre **chserver**. Només es pot establir executant **mkserver**.
clientData	Crea un instantània de la informació (nivell de sistema operatiu i conjunts de fitxers instal•lats) sobre el client de TNC. el camí d'accés *clientDataPath* identifica on s'emmagatzema la informació de recopilació d'instantànies. La ubicació per defecte és el directori `/var/tnc/clientData/` del servidor de TNC. Podeu canviar o definir el camí d'accés *clientDataPath* utilitzant la subordre **chserver** o **mkserver**. Podeu iniciar la recopilació d'instantànies del client de TNC des de la línia d'ordres executant la subordre **clientData** des del servidor de TNC. La subordre **clientData** que s'executa des de la línia d'ordres depèn de l'interval **clientData_interval**.

Element	Descripció
clientData_interval	Podeu utilitzar una subordre **chserver** o **mkserver** per configurar la recopilació d'instantànies que s'han de produir en intervals regulars especificant un valor per a l'interval **clientData_interval**. La recopilació d'instantànies comença automàticament quan l'interval **clientData_interval** té un valor diferent de 0 (zero). Per defecte, la recopilació d'instantànies està inhabilitada pel planificador. Per habilitar el planificador, especifiqueu un valor **clientData_interval** que sigui igual o més gran que 30. Per inhabilitar el planificador, especifiqueu un valor de **clientData_interval** de 0 (zero). L'interval admès per a **clientData_interval** és entre 30 i 525600 minuts.
dbpath	Especifica la ubicació de la base de dades de TNC. El valor per defecte és `/var/tnc`.
default_policy	Habilita o inhabilita la verificació automàtica dels clients de TNC per a la correcció provisional (ifix) i els APAR al mateix nivell que el client. Especifiqueu *yes* per tal d'habilitar la verificació automàtica. Especifiqueu *no* per inhabilitar la verificació automàtica. Per obtenir més informació sobre la informació **default_policy**, consulteu la Taula default_policy.
delete	Suprimeix una política o la informació del client.
export	Exporta el certificat de client o servidor, o la base de dades del servidor de TNC.
fspolicy	Especifica la política de conjunt de fitxers de la versió, del nivell tecnològic i del paquet de servei que s'utilitzen per a la verificació de clients de TNC.
import	Importa un certificat al client o servidor, o una base de dades al servidor de TNC.
ipgroup	Especifica el grup de protocol d'Internet (IP) que conté diverses adreces IP o noms d'amfitrió.
list	Mostra informació sobre el servidor de TNC, el client de TNC o el SUMA.
log	Estableix el nivell de registre per a components de TNC.
mkclient	Configura el client de TNC.
mkipref	Configura l'IPRef de TNC.
mkserver	Configura el servidor de TNC.
Openpkggrp	Especifica el nom de grup openpkg com a part de la política del conjunt de fitxer que s'utilitza per verificar clients.
pmport	Especifica el número de port en el qual **pmserver** escolta. El valor per defecte és 38240.
pmserver	Especifica el nom d'amfitrió o l'adreça IP de l'ordre **suma** que baixa els paquets de servei i les correccions de seguretat més recents que hi hagi disponibles al lloc web de l'ECC d'IBM® i al lloc web d'IBM Fix Central.
reboot	Rearranca el client de TNC que s'ha identificat mitjançant l'adreça IP a la variable *<amfitrió>*.
recheck_interval	Especifica l'interval en minuts o en el format d (dies) : h (hores) : m (minuts) perquè el servidor de TNC verifiqui els clients de TNC. L'interval admès per a **recheck_interval** és entre 30 i 525600 minuts. **Nota:** Un valor de **recheck_interval=0** significa que el planificador no inicia la verificació dels clients a intervals regular i que els clients registrats es verifiquen automàticament quan s'inicien. En aquests casos, el client es pot verificar manualment.
report	Genera un informes que té una extensió de fitxer .txt o .csv.
restart	Reinicia el client de TNC, el servidor de TNC o l'IPRef de TNC.
rmclient	Desconfigura el client de TNC.
rmipref	Desconfigura l'IPRef de TNC.
rmserver	Desconfigura el servidor de TNC.
start	Inicia el client de TNC, el servidor de TNC o l'IPRef de TNC.

Element	Descripció
status	Mostra l'estat de la configuració de TNC.
stop	Atura el client de TNC, el servidor de TNC o l'IPRef de TNC.
tncport	Especifica el número de port en el qual el servidor de TNC escolta. El valor per defecte és 42830.
tncserver	Especifica el servidor de TNC que verifica o actualitza els clients de TNC.
tssserver	Especifica l'IP o el nom d'amfitrió del servidor de Trusted Surveyor.
update	Instal•la pedaços al client.
verify	Inicia una verificació manual del client.

A la taula següent es mostren els resultats de configurar la subordre **default_policy** en els valors *yes* o *no*:

Taula 16. Resultats de la subordre default_policy

FSpolicy (política Fileset)	default policy=*yes*	default policy=*no*
El client de TNC pertany a una política de conjunt de fitxers amb uns grups de correccions provisionals (iFix) i d'APAR definits	La política per defecte la sobreescriuen les correccions provisionals i els APAR que es proporcionen a la política de conjunt de fitxers.	No s'utilitza la política per defecte. Les correccions provisionals i els APAR proporcionats a la política de conjunt de fiters es tenen en compte durant el procés de verificació pel client de TNC.
El client de TNC pertany a una política de conjunt de fitxers sense grups de correccions provisionals ni APAR definits	La política per defecte s'utilitza amb les correccions provisionals i el APAR durant el procés de verificació del client de TNC. Durant el procés de verificació només es fan servir les correccions provisional i els APAR que coincideixen amb el nivell de client de TNC.	No s'utilitza la política per defecte.

Senyaladors

Element	Descripció
-A <nom_advertiment>	Especifica el nom d'advertiment de l'informe.
-B <info_muntatge>	Especifica la informació de muntatge per prepara un informe sobre el pedaç.

-c	Mostra els atributs d'usuari en registres separats per dos punts, tal com s'indica a continuació:
	`# name: atribut1: atribut2: ...`
	`policy: valor1: valor2: ...`

-C	Especifica que l'operació és per al component de client.
-d *ubicació fitxer de base de dades/camí directori de base de dades*	Especifica la ubicació del camí d'accés de fitxer per importar la base de dades, o bé la ubicació del camí d'accés del directori per exportar la base de dades.
-D *aaaa-mm-dd*	Especifica la data per a un client en qüestió a l'historial de registre, on *aaaa* és l'any, *mm* el mes, i *dd* és el dia.
-e *ID_correu_electrònic* **ipgroup=[±]***g1, g2...*	Especifica l'ID de correu electrònic seguit d'una llista de noms de grups d'IP separats per comes.
-E | **FAIL** | **COMPLIANT** | **ALL** |	Especifica l'esdeveniment pel qual cal enviar correus electrònics a l'ID de correu electrònic configurat. FAIL- Els correus s'envien quan l'estat de verificació del client és FAILED. COMPLIANT- Els correus s'envien quan l'estat de verificació del client és COMPLIANT. ALL- Els correus s'envien per a tots els estats de verificació de clients.
-f *nom_fitxer*	Especifica el fitxer des del qual cal llegir la clau del certificat en el cas d'una operació d'importació, o la ubicació en què cal escriure el certificat en cas d'una operació d'exportació.
-F *info_muntatge política_conjunt_fitxers*	Especifica el nom de política del sistema de fitxers, seguit de la informació de muntatge. La informació de muntatge es pot proporcionar en el format següent: `6100-04-01`, on `6100` representa la versió 6.1, `04` és el nivell de manteniment, i `01` és el paquet de servei.
-g	Executa la subordre **clientData** al client de TNC especificat. Aquest senyalador només està disponible amb la subordre **clientData**.

Element	Descripció
-G*nom_grup_ip* **ip=[±]***ip1, ip2...*	Especifica el nom de grup d'IP seguit d'una llista separada per comes.
-H	Llista el registre de l'historial.
-i *amfitrió*	Especifica l'adreça IP o el nom d'amfitrió.
-I ip=[±]*ip1, ip2...* | [±] host1,host2...	Especifica l'IP/nom d'amfitrió que cal passar per alt durant el procés de verificació.
-k *nom_fitxer*	Especifica el fitxer des del qual cal llegir la clau del certificat en el cas d'una operació d'importació.
-l	Llista els detalls de la instantània al servidor de TNC pel client de TNC especificat. Aquest senyalador només està disponible amb la subordre **clientData**.
-O <grup_openpkg>	Especifica el nom de grup openpkg per la política.
-p	Mostra una visualització prèvia de l'actualització del client de TNC.
-P <nom_política>	Especifica el nom de política per preparar un informe de política de client.
-q	Suprimeix la informació de capçalera.
-r *info_muntatge*	Genera l'informe basant-se en la informació de muntatge. La informació de muntatge es pot proporcionar en el format següent: `6100-04-01`, on `6100` representa la versió 6.1, `04` és el nivell de manteniment, i `01` és el paquet de servei.
-R	Especifica que l'operació és per al component IPRef.
-s COMPLIANT | IGNORE | FAILED | ALL	Mostra el client per estat de la manera següent: **COMPLIANT** Mostra els clients actius. **IGNORE** Mostra els clients que s'exclouen d'una verificació. **FAILED** Mostra els clients no han fallat la verificació segons la política configurada. **ALL** Mostra tots els clients independentment dels seus estats.
-S <amfitrió>	Especifica el nom d'amfitrió per preparar un informe de correcció de seguretat de client.
-t TRUSTED | UNTRUSTED	Marca el client especificat com a fiable o no fiable. **Nota:** Només els administradors del sistema poden verificar si servidor o el client és fiable o no fiable.
-T	Especifica que el client pot acceptar sol•licituds de qualsevol servidor de TS que tingui un certificat vàlid.
-u	Desinstal•la una correcció provisional que s'ha instal•lat en un client de TNC.
-v<*CVEid*|*ALL*>	Mostra les exposicions i les vulnerabilitats comuns pels paquets de servei registrats. **CVEid** **All** Mostra totes les exposicions i les vulnerabilitats comuns pels paquets de servei registrats.
-v<*correcció_provisional1, correcció_provisional2,...*>	Especifica una llista de correccions provisionals separades per comes.
-V<*grup_corr_prov*>	Especifica el nom de grup de les correccions provisionals.
-V <*grup_corr_prov*> autoupdate=<yes|no>	Especifica si les correccions provisionals que hi ha al nom de grup de correccions provisionals especificat s'actualitzen automàticament. **Sí** S'actualitza la política definida per fspolicy de forma automàtica quan es reben noves correccions provisionals al servidor de TNC. **No** Especifica que les correccions provisionals noves s'assignaran manualment a la política una vegada les hagi rebut el servidor de TNC. No és el valor per defecte.

Estat de sortida

Aquesta ordre torna els valors de sortida següents:

Element	Descripció
0	L'ordre s'ha executat correctament i s'han realitzat tots els canvis sol•licitats.
>0	S'ha produït un error. El missatge d'error imprès inclou més detalls sobre el tipus de fallada.

Exemples

1. Per iniciar el servidor de TNC, introduïu l'ordre següent:
   ```
   psconf start server
   ```
2. Per afegir una política de sistema de fitxers anomenada `71D_latest` al muntatge `7100-04-02`, introduïu l'ordre següent:
   ```
   psconf add -F 71D_latest 7100-04-02
   ```
3. Per suprimir una política de sistema de fitxers anomenada `71D_old`, introduïu l'ordre següent:
   ```
   psconf delete -F 71D_old
   ```
4. Per validar que el client que té l'adreça IP `11.11.11.11` sigui **fiable**, introduïu l'ordre següent:
   ```
   psconf certadd -i 11.11.11.11 -t TRUSTED
   ```
5. Per suprimir el client que té l'adreça IP `11.11.11.11` del servidor, introduïu l'ordre següent:
   ```
   psconf certdel -i 11.11.11.11
   ```
6. Per verificar la informació del client que té l'adreça IP `11.11.11.11`, introduïu l'ordre següent:
   ```
   psconf verify -i 11.11.11.11
   ```
7. Per visualitzar la informació de client que té l'adreça IP `11.11.11.11`, introduïu l'ordre següent:
   ```
   psconf list -i 11.11.11.11
   ```
8. Per generar l'informe per clients que tinguin l'estat **COMPLIANT**, escriviu l'ordre següent:
   ```
   psconf list -s CPMPLIANT -i ALL
   ```
9. Per generar l'informe per al muntatge `7100-04-02`, introduïu l'ordre següent:
   ```
   psconf list -r 7100-04-02
   ```
10. Per visualitzar l'historial de connexions d'un client que té l'adreça IP `11.11.11.11`, introduïu l'ordre següent:
    ```
    psconf list -H -i 11.11.11.11
    ```
11. Per suprimir l'entrada del client que té l'adreça IP `11.11.11.11` del registre de l'historial anterior o igual a 1 de febrer del 2009, escriviu l'ordre següent:
    ```
    psconf delete -H -i 11.11.11.11 -D 2009-02-01
    ```
12. Per importar el certificat de client d'un client que té l'adreça IP `11.11.11.11` del servidor, introduïu l'ordre següent:
    ```
    psconf import -C -i 11.11.11.11 -f /tmp/client.txt
    ```
13. Per exportar el certificat de servidor des d'un client, introduïu l'ordre següent:
    ```
    psconf export -S -f /tmp/server.txt
    ```
14. Per actualitzar el client que té l'adreça IP `11.11.11.11` a un nivell adequat des del servidor, introduïu l'ordre següent:
    ```
    psconf update -i 11.11.11.11
    ```
15. Per visualitzar els estats del client, introduïu l'ordre següent:
    ```
    psconf status
    ```
16. Per visualitzar el certificat de client, introduïu l'ordre següent:
    ```
    psconf list -C
    ```
17. Per iniciar el client, introduïu l'ordre següent:
    ```
    psconf start client
    ```
18. Per visualitzar la informació d'instantànies que s'ha recopilat amb la subordre **clientData**, escriviu l'ordre següent:
    ```
    psconf clientData -l [ip|host]
    ```

19. Per visualitzar l'historial del client de TNC, escriviu l'ordre següent:
    ```
    psconf list –H –i [ip|ALL]
    ```

Seguretat

Usuaris RBAC d'atenció i usuaris de l'AIX fiables:

Aquesta ordre pot dur a terme operacions privilegiades. Només els usuaris amb privilegis poden executar operacions amb privilegis. Per obtenir més informació sobre les autoritzacions i els privilegis, consulteu Base de dades d'ordres amb privilegis a Seguretat. Per obtenir una llista de privilegis i les autoritzacions associades amb aquesta ordre, consulteu l'ordre **lssecattr** o la subordre **getcmdattr**.

Ordre pscuiserverctl

Finalitat

S'utilitza per configurar les opcions del servidor de la GUI del PowerSC.

Sintaxi

pscuiserverctl -r set [arg1 [arg2 [arg3]]]

pscuiserverctl set [httpPort]

pscuiserverctl set [httpsPort]

pscuiserverctl set [administratorGroupList]

pscuiserverctl set [logonGroupList]

pscuiserverctl set [powervcKeystoneUrl]

pscuiserverctl set [QRadarSyslogResponseEnabled]

pscuiserverctl set [tncServer]

Senyaladors

-r Reinicia el servidor de la GUI del PowerSC després d'aplicar un paràmetre.

set
Estableix o obté una opció del servidor de la GUI del PowerSC.

Paràmetres

httpPort *httpPortno*
Visualitza o especifica el port per defecte que utilitza la GUI del PowerSC.

httpsPort *httpsPortno*
Visualitza o especifica el port segur per defecte que utilitza la GUI del PowerSC.

administratorGroupList *unixgrp1,unixgrp2,...*
Visualitza o especifica els grups UNIX que disposen de permís per dur a terme funcions d'administrador mitjançant la GUI del PowerSC.

logonGroupList *unixgrp1,unixgrp2,...*
Visualitza o especifica els grups UNIX que disposen de permís per iniciar sessió amb la GUI del PowerSC.

powervcKeystoneUrl ***powervcKeystoneurl***
Visualitza o especifica l'URL del servidor del magatzem de claus del PowerVC.

QRadarSyslogResponseEnabled on | off
Visualitza el paràmetre actual del registre Syslog des de la GUI del PowerSC o estableix el registre Syslog en actiu o inactiu.

tncServer ***tncserver.abc.com***
Visualitza o especifica el nom d'amfitrió del servidor de TNC. Si canvieu el nom d'amfitrió del servidor de TNC heu de reiniciar el servidor de la GUI del PowerSC.

Estat de sortida

Aquesta ordre torna els valors de sortida següents:

0 S'ha executat correctament.

>0 S'ha produït un error.

Exemples

1. Per veure què s'ha especificat actualment com a port per defecte utilitzat mitjançant la GUI del PowerSC:
   ```
   pscuiserverctl set httpPort
   ```
2. Per veure el port per defecte que utilitza la GUI del PowerSC:
   ```
   pscuiserverctl set httpPort 80
   ```
3. Per veure què s'ha especificat com a port de seguretat per defecte utilitzat per la GUI del PowerSC:
   ```
   pscuiserverctl set httpsPort
   ```
4. Per veure el port de seguretat per defecte utilitzat per la GUI del PowerSC:
   ```
   pscuiserverctl set httpsPort 483
   ```
5. Per veure quins grups UNIX tenen permís per dur a terme funcions d'administrador utilitzant la GUI del PowerSC:
   ```
   pscuiserverctl set administratorGroupList
   ```
6. Per establir els grups UNIX que disposen de permís per dur a terme funcions d'administrador mitjançant la GUI del PowerSC:
   ```
   pscuiserverctl set administratorGroupList securitygroup1,admingrp1
   ```
7. Per veure quins grups UNIX disposen de permís per iniciar sessió a la GUI del PowerSC:
   ```
   pscuiserverctl set logonGroupList
   ```
8. Per establir els grups UNIX que disposen de permís per iniciar sessió a la GUI del PowerSC:
   ```
   pscuiserverctl set logonGroupList unixgroup1,unixgrp2
   ```
9. Per veure l'URL del servidor del magatzem de claus del PowerVC:
   ```
   pscuiserverctl set powervcKeystoneUrl
   ```
10. Per establir l'URL del servidor del magatzem de claus del PowerVC:
    ```
    pscuiserverctl set powervcKeystoneUrl https://powervc/server/example/
    ```
11. Per veure si el registre Syslog de la GUI del PowerSC està actiu o inactiu:
    ```
    pscuiserverctl set QRadarSyslogResponseEnabled
    ```
12. Per establir el registre Syslog des de la GUI del PowerSC per tal d'activar-lo o desactivar-lo:
    ```
    pscuiserverctl set QRadarSyslogResponseEnabled on
    pscuiserverctl set QRadarSyslogResponseEnabled off
    ```
13. Per veure el nom d'amfitrió del servidor de TNC:
    ```
    pscuiserverctl set tncServer
    ```
14. Per establir el nom d'amfitrió del servidor de TNC:
    ```
    pscuiserverctl set tncServer tncserver.abc.com
    ```

15. L'establiment del nom d'amfitrió del servidor de TNC requereix reiniciar el servidor de la GUI del PowerSC. Per reiniciar el servidor de la GUI del PowerSC:

```
pscuiserverctl -r set tncServer tncs1.rs.com
```

Ordre pscxpert

Finalitat

Ajuda l'administrador del sistema en la configuració dels valors de seguretat

Sintaxi

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

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

pscxpert -f Profile [**-p**] [**-r**|**-R**]

pscxpert -u [**-p**]

pscxpert -c [**-p**] [**-r**|**-R**] [**-P** Profile] [**-l** Level]

pscxpert -t

pscxpert -l <Level> [**-p**] <**-a** *File1* | **-n** *File2* | **-a** *File3* **-n** *File4*>

pscxpert -f Profile **-a** File [**-p**]

pscxpert -d

Descripció

L'ordre **pscxpert** defineix diversos paràmetres de configuració del sistema per habilitar el nivell de seguretat especificat.

Executar l'ordre **pscxpert** només amb el conjunt de senyaladors **-l** implementa els paràmetres de seguretats immediatament sense permetre que l'usuari pugui configurar els paràmetres. Per exemple, l'execució de l'ordre **pscxpert -l high** s'aplica a tots els paràmetres de seguretat de nivell elevat al sistema automàticament. Això no obstant, l'execució de l'ordre **pscxpert -l** amb els senyaladors **-n** i **-a** desa els paràmetres de seguretat en un fitxer especificat mitjançant el paràmetre *File*. El senyalador **-f** s'aplica a les noves configuracions.

Després de la selecció inicial, es mostra un menú amb els elements de totes les opcions de configuració de seguretat associats al nivell de seguretat seleccionat. Aquestes opcions es poden acceptar globalment o desactivar, o bé activar de forma individual. Després dels canvis secundaris, l'ordre **pscxpert** continua aplicant els paràmetres de seguretat al sistema.

Executeu l'ordre **pscxpert** com a usuari root del servidor d'E/S virtual. Quan hagueu iniciat sessió com a usuari root del servidor d'E/S virtual de destinació, executeu l'ordre **oem_setup_env** abans d'executar l'ordre.

Si executeu l'ordre **pscxpert** quan ja s'està executant una altra instància de l'ordre **pscxpert**, s'abandona l'ordre **pscxpert** amb un missatge d'error.

Nota: Torneu a executar l'ordre **pscxpert** després de dur a terme els principals canvis al sistema com, per exemple, la instal•lació o les actualitzacions del programari. Si un element determinat de configuració de seguretat no s'ha seleccionat quan s'ha tornat a executar **pscxpert**, es passarà per alt.

Senyaladors

Element	Descripció
-a	Els valors amb les opcions de nivell de seguretat associades s'escriuen al fitxer especificat en un format abreujat.
-c	Comprova els paràmetres de seguretat en relació al conjunt aplicat de regles. Si aquesta comprovació falla, també es comprovaran les anteriors versions de la regla. Aquest procés continua fins que la comprovació es finalitza, o fins que totes les instàncies de la regla fallida al fitxer `/etc/security/aixpert/core/appliedaixpert.xml` s'han comprovat. Podeu executar aquesta comprovació en qualsevol perfil per defecte o perfil personalitzat.
-d	Mostra la definició del tipus de document (DTD).
-f	Aplica els paràmetres de seguretat que se subministren en el fitxer *Profile* especificat. Els perfils es troben al directori `/etc/security/aixpert/custom`. Els perfils disponibles són els següents perfils estàndard: **DataBase.xml** Aquest fitxer conté els requisits per als paràmetres de base de dades per defecte. **DoD.xml** Aquest fitxer conté els requisits per als paràmetres de Security Technical Implementation Guide (STIG) del Departament de Defensa. **DoD_to_AIXDefault.xml** Això canvia la configuració pels paràmetres per defecte de l'AIX. **DoDv2.xml** Aquest fitxer conté els requisits per a la versió 2 dels paràmetres de Security Technical Implementation Guide (STIG) del Departament de Defensa. **DoDv2_to_AIXDefault.xml** Això canvia la configuració pels paràmetres per defecte de l'AIX. **Hipaa.xml** Aquest fitxer conté els requisits per als paràmetres de la Llei de responsabilitat i portabilitat de l'assegurança mèdica (HIPAA). **NERC.xml** Aquest fitxer conté els requeriments per als paràmetres de la North American Electric Reliability Corporation (NERC). **NERC_to_AIXDefault.xml** Aquest fitxer canvia els paràmetres del NERC pels paràmetres per defecte de l'AIX. **PCI.xml** Aquest fitxer conté els requisits per als paràmetres de seguretat estàndard de les dades del sector de targetes de pagament. **PCIv3.xml** Aquest fitxer conté els requisits per a la versió 3 dels paràmetres de seguretat estàndard de les dades del sector de targetes de pagament. **PCI_to_AIXDefault.xml** Aquest fitxer canvia els paràmetres pels paràmetres per defecte de l'AIX. **PCIv3_to_AIXDefault.xml** Aquest fitxer canvia els paràmetres pels paràmetres per defecte de l'AIX. **SOX-COBIT.xml** Aquest fitxer conté els requisits per als paràmetres de la Llei Sarbanes-Oxley i COBIT.

Element	Descripció
	També podeu crear perfils personalitzats al mateix directori i aplicar-los en els canviant el nom i modificant els fitxers XML existents. Per exemple, l'ordre següent aplica el perfil HIPAA al vostre sistema: `pscxpert -f /etc/security/aixpert/custom/Hipaa.xml` Quan s'especifica el senyalador **-f**, els paràmetres de seguretat s'apliquen coherentment de sistema en sistema transferint i aplicant de forma segura un fitxer **appliedaixpert.xml** de sistema en sistema. Totes les normes aplicades correctament es registren al fitxer `/etc/security/aixpert/core/appliedaixpert.xml` i les normes d'acció de `desfer` corresponents s'escriuen al fitxer `/etc/security/aixpert/core/undo.xml`.
-l	Estableix els paràmetres de seguretat del sistema en el nivell especificat. Aquest senyalador té les opcions següents: **h | high** Especifica les opcions de seguretat de nivell superior. **m | medium** Especifica les opcions de seguretat de nivell mitjà. **l | low** Especifica les opcions de seguretat de nivell baix. **d | default** Especifica les opcions de seguretat de nivells estàndard de l'AIX. **s | sox-cobit** Especifica les opcions de seguretat de la llei Sarbanes-Oxley i del COBIT. Si especifiqueu els senyaladors **-l** i **-n**, els paràmetres de seguretat no s'implementen al sistema; això no obstant, només s'escriuen al fitxer especificat. Totes les normes aplicades correctament es registren al fitxer `/etc/security/aixpert/core/appliedaixpert.xml` i les normes d'acció de desfer corresponents s'escriuen al fitxer `/etc/security/aixpert/core/undo.xml`. **Atenció:** Quan s'utilitza el senyalador **d | default**, el senyalador pot sobreescriure els paràmetres de seguretat configurats que anteriorment havíeu establert utilitzant l'ordre **pscxpert** o de forma independent, i restaura el sistema en la configuració tradicional oberta.
-n	Escriu els paràmetres amb les opcions de nivell de seguretat corresponents en el fitxer especificat.
-p	Especifica que la sortida de les normes de seguretat es mostra utilitzant la sortida detallada. El senyalador **-p** registra les regles que es processen al subsistema d'auditoria si s'activa l'opció **auditing**. Aquesta opció es pot utilitzar amb qualsevol altre dels senyaladors **-l**, **-u**, **-c** i **-f**. El senyalador **-p** habilita la sortida detallada al terminal i al fitxer aixpert.log.
-P	Accepta el nom de perfil com a entrada. Aquesta opció s'utilitza juntament amb els senyaladors **-c**. Els senyaladors **-c** i **-P** s'utilitzen per comprovar la compatibilitat del sistema amb el perfil que s'ha passat.
-r	Escriu els valors existents el sistema al fitxer `/etc/security/aixpert/check_report.txt`. Podeu utilitzar la sortida en informes d'auditoria de seguretat o d'auditoria. L'informe descriu cada valor, com pot estar vinculat a un requisit de conformitat de reglament i si la comprovació ha sigut correcte o ha fallat. **Nota:** • El senyalador -r només admet l'operació d'aplicar als perfils. No admet l'operació aplicar als nivells. • L'opció -r mostra el missatge sencer (una línia o més) d'una regla.
-R	Genera la mateixa sortida que el senyalador **-r**. A més, aquest senyalador afegeix una descripció de l'script o del programa de regles que s'utilitza per implementar el paràmetre de configuració. **Nota:** • El senyalador -R només admet l'operació d'aplicar als perfils. No admet l'operació aplicar als nivells.
-t	Mostra el tipus de perfil que s'aplica al sistema.

Element	Descripció
-u	Desfà la configuració de seguretat que s'han aplicat. **Nota:** • No podeu utilitzar el senyalador **-u** per invertir l'aplicació dels perfils DoD, DoDv2, NERC, PCI o PCIv3. Per eliminar aquests perfils una vegada afegits, apliqueu el perfil que acaba en `_AIXDefault.xml`. Per exemple, per eliminar el perfil NERC.xml, heu d'aplicar el perfil NERC_to_AIXDefault.xml. • Els canvis al sistema després de dur-hi a terme alguna operació es perdran amb una operació de desfer. Els paràmetres tornen al valor que existia abans de l'operació.

Paràmetres

Element	Descripció
Fitxer	El fitxer de sortida que emmagatzema els paràmetres de seguretat. Es necessita permís root per accedir a aquest fitxer.
Nivell	El nivell personalitzat per realitzar una comprovació respecte dels valors aplicats anteriorment.
Perfil	El nom de fitxer del perfil que proporciona les normes de conformitat del sistema. Es necessita permís root per accedir a aquest fitxer.

Seguretat

L'ordre **pscxpert** només es pot executar amb root.

Exemples

1. Per escriure totes les opcions de seguretat de nivell superior a un fitxer de sortida, introduïu l'ordre següent:

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

   Després d'executar aquesta ordre, es pot editar el fiter de sortida i es poden descomentar els rols de seguretat específics escrivint-los en la cadena de comentaris XML estàndard (amb `<--` es comença el comentari i amb `-\>` es tanca el comentari).
2. Per aplicar els valors de seguretat del fitxer de configuració STIG del Departament de Defensa, introduïu l'ordre següent:

   ```
   pscxpert -f /etc/security/aixpert/custom/DoD.xml
   ```
3. Per aplicar els valors de seguretat del fitxer de configuració HIPAA,introduïu l'ordre següent:

   ```
   pscxpert -f /etc/security/aixpert/custom/Hipaa.xml
   ```
4. Per comprovar els paràmetres de seguretat del sistema i registrar les regles que han fallat en un subsistema d'auditoria, escriviu l'ordre següent:

   ```
   pscxpert -c -p
   ```
5. Per comprovar el nivell personalitzat dels paràmetres de seguretat pel perfil del NERC al sistema i per registrar regles que han fallat al subsistema d'auditoria, escriviu l'ordre següent:

   ```
   pscxpert -c -p -l NERC
   ```
6. Per generar informes i escriure'l al fitxer `/etc/security/aixpert/check_report.txt`, escriviu l'ordre següent:

   ```
   pscxpert -c -r
   ```

Ubicació

Element	Descripció
/usr/sbin/pscxpert	Conté l'ordre **pscxpert**.

Fitxers

Element	Descripció
/etc/security/aixpert/log/aixpert.log	Conté un registre de seguiment de valors de seguretat aplicats. Aquest fitxer no utilitza l'estàndard syslog. L'ordre **pscxpert** escriu la informació directament al fitxer, té permís de lectura/gravació i requereix seguretat root.
/etc/security/aixpert/log/firstboot.log	Conté un registre de seguiment dels valors de seguretat que s'han aplicat durant el primer inici de la instal•lació Secure by Default (SbD).
/etc/security/aixpert/core/undo.xml	Conté un llistat XML de cadenes de seguretat que es poden desfer.

Ordre rmvfilt

Finalitat

Elimina les normes de filtre d'encreuament LAN virtual de la taula de filtres.

Sintaxi

rmvfilt -n [**fid**|**all**>]

Descripció

L'ordre **rmvfilt** es fa servir per eliminar les normes de filtre d'encreuament LAN virtual de la taula de filtres.

Senyaladors

-n Especifica l'ID de la norma de filtre que s'eliminarà. S'utilitza l'opció **all** per eliminar totes les normes de filtre.

Estat de sortida

Aquesta ordre torna els valors de sortida següents:

0 S'ha executat correctament.

>0 S'ha produït un error.

Exemples

1. Per eliminar les normes de filtre al kernel, escriviu l'ordre tal com s'indica a continuació:

   ```
   rmvfilt -n all
   ```

Conceptes relacionats:

"Desactivació de regles" a la pàgina 129
Podeu desactivar regles que permetin l'encaminament a través de VLAN en la funció Tallafoc fiable.

Ordre vlantfw

Finalitat

Visualitza o esborra la informació de mapatge d'IP i MAC (Control d'accés als suports d'emmagatzematge) i controla la funció de registre.

Sintaxi

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

Descripció

L'ordre **vlantfw** visualitza o esborra les entrades de mapatge d'IP i MAC. També proporciona la capacitat d'iniciar o aturar el recurs de registre del tallafoc fiable.

Senyaladors

-d Mostra tota la informació de mapatge d'IP.

-D Mostra les dades de connexió recopilades.

-E Mostra les dades de connexió entre les particions lògiques (LPAR) a diferents complexos de processadors centrals.

-f Elimina tota la informació de mapatge d'IP.

-F Esborra la memòria cau de la connexió.

-G Mostra les normes de filtre, que es poden configurar per encaminar el trànsit internament mitjançant el tallafoc fiable.

-I Mostra les dades de connexió entre LPAR associades amb ID de VLAN diferents, però que comparteixen els mateixos complexos de processadors centrals.

-l Inicia el recurs de registre de tallafoc fiable.

-L Atura el recurs de registre del tallafoc fiable i redirigeix el contingut del fitxer de traça al fitxer `/home/padmin/svm/svm.log`.

-m Habilita la supervisió del tallafoc fiable.

-M Inhabilita la supervisió del tallafoc fiable.

-q Consulta l'estat de la màquina virtual segura.

-s Inicia el tallafoc fiable.

-t Atura el tallafoc fiable.

Paràmetres

-N *enter*
Mostra la norma de filtre que correspon al número enter que s'ha especificat.

Estat de sortida

Aquesta ordre torna els valors de sortida següents:

0 S'ha executat correctament.

>0 S'ha produït un error.

Exemples

1. Per veure tots els mapatges d'IP, escriviu l'ordre tal com s'indica a continuació:
   ```
   vlantfw -d
   ```
2. Per eliminar tots els mapatges d'IP, escriviu l'ordre tal com s'indica a continuació:
   ```
   vlantfw -f
   ```
3. Per iniciar la funció de registre del tallafoc fiable, escriviu l'ordre tal com s'indica a continuació:
   ```
   vlantfw -l
   ```

4. Per comprovar l'estat d'una màquina virtual segura, escriviu l'ordre tal com s'indica a continuació:
   ```
   vlantfw -q
   ```
5. Per iniciar el tallafoc fiable, escriviu l'ordre tal com s'indica a continuació:
   ```
   vlantfw -s
   ```
6. Per aturar el tallafoc fiable, escriviu l'ordre tal com s'indica a continuació:
   ```
   vlantfw -t
   ```
7. Per visualitzar les normes corresponents que es poden utilitzar per generar filtres que encaminin el trànsit del complex de processador central, escriviu l'ordre de la manera següent:
   ```
   vlantfw -G
   ```

Referència relacionada:

"Ordre genvfilt" a la pàgina 172

Avisos

Aquesta informació s'ha desenvolupat per als productes i serveis que s'ofereixen als EUA.

És possible que IBM no comercialitzi els productes, serveis o característiques que es descriuen en aquesta documentació a altres països. Poseu-vos en contacte amb el representant d'IBM per saber quins productes i serveis hi ha disponibles al vostre país. Qualsevol referència a un producte, programa o servei d'IBM no signifiquen ni impliquen que només es pugui utilitzar aquest producte, programa o servei d'IBM. Es pot utilitzar qualsevol producte, programa o servei equivalent en funcions que no infringeixi cap dret de propietat intel•lectual d'IBM. Malgrat això, és responsabilitat de l'usuari avaluar i comprovar el funcionament de qualsevol producte, programa o servei que no sigui d'IBM.

IBM pot tenir aplicacions amb patent o pendents de patent que cobreixin el tema descrit en aquest document. El fet de disposar d'aquest document no us dóna cap llicència sobre aquestes patents. Podeu enviar consultes de llicències, per escrit, a:

IBM Director of Licensing
IBM Corporation
North Castle Drive, MD-NC119
Armonk, NY 10504-1785
EUA

Per efectuar consultes en relació a informació sobre el joc de caràcters de doble byte (DBCS), poseu-vos en contacte amb el Departament de propietat intel•lectual d'IBM del vostre país o envieu les consultes, per escrit, a:

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

INTERNATIONAL BUSINESS MACHINES CORPORATION PROPORCIONA AQUESTA PUBLICACIÓ "TAL QUAL" SENSE CAP TIPUS DE GARANTIA, EXPLÍCITA O IMPLÍCITA, INCLOENT-HI, ENTRE D'ALTRES, LES GARANTIES IMPLÍCITES DE NO INFRACCIÓ, COMERCIALITZACIÓ O IDONEÏTAT PER A UNA FINALITAT DETERMINADA. Algunes jurisdiccions no permeten la renúncia de les garanties explícites o implícites en determinades transaccions; per tant, pot ser que aquesta declaració no s'apliqui en el vostre cas.

Aquesta informació pot incloure dades tècniques inexactes o errors tipogràfics. De manera periòdica es realitzen canvis a la informació que s'inclou aquí; aquests canvis s'incorporaran en noves edicions de la publicació. IBM pot incorporar millores o canvis als productes i programes descrits en aquesta publicació sense cap advertiment previ.

Qualsevol referència en aquesta publicació a indrets web que no siguin d'IBM es proporciona només per a la vostra comoditat i de cap manera s'han d'entendre com un aval d'aquests indrets web. La informació d'aquests llocs web no forma part de la informació d'aquest producte d'IBM i l'usuari és responsable de l'ús d'aquests llocs web.

IBM pot utilitzar o distribuir la informació que l'usuari proporcioni de la manera que consideri adequada, sense que això li suposi cap obligació respecte l'usuari.

Les persones que tinguin llicència d'aquest programa i vulguin obtenir-ne informació a efectes de permetre: (i) l'intercanvi d'informació entre programes creats de forma independent i d'altres programes (inclòs aquest) i (ii) l'ús mutu de la informació que s'hagi intercanviat, han de posar-se en contacte amb:

IBM Director of Licensing
IBM Corporation
North Castle Drive, MD-NC119
Armonk, NY 10504-1785
EUA

Aquesta informació pot estar disponible, segons els termes i condicions corresponents, incloent-hi, en alguns casos, el pagament d'una tarifa.

El programa sota llicència descrit en aquesta documentació, i tot el material sota llicència relacionat amb el programa, està proporcionat per IBM d'acord amb els termes de l'IBM Customer Agreement, IBM International Program License Agreement o qualsevol altre acord equivalent entre les parts.

Les dades de rendiment i els exemples de clients citats s'ofereixen únicament amb finalitats il•lustratives. Els resultats de rendiment reals poden variar en funció de les configuracions i condicions operatives específiques.

La informació sobre els productes no IBM s'ha obtingut dels proveïdors d'aquests productes, dels anuncis publicats o altres fonts disponibles públicament. IBM no ha comprovat aquests productes i no pot confirmar la precisió de les afirmacions sobre rendiment, compatibilitat o d'altra mena relacionades amb aquests productes. Els dubtes relacionats sobre els productes no IBM s'han d'adreçar als proveïdors d'aquests productes.

Les declaracions relacionades amb futurs plans o intencions d'IBM estan subjectes a canvi o abandonament sense cap avís previ i només representen propòsits i objectius.

Tots els preus que es mostren són preus de venda al detall suggerits per IBM són actualitzats i poden canviar sense avís previ. Els preus dels subministradors poden variar.

Aquesta informació només es proporciona a efectes de planificació. La informació d'aquest document pot canviar abans que els productes estiguin disponibles.

Aquesta informació conté exemples de dades i informes utilitzats en operacions diàries d'empresa. Perquè siguin el més versemblants possible, els exemples inclouen noms d'individus, companyies, marques i productes. Tots aquests noms són ficticis i qualsevol semblança amb persones o empreses reals és una simple coincidència.

LLICÈNCIA DE COPYRIGHT:

Aquesta informació conté programes d'aplicació d'exemple en llenguatge font, que il•lustren tècniques de programació en diverses plataformes operatives. Podeu copiar, modificar i distribuir aquests programes de mostra en qualsevol format sense haver d'efectuar cap pagament a IBM, amb l'objectiu de desenvolupar, utilitzar, comercialitzar o distribuir programes d'aplicació segons la interfície de programació d'aplicacions per a la plataforma operativa per a la qual estan escrits els programes de mostra. Aquests exemples no s'han provat amb minuciositat sota totes les condicions. Per aquest motiu, IBM no pot garantir ni oferir la fiabilitat, l'operativitat ni el funcionament d'aquests programes. Els programes d'exemple es proporcionen "TAL QUAL", sense cap garantia de cap tipus. IBM no serà responsable dels danys causats per l'ús dels programes d'exemple.

Totes les còpies o parts d'aquests programes de mostra o treballs derivats han d'incloure un avís de copyright com el següent:

© (el nom de la vostra empresa) (any).

Parts d'aquest codi s'han derivat de programes d'exemple d'IBM Corp.

Consideracions de la política de privacitat

Els productes de programari d'IBM, com ara el programari com a solucions del servei, (“Ofertes de programari”) poden utilitzar galetes o altres tecnologies per recopilar informació de l'ús del producte i millorar l'experiència de l'usuari final per adaptar les interacciones amb l'usuari final o per a altres finalitats. En molts casos, les Ofertes de programari no recopilen informació d'identificació personal. Algunes de les nostres Ofertes de programari us poden ajudar a recopilar informació d'identificació personal. En el cas que utilitzin galetes per recopilar aquest tipus d'informació, tot seguit s'indica informació específica sobre l'ús de les galetes que fan aquestes ofertes.

Aquesta Oferta de programari no utilitza galetes ni altres tecnologies per recopilar informació d'identificació personal.

Si les configuracions desplegades per a aquesta Oferta de programari us proporcionen com a client, la capacitat de recopilar informació d'identificació personal d'usuaris finals mitjançant galetes i altres tecnologies, hauríeu de cercar assessorament judicial sobre les lleis aplicables referents a la recopilació de dades i ésser conscient dels requisits de notificació i consentiment.

Si voleu obtenir més informació sobre l'ús de diverses tecnologies i galetes per a la recopilació de dades, consulteu la Política de privadesa d'IBM a http://www.ibm.com/privacy i la Declaració de privadesa en línia d'IBM a http://www.ibm.com/privacy/details; la secció anomenada "Cookies, Web Beacons and Other Technologies” (Galetes, senyals webs i altres tecnologies” i "IBM Software Products and Software-as-a-Service Privacy Statement" (Declaració de privadesa dels productes de programari d'IBM i ofertes de Software-as-a-Service) a http://www.ibm.com/software/info/product-privacy.

Marques registrades

IBM, el logotip d'IBM i ibm.com són marques registrades o marques comercials d'International Business Machines Corp., registrades en moltes jurisdiccions de tot el món. És possible que d'altres productes o noms de servei siguin marques registrades d'IBM o d'altres empreses. Hi ha disponible una llista de les marques registrades d'IBM al lloc web a l'apartat Copyright and trademark information a www.ibm.com/legal/copytrade.shtml.

Linux és una marca registrada de Linus Torvalds als Estats Units, o a d'altres països.

Java i totes les marques registrades i logotips basats en Java són marques registrades de Oracle i/o els seus afiliats.

Índex

M

N

O

P

R

S

T

V

Imprès a Espanya