IBM PowerSC

Standard Edition

Versión 1.1.6

PowerSC Standard Edition

IBM PowerSC

Standard Edition

Versión 1.1.6

PowerSC Standard Edition

Nota

Antes de utilizar esta información y el producto al que da soporte, lea la información del apartado “Avisos” en la página 193.

Esta edición se aplica a IBM PowerSC Standard Edition Versión 1.1.6 y a todos los releases y modificaciones subsiguientes hasta que se indique lo contrario en nuevas ediciones.

Contenido

Acerca de este documento

Este documento proporciona a los administradores de sistema información completa sobre la seguridad de archivo, sistema y red.

Resaltado

Se utilizan los siguientes convenios de resaltado en este documento:

Negrita	Identifica mandatos, subrutinas, palabras clave, archivos, estructuras, directorios y otros elementos cuyos nombres vienen predefinidos por el sistema. También identifica objetos gráficos como botones, etiquetas e iconos que el usuario selecciona.
Cursiva	Identifica los parámetros cuyos nombres o valores reales debe suministrar el usuario.
`Monoespaciado`	Identifica ejemplos de valores de datos específicos, ejemplos de texto similar al que puede ver visualizado, ejemplos de partes de código de programa similar al que puede escribir como programador, mensajes del sistema o información que realmente debe escribir.

Distinción de mayúsculas y minúsculas en AIX

En el sistema operativo AIX todo es sensible a las mayúsculas y minúsculas, lo que significa que establece una distinción entre las letras en mayúsculas y en minúsculas. Por ejemplo, puede utilizar el mandato **ls** para obtener una lista de archivos. Si escribe `LS`, el sistema responde que el mandato `no se encuentra`. Del mismo modo, `FILEA`, `FiLea`, y `filea` son tres nombres de archivos distintos, aunque residan en el mismo directorio. Para evitar que se produzcan acciones no deseadas, asegúrese siempre de utilizar el tipo de letra, mayúsculas o minúsculas, correcto.

ISO 9000

En el desarrollo y la fabricación de este producto se han utilizado sistemas de calidad registrados ISO 9000.

Novedades de PowerSC Standard Edition

Lea información nueva o significativamente cambiada sobre la recopilación del tema de la versión de PowerSC Standard Edition.

En este archivo PDF, puede que vea barras de revisión (|) en el margen izquierdo que identifica información nueva y modificada.

Septiembre de 2017

Se han añadido las características siguientes para la GUI de PowerSC:

- Se ha añadido un panel de instrumentos de seguridad y conformidad de alto nivel que proporciona un resumen a simple vista de toda la información de estado de integridad de archivo en tiempo real y de conformidad.
- Se ha añadido integración con gestores de virtualización, como por ejemplo PowerVC a través de la integración de Open Stack, proporcionando un descubrimiento seguro de puntos finales. Además, la integración soporta un entorno de nube con visibilidad de seguridad desde el primer momento de creación de VM.
- Se han añadido funciones de informes para soportar auditorías. Ahora hay informes sobre la visión general y la integridad de archivos y conformidad de disponibles en formato HTML y como archivo CSV. Estos informes pueden programarse para su distribución inmediata o a diario.
- El Editor de perfiles mejorados mejora la capacidad para personalizar los perfiles y las reglas de conformidad. Ahora las reglas pueden combinarse de varias fuentes y editarse a través de la GUI.
- Se ha añadido integración con los gestores de información de suceso de seguridad como QRadar. Si se proporcionan entradas de Syslog para sucesos de integridad de archivos y conformidad significativos, la integridad es fácil.
- Las capacidades UNDO mejoradas ayudan a simplificar la tarea compleja de deshacer un perfil aplicado. PowerSC 1.1.6 realiza pasos significativos hacia una capacidad UNDO continua con el perfil PCI.
- Se ha mejorado la escalabilidad de GUI para la conformidad. El servidor de GUI es escalable horizontalmente y cada instancia puede soportar un máximo de 1.000 puntos finales o más.

Se han añadido las siguientes características para Trusted Network Connect Patch Management (TNCPM):

- Se presenta un servidor proxy que proporciona una capa adicional de seguridad permitiendo que TNCPM se aísle de Internet.
- La integración de arreglos provisionales (iFixes) en TNCPM está ahora totalmente automatizado. TNCPM puede supervisar y revisar las vulnerabilidades aplicables al sistema operativo sin necesidad de intervención del usuario.
- Descarga de paquetes de código abierto está ahora integrado en TNCPM, racionalizando el flujo de trabajo de código abierto.

Se ha añadido la siguiente característica para mejorar las capacidades de conformidad:

- Se ha añadido una opción de informe que proporciona detalles sobre las reglas incluidas en un perfil cuando se aplica.

Archivos PDF de PowerSC Standard Edition

Puede ver la documentación de PowerSC Standard Edition como archivos PDF.

- PowerSC Standard Edititon
- Notas del release de PowerSC Standard Edition

Conceptos sobre PowerSC Standard Edition

Esta visión general de PowerSC Standard Edition explica las características, los componentes y el soporte de hardware relacionados con la característica PowerSC Standard Edition.

PowerSC Standard Edition proporciona seguridad y control de los sistemas operativos en una nube o en centros de datos virtualizados y proporciona una vista empresarial y prestaciones de gestión. PowerSC Standard Edition es un conjunto de características que incluye Automatización de la seguridad y conformidad, Arranque fiable, Cortafuegos fiable, Registro fiable y Trusted Network Connect and Patch Management. La tecnología de seguridad que se pone en la capa de virtualización proporciona seguridad adicional a los sistemas autónomos.

La tabla siguiente proporciona detalles sobre el ediciones, las características incluidas en las ediciones, los componentes y el hardware basado procesador en el que cada componente está disponible.

Tabla 1. Componentes, descripción, soporte de sistema operativo y soporte de hardware de PowerSC Standard Edition

Componentes	Descripción	Sistema operativo soportado	Hardware soportado
Automatización de la seguridad y conformidad	Automatiza el establecimiento, la supervisión y la auditoría de la configuración de la seguridad y conformidad para los estándares siguientes: • Payment Card Industry Data Security Standard (PCI DSS) • Conformidad con la ley Sarbanes-Oxley y COBIT (SOX/COBIT) • U.S. Department of Defense (DoD) STIG • Health Insurance Portability and Accountability Act (HIPAA)	• AIX 5.3 • AIX 6.1 • AIX 7.1 • AIX 7.2	• POWER5 • POWER6 • POWER7 • POWER8
Arranque fiable	Mide la imagen de arranque, el sistema operativo y las aplicaciones y demuestra su confianza utilizando la tecnología de módulo de plataforma fiable (TPM) virtual.	• AIX 6 con 6100-07 o posterior • AIX 7 con 7100-01 o posterior	Firmware POWER7 eFW7.4 o posterior
Cortafuegos fiable	Ahorra tiempo y recursos habilitando el direccionamiento dirigido a través de LAN virtuales (VLAN) especificadas controladas por el mismo Virtual I/O Server.	• AIX 6.1 • AIX 7.1 • AIX 7.2 • VIOS Versión 2.2.1.4 o posterior	• POWER6 • POWER7 • POWER8 • Virtual I/O Server Versión 6.1S o posterior
Registro fiable	Los registros de AIX se encuentran en una ubicación central en Virtual I/O Server (VIOS) en tiempo real. Esta característica proporciona la creación de registros segura y la copia de seguridad y la gestión prácticas de los registros.	• AIX 5.3 • AIX 6.1 • AIX 7.1 • AIX 7.2	• POWER5 • POWER6 • POWER7 • POWER8

Tabla 1. Componentes, descripción, soporte de sistema operativo y soporte de hardware de PowerSC Standard Edition (continuación)

Componentes	Descripción	Sistema operativo soportado	Hardware soportado
Trusted Network Connect and Patch Management	Verifica que todos los sistemas AIX del entorno virtual estén en el nivel de software y parche especificado y proporciona herramientas de gestión para asegurarse de que todos los sistemas AIX están en el nivel de software especificado. Proporciona alertas si se añade a la red un sistema virtual de nivel inferior o si se emite un parche de seguridad que afecta a los sistemas.	• AIX 5.3 • AIX 6.1 • AIX 7.1 • AIX 7.2	• POWER5 • POWER6 • POWER7 • POWER8
Cliente de Trusted Network Connect	El cliente de Trusted Network Connect necesita uno de los componentes listados con el sistema operativo.	• AIX 6.1 con 6100-06 o posterior • Sistema de consola de Service Update Management Assistant (SUMA) de AIX versión 7.1 en el entorno de SUMA para la gestión de parches • Consola de sistema de Service Update Management Assistant (SUMA) de AIX versión 7.2.1 en el entorno de SUMA para la gestión de parches	

Instalación de PowerSC Standard Edition

Debe instalar un conjunto de archivos para cada función específica de PowerSC Standard Edition.

Los siguientes conjuntos de archivos están disponibles para PowerSC Standard Edition y la Interfaz gráfica de usuario (GUI) de PowerSC:

- `powerscStd.ice`: se instala en sistemas AIX que necesitan la característica de Automatización de la seguridad y conformidad de PowerSC Standard Edition. El programa de conformidad necesita como mínimo 5 MB de espacio de disco disponible en el sistema de archivos "/".
- `powerscStd.vtpm`: se instala en sistemas AIX que necesitan la característica de Arranque fiable de PowerSC Standard Edition. Puede obtener el conjunto de archivos powerscStd.vtpm en el soporte base de AIX o en https://www-01.ibm.com/marketing/iwm/iwm/web/preLogin.do?source=aixbp &S_PKG=vtpm.
- `powerscStd.vlog`: se instala en sistemas AIX que necesitan la característica Registro fiable de PowerSC Standard Edition.
- `powerscStd.tnc_pm`: se instala en AIX Versión 7.1 TL4 o posterior, con el sistema de consola SUMA (Service Update Management Assistant) en el entorno de SUMA para la gestión de parches en 7.2.1.0. Curl 7.52.1-1 debe instalarse en TNC Patch Manager para la transmisión segura de arreglos temporales del sitio de seguridad de IBM.
- `powerscStd.svm`: se instala en sistemas AIX que pueden beneficiarse de la característica de direccionamiento de PowerSC Standard Edition.
- `powerscStd.rtc`: se instala en sistemas AIX que necesitan la característica Conformidad en tiempo real de PowerSC Standard Edition.
- `powerscStd.uiAgent.rte`: se instala en sistemas AIX que se gestionarán utilizando la Interfaz gráfica de usuario (GUI) de PowerSC. Se necesita el conjunto de archivos powerscStd.ice 115 o superior para instalar powerscStd.uiAgent.rte 116.
- `powerscStd.uiServer.rte`: se instala en el sistema AIX configurado específicamente para ejecutar el servidor de la Interfaz gráfica de usuario (GUI) de PowerSC.

Puede instalar PowerSC Standard Edition y la Interfaz gráfica de usuario (GUI) de PowerSC utilizando una de las interfaces siguientes:

- El mandato **installp** de la interfaz de línea de mandatos (CLI)
- La interfaz SMIT

Para instalar PowerSC Standard Edition utilizando la interfaz SMIT, siga los pasos siguientes:

1. Ejecute el siguiente mandato:
   ```
   % smitty installp
   ```
2. Seleccione la opción **Instalar software**.
3. Seleccione el dispositivo de entrada o directorio para el software para especificar la ubicación y el archivo de instalación de la imagen de instalación de IBM Compliance Expert. Por ejemplo, si la imagen de instalación tiene la vía de acceso de directorio y el nombre de archivo `/usr/sys/inst.images/powerscStd.vtpm`, debe especificar la vía de acceso de archivo en el campo **INPUT**.
4. Vea y acepte el acuerdo de licencia. Acepte el acuerdo de licencia utilizando la flecha abajo para seleccionar **ACEPTAR nuevos acuerdos de licencia** y pulse la tecla de tabulación para cambiar el valor a **Sí**.
5. Pulse **Intro** para iniciar la instalación.
6. Verifique que el estado del mandato sea **Correcto** después de que la instalación se haya completado.

Consulte “Instalación de la GUI de PowerSC” en la página 147 para obtener más información sobre la instalación de la Interfaz gráfica de usuario (GUI) de PowerSC

Visualización de la licencia de software

La licencia de software puede verse en la CLI utilizando el mandato siguiente:

```
% installp –lE –d vía_acceso/nombre_archivo
```

Donde *vía_acceso/nombre_archivo* especifica la imagen de instalación de PowerSC Standard Edition.

Por ejemplo, puede especificar el mandato siguiente utilizando la CLI para especificar la información de licencia relacionada con PowerSC Standard Edition:

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

Conceptos relacionados:

“Conceptos sobre PowerSC Standard Edition” en la página 5
Esta visión general de PowerSC Standard Edition explica las características, los componentes y el soporte de hardware relacionados con la característica PowerSC Standard Edition.

“Instalación del arranque fiable” en la página 113
Hay algunas configuraciones de hardware y software necesarias que se requieren para instalar el Arranque fiable.

Tareas relacionadas:

“Instalación del Cortafuegos fiable” en la página 121
La instalación del Cortafuegos fiable de PowerSC es similar a la instalación de otras características de PowerSC.

“Instalación del Registro fiable” en la página 128
Puede instalar la característica Registro fiable de PowerSC utilizando la interfaz de línea de mandatos o la herramienta SMIT.

“Configuración de los componentes de TNC” en la página 134
Cada uno de los componentes de Trusted Network Connect (TNC) necesita configuración para ejecutarse en el entorno específico.

Automatización de la seguridad y conformidad

AIX Profile Manager gestiona los perfiles predefinidos para la seguridad y conformidad. PowerSC Conformidad en tiempo real supervisa continuamente los sistemas AIX habilitados para asegurarse de que están configurados de forma coherente y segura.

Los perfiles XML automatizan la configuración de sistema AIX recomendada de IBM para ser coherente con Payment Card Data Security Standard, la ley Sarbanes-Oxley o U.S. Department of Defense UNIX Security Technical Implementation Guide y Health Insurance Portability and Accountability Act (HIPAA). Las organizaciones que cumplan con los estándares de seguridad deben utilizar los valores de seguridad de sistema predefinidos.

AIX Profile Manager funciona como un plug-in de IBM® Systems Director que simplifica la aplicación de valores de seguridad, la supervisión de valores de seguridad y la auditoría de valores de seguridad para el sistema operativo AIX y los sistemas Virtual I/O Server (VIOS). Para utilizar la característica de conformidad de seguridad, la aplicación PowerSC debe instalarse en los sistemas gestionados AIX que cumplen con los estándares de conformidad. La característica de Automatización de la seguridad y conformidad se incluye en PowerSC Standard Edition.

El paquete de instalación de PowerSC Standard Edition, 5765-PSE, debe instalarse en sistemas gestionados AIX. El paquete de instalación instala el conjunto de archivos `powerscStd.ice` que puede implementarse en el sistema utilizando AIX Profile Manager o el mandato **pscxpert**. PowerSC con la conformidad de IBM Compliance Expert Express (ICEE) está habilitado para gestionar y mejorar los perfiles XML. AIX Profile Manager gestiona los perfiles XML.

Nota: Instale todas las aplicaciones en el sistema antes de aplicar un perfil de seguridad.

Conceptos sobre la Automatización de la seguridad y conformidad

La característica de seguridad y conformidad de PowerSC es un método automatizado para configurar y auditar sistemas AIX de acuerdo con U.S. Department of Defense (DoD) Security Technical Implementation Guide (STIG), Payment Card Industry (PCI) Data Security Standard (DSS), la ley Sarbanes-Oxley, conformidad COBIT (SOX/COBIT) y Health Insurance Portability and Accountability Act (HIPAA).

PowerSC ayuda a automatizar la configuración y supervisión de los sistemas que deben ser compatible con Payment Card Industry (PCI) Data Security Standard (DSS) versión 1.2, 2.0, o 3.0. Por consiguiente, la característica de seguridad y conformidad de PowerSC es un método preciso y completo de automatización de configuración de seguridad que se utiliza para satisfacer los requisitos de conformidad con la TI de DoD UNIX STIG, PCI DSS, la ley Sarbanes-Oxley, conformidad COBIT (SOX/COBIT) y Health Insurance Portability and Accountability Act (HIPAA).

Nota: La seguridad y conformidad de PowerSC actualizan los perfiles XML existentes utilizados por la edición IBM Compliance Expert Express (ICEE). Puede utilizar los perfiles XML de PowerSC Standard Edition con el mandato **pscxpert**, similar a ICEE.

Los perfiles de conformidad preconfigurados que se entregan con PowerSC Standard Edition reducen la carga de trabajo administrativa de interpretar la documentación de conformidad y de implementar los estándares como parámetros de configuración de sistema específicos. Esta tecnología reduce el coste de configuración y auditoría de conformidad automatizando los procesos. IBMPowerSC Standard Edition está diseñado para ayudar a gestionar eficazmente el requisito de sistema asociado con la conformidad de estándar externo que potencialmente puede reducir los costes y mejorar la conformidad.

Conformidad con Department of Defense STIG

El Department of Defense (DoD) de EE.UU. necesita sistemas informáticos altamente seguros. Este nivel de seguridad y calidad definido por DoD cumple con la calidad y la base de clientes de AIX en el servidor Power Systems.

Un sistema operativo seguro, como AIX, debe configurarse con precisión para conseguir los objetivos de seguridad especificados. En la Directiva 8500.1, el DoD reconoció la necesidad de configuraciones de seguridad de todos los sistemas operativos. Esta directiva establecía la política y asignaba la responsabilidad a la agencia de seguridad de la información de defensa (DISA) de EE.UU. para proporcionar orientación de configuración de seguridad.

DISA elaboró los principios y directrices en la publicación UNIX Security Technical Implementation Guide (STIG) que proporciona un entorno que cumple o supera los requisitos de seguridad de los sistemas de DoD que están funcionando a nivel confidencial II de categoría de garantía de misión (MAC, que contiene información confidencial. El DoD de EE.UU. tiene requisitos de seguridad de TI estrictos y enumeraba los detalles de los valores de configuración necesarios para asegurar que el sistema funciona de una manera segura, Puede utilizar la orientación de expertos necesaria. PowerSC Standard Edition ayuda a automatizar el proceso de configuración de los valores tal como se ha definido en DoD.

Nota: Todos los archivos de script personalizado que se proporcionan para mantener la conformidad DoD están en el auditorio `/etc/security/pscexpert/dodv2`.

PowerSC Standard Edition soporta los requisitos de la versión 1 release 2 de la STIG de DoD de AIX. Un resumen de los requisitos y cómo garantizar que se proporcionan conformidad en las tablas que siguen.

Tabla 2. Requisitos generales de DoD

ID de punto de comprobación de Department of Defense STIG	Categoría de la regla de STIG	Descripción	Ubicación del script donde se define la acción y los resultados de la acción que permite la conformidad
AIX00020	2	Se debe implementar el software de AIX Trusted Computing Base.	**Ubicación** `/etc/security/pscexpert/dodv2/trust` **Acción de conformidad** Asegura que el sistema cumpla los requisitos especificados.
AIX00040	2	Se debe utilizar el mandato **securetcpip**.	**Ubicación** `/etc/security/pscexpert/dodv2/dodsecuretcpip` **Acción de conformidad** Asegura que el sistema cumpla los requisitos especificados.
AIX00060	2	El sistema debe comprobarse semanalmente para ver si hay archivos `setuid` no autorizados y modificación no autorizada en archivos `setuid` autorizados.	**Ubicación** `/etc/security/pscexpert/dodv2/trust` **Acción de conformidad** Comprueba semanalmente para identificar cambios en los archivos especificados.

Tabla 2. Requisitos generales de DoD (continuación)

ID de punto de comprobación de Department of Defense STIG	Categoría de la regla de STIG	Descripción	Ubicación del script donde se define la acción y los resultados de la acción que permite la conformidad
AIX00080	1	El atributo `SYSTEM` no debe establecerse en *none* para ninguna cuenta.	**Ubicación** `/etc/security/pscexpert/dodv2/SYSattr` **Acción de conformidad** Asegura que el atributo especificado se establezca en un valor distinto de *none*. **Nota:** Este valor no cambia automáticamente cuando la política se restablece en la política predeterminada de AIX utilizando el archivo `DoDv2_to_AIXDefault.xml`. Debe cambiar manualmente este valor.
AIX00200	2	El sistema no debe permitir que las difusiones dirigidas se desplacen a través de la pasarela.	**Ubicación** `/etc/security/pscexpert/dodv2/ntwkoptsdod` **Acción de conformidad** Establece el valor de la opción de red `direct_broadcast` en *0*.
AIX00210	2	El sistema debe proporcionar protección contra ataques de ICMP (Protocolo de mensajes de control de Internet) en conexiones TCP.	**Ubicación** `/etc/security/pscexpert/dodv2/ntwkoptsdod` **Acción de conformidad** Establece el valor de la opción de red `tcp_icmpsecure` en *1*.
AIX00220	2	El sistema debe proporcionar protección para la pila TCP contra los restablecimientos de conexión, la sincronización (SYN) y los ataque por inyección de datos.	**Ubicación** `/etc/security/pscexpert/dodv2/ntwkoptsdod` **Acción de conformidad** Asegura que el valor de la opción de red `tcp_tcpsecure` se establece en *7*.
AIX00230	2	El sistema debe proporcionar protección contra ataques de fragmentación de IP.	**Ubicación** `/etc/security/pscexpert/dodv2/ntwkoptsdod` **Acción de conformidad** Establece el valor de la opción de red `ip_nfrag` en *200*.
AIX00300	1,2,3	El sistema no debe tener el servicio `bootp` activo.	**Ubicación** `/etc/security/pscexpert/dodv2/inetdservices` **Acción de conformidad** Inhabilita el servicio especificado.
AIX00310	2	Los archivos `/etc/ftpaccess.ctl` deben existir.	**Ubicación** `/etc/security/pscexpert/dodv2/dodv2loginherald` **Acción de conformidad** Asegura que el archivo existe.

Tabla 2. Requisitos generales de DoD (continuación)

ID de punto de comprobación de Department of Defense STIG	Categoría de la regla de STIG	Descripción	Ubicación del script donde se define la acción y los resultados de la acción que permite la conformidad
GEN000020	2	El sistema debe requerir autenticación al iniciar en la modalidad de un solo usuario.	**Ubicación** `/etc/security/pscexpert/dodv2/rootpasswd_home` **Acción de conformidad** Asegura que la cuenta root para las particiones arrancables tiene una contraseña en el archivo `/etc/security/passwd`. **Nota:** Este valor no cambia automáticamente cuando la política se restablece en la política predeterminada de AIX utilizando el archivo `DoDv2_to_AIXDefault.xml`. Debe cambiar manualmente este valor.
GEN000100	1	El sistema operativo debe ser un release soportado.	**Ubicación** `/etc/security/pscexpert/dodv2/dodv2cat1` **Acción de conformidad** Muestra los resultados de las pruebas de regla especificadas.

GEN000120	2	Se deben instalar los parches y las actualizaciones de seguridad de sistema más actuales.	**Ubicación**
			`/usr/sbin/instfix -i`
			`/etc/security/pscexpert/dodv2/dodv2cat1`
			Acción de conformidad
			Configure esto utilizando la característica Trusted Network Connect.

GEN000140	2	El sistema debe comprobarse semanalmente para ver si hay archivos `setuid` no autorizados y modificación no autorizada en archivos `setuid` autorizados.	**Ubicación** `/etc/security/pscexpert/dodv2/trust` **Acción de conformidad** Comprueba semanalmente para identificar cambios en los archivos especificados.
GEN000220	2	El sistema debe comprobarse semanalmente para ver si hay archivos `setuid` no autorizados y modificación no autorizada en archivos `setuid` autorizados.	**Ubicación** `/etc/security/pscexpert/dodv2/trust` **Acción de conformidad** Comprueba semanalmente para identificar cambios en los archivos especificados.
GEN000240	2	El reloj del sistema debe estar sincronizado con un origen de tiempo del Department of Defense (DoD) autorizado.	**Ubicación** `/etc/security/pscexpert/dodv2/dodv2cmntrows` **Acción de conformidad** Asegura que el reloj del sistema es compatible.
GEN000241	2	El reloj del sistema debe sincronizarse continuamente o como mínimo a diario.	**Ubicación** `/etc/security/pscexpert/dodv2/dodv2cmntrows` **Acción de conformidad** Asegura que el reloj del sistema es compatible.

Tabla 2. Requisitos generales de DoD (continuación)

ID de punto de comprobación de Department of Defense STIG	Categoría de la regla de STIG	Descripción	Ubicación del script donde se define la acción y los resultados de la acción que permite la conformidad
GEN000242	2	El sistema debe utilizar como mínimo dos orígenes de tiempo para la sincronización del reloj.	**Ubicación** `/etc/security/pscexpert/dodv2/dodv2netrules` **Acción de conformidad** Asegura que se utilice más de un origen de tiempo para sincronizar el reloj.
GEN000280	2	No se deben permitir inicios de sesión directos en los siguientes tipos de cuentas: • aplicación • predeterminada • compartida • programa de utilidad	**Ubicación** `/etc/security/pscexpert/dodv2/lockacc_rlogin` **Acción de conformidad** Impide inicios de sesión directos en las cuentas especificadas.
GEN000290	2	El sistema no debe tener cuentas innecesarias.	**Ubicación** `/etc/security/pscexpert/dodv2/lockacc_rlogin` **Acción de conformidad** Asegura que no haya cuentas no utilizadas.
GEN000300 (relacionado con GEN000320, GEN000380, GEN000880)	2	Todas las cuentas del sistema deben tener nombres de usuario o cuenta exclusivos y contraseñas de usuario o cuenta exclusivas.	**Ubicación** `/etc/security/pscexpert/dodv2/grpusrpass_chk` **Acción de conformidad** Asegura que todas las cuentas cumplan los requisitos especificados. **Nota:** Este valor no cambia automáticamente cuando la política se restablece en la política predeterminada de AIX utilizando el archivo `DoDv2_to_AIXDefault.xml`. Debe cambiar manualmente este valor.
GEN000320 (relacionado con GEN000300, GEN000380, GEN000880)	2	Todas las cuentas del sistema deben tener nombres de usuario o cuenta exclusivos y contraseñas de usuario o cuenta exclusivas.	**Ubicación** `/etc/security/pscexpert/dodv2/grpusrpass_chk` **Acción de conformidad** Asegura que todas las cuentas cumplan los requisitos especificados. **Nota:** Este valor no cambia automáticamente cuando la política se restablece en la política predeterminada de AIX utilizando el archivo `DoDv2_to_AIXDefault.xml`. Debe cambiar manualmente este valor.
GEN000340	2	Los ID de usuario (UID) y los ID de grupo (GID) que están reservados para las cuentas de sistema no se deben asignar a cuentas que no son de sistema y grupos que no son de sistema.	**Ubicación** `/etc/security/pscexpert/dodv2/account` **Acción de conformidad** Este valor se habilita automáticamente para aplicar esta regla.

Tabla 2. Requisitos generales de DoD (continuación)

ID de punto de comprobación de Department of Defense STIG	Categoría de la regla de STIG	Descripción	Ubicación del script donde se define la acción y los resultados de la acción que permite la conformidad
GEN000360	2	Los UID y los GID que están reservados para cuentas de sistema no se deben asignar a cuentas que no son de sistema y grupos que no son de sistema.	**Ubicación** `/etc/security/pscexpert/dodv2/account` **Acción de conformidad** Este valor se habilita automáticamente para aplicar esta regla.
GEN000380 (relacionado con GEN000300, GEN000320, GEN000880)	2	Todas las cuentas del sistema deben tener nombres de usuario o cuenta exclusivos y contraseñas de usuario o cuenta exclusivas.	**Ubicación** `/etc/security/pscexpert/dodv2/grpusrpass_chk` **Acción de conformidad** Asegura que todas las cuentas cumplan los requisitos especificados.
GEN000400	2	El banner de inicio de sesión de DoD (Department of Defense) debe visualizarse inmediatamente antes, o como parte, de las solicitudes de inicio de sesión de consola.	**Ubicación** `/etc/security/pscexpert/dodv2/dodv2loginherald` **Acción de conformidad** Visualiza el banner necesario.
GEN000402	2	Se debe visualizar el banner de inicio de sesión de DoD inmediatamente antes, o como parte, de las solicitudes de inicio de sesión de entorno de escritorio gráfico.	**Ubicación** `/etc/security/pscexpert/dodv2/dodv2loginherald` **Acción de conformidad** El banner de inicio de sesión se establece en el banner de Department of Defense.
GEN000410	2	El servicio FTPS (Protocolo de transferencia de archivos sobre SSL) o FTP (Protocolo de transferencia de archivos) del sistema se debe configurar con el banner de inicio de sesión de DoD.	**Ubicación** `/etc/security/pscexpert/dodv2/dodv2loginherald` **Acción de conformidad** Visualiza el banner cuando se utiliza FTP.
GEN000440	2	Se deben registrar los intentos satisfactorios y no satisfactorios de inicio de sesión y de cierre de sesión.	**Ubicación** `/etc/security/pscexpert/dodv2/loginout` **Acción de conformidad** Habilita el registro necesario.
GEN000452	2	El sistema debe visualizar la fecha y hora del último inicio de sesión de cuenta satisfactorio en el momento de cada inicio de sesión.	**Ubicación** `/etc/security/pscexpert/dodv2/sshDoDconfig` **Acción de conformidad** Visualiza la información necesaria.

Tabla 2. Requisitos generales de DoD (continuación)

ID de punto de comprobación de Department of Defense STIG	Categoría de la regla de STIG	Descripción	Ubicación del script donde se define la acción y los resultados de la acción que permite la conformidad
GEN000460	2	Esta regla inhabilita una cuenta después de 3 intentos de inicio de sesión erróneos consecutivos.	**Ubicación** `/etc/security/pscexpert/dodv2/chusrattrdod` **Acción de conformidad** Establece el límite de intentos de inicio de sesión en el valor especificado.
GEN000480	2	Esta regla establece el tiempo de retardo de inicio de sesión en 4 segundos.	**Ubicación** `/etc/security/pscexpert/dodv2/chdefstanzadod` **Acción de conformidad** Establece el tiempo de retardo de inicio de sesión en el valor necesario.
GEN000540	2	Esta regla asegura que los archivos de configuración de contraseña globales de sistema estén configurados según los requisitos de contraseña.	**Ubicación** `/etc/security/pscexpert/dodv2/chusrattrdod` **Acción de conformidad** Establece los valores de contraseña necesarios.
GEN000560	1	Todas las cuentas del sistema deben tener contraseñas válidas.	**Ubicación** `/etc/security/pscexpert/dodv2/grpusrpass_chk` **Acción de conformidad** Asegura que las cuentas tengan contraseñas.
GEN000580	2	Esta regla asegura que todas las contraseñas tengan un mínimo de 14 caracteres.	**Ubicación** `/etc/security/pscexpert/dodv2/chusrattrdod` **Acción de conformidad** Establece la longitud mínima de contraseña en 14 caracteres.
GEN000585	2	El sistema debe utilizar un algoritmo de hash criptográfico aprobado 140-2 de FIPS (Estándar federal de procesamiento de información) para generar hashes de contraseña de cuenta.	**Ubicación** `/etc/security/pscexpert/dodv2/fipspasswd` **Acción de conformidad** Asegura que los hashes de contraseña utilicen un algoritmo de hash aprobado.
GEN000590	2	El sistema debe utilizar un algoritmo de hash criptográfico aprobado FIPS 140-2 para generar hashes de contraseña de cuenta.	**Ubicación** `/etc/security/pscexpert/dodv2/fipspasswd` **Acción de conformidad** Asegura que los hashes de contraseña utilicen un algoritmo de hash aprobado.
GEN000595	2	Utilice un algoritmo de hash criptográfico aprobado FIPS 140-2 al generar los hash de contraseña que se almacenan en el sistema.	**Ubicación** `/etc/security/pscexpert/dodv2/fipspasswd` **Acción de conformidad** Asegura que los hashes de contraseña utilicen un algoritmo de hash aprobado.

Tabla 2. Requisitos generales de DoD (continuación)

ID de punto de comprobación de Department of Defense STIG	Categoría de la regla de STIG	Descripción	Ubicación del script donde se define la acción y los resultados de la acción que permite la conformidad
GEN000640	2	Esta regla necesita un mínimo de un carácter no alfabético en una contraseña	**Ubicación** `/etc/security/pscexpert/dodv2/chusrattrdod` **Acción de conformidad** Establece el número mínimo de caracteres no alfabéticos de una contraseña en 1.
GEN000680	2	Esta regla asegura que las contraseñas no contengan más de tres caracteres repetidos consecutivos	**Ubicación** `/etc/security/pscexpert/dodv2/chusrattrdod` **Acción de conformidad** Establece el número máximo de caracteres repetidos de una contraseña en 3.
GEN000700	2	Esta regla asegura que los archivos de configuración de contraseña globales de sistema estén configurados según los requisitos de contraseña.	**Ubicación** `/etc/security/pscexpert/dodv2/chusrattrdod` **Acción de conformidad** Asegura que los archivos de configuración de contraseña cumplan los requisitos.

GEN000740	2	Todas las contraseñas de cuenta de proceso automatizado y no interactivo se deben bloquear (GEN000280). No se deben permitir inicios de sesión directos en cuentas de programa de utilidad, o aplicación, predeterminadas o compartidas. (GEN002640) Las cuentas de sistema predeterminadas se deben inhabilitar o eliminar.	**Ubicación**
			`/etc/security/pscexpert/dodv2/loginout`
			`/etc/security/pscexpert/dodv2/lockacc_rlogin`
			Acción de conformidad
			Este valor se habilita automáticamente.

GEN000740	2	Todas las contraseñas de cuenta de proceso automatizado y no interactivo se deben cambiar al menos una vez por año o bloquear.	**Ubicación** `/etc/security/pscexpert/dodv2/lockacc_rlogin` **Acción de conformidad** Asegura que las contraseñas especificadas se cambien anualmente o se bloqueen.
GEN000750	2	Esta regla requiere nuevas contraseñas para contener un mínimo de 4 caracteres que no estaban en la contraseña anterior.	**Ubicación** `/etc/security/pscexpert/dodv2/chusrattrdod` **Acción de conformidad** Establece en 4 el número mínimo de caracteres nuevos que son necesarios en una nueva contraseña.
GEN000760	2	Las cuentas deben bloquearse después de 35 días de inactividad.	**Ubicación** `/etc/security/pscexpert/dodv2/disableacctdod` **Acción de conformidad** Bloquea las cuentas después de 35 días de inactividad.

Tabla 2. Requisitos generales de DoD (continuación)

ID de punto de comprobación de Department of Defense STIG	Categoría de la regla de STIG	Descripción	Ubicación del script donde se define la acción y los resultados de la acción que permite la conformidad
GEN000790	2	El sistema debe impedir el uso de palabras de diccionario para las contraseñas.	**Ubicación** `/etc/security/pscexpert/dodv2/chuserstanzadod` **Acción de conformidad** Asegura que la contraseña predeterminada que se está estableciendo no sea débil.
GEN000800	2	Esta regla asegura que no se reutilicen las últimas cinco contraseñas.	**Ubicación** `/etc/security/pscexpert/dodv2/chusrattrdod` **Acción de conformidad** Asegura que la nueva contraseña no sea igual que cualquiera de las últimas 5 contraseñas.
GEN000880 (relacionado con GEN000300, GEN000320, GEN000380)	2	Todas las cuentas del sistema deben tener nombres de usuario o cuenta exclusivos y contraseñas de usuario o cuenta exclusivas.	**Ubicación** `/etc/security/pscexpert/dodv2/grpusrpass_chk` **Acción de conformidad** Asegura que todas las cuentas cumplan los requisitos especificados.
GEN000900	3	El directorio de inicio del usuario root no debe ser el directorio raíz (/).	**Ubicación** `/etc/security/pscexpert/dodv2/rootpasswd_home` **Acción de conformidad** Asegura que el sistema cumpla el requisito especificado. **Nota:** Este valor no cambia automáticamente cuando la política se restablece en la política predeterminada de AIX utilizando el archivo `DoDv2_to_AIXDefault.xml`. Debe cambiar manualmente este valor.
GEN000940	2	La vía de acceso de búsqueda ejecutable de la cuenta root debe ser el valor predeterminado de proveedor y debe contener sólo vías de acceso absolutas.	**Ubicación** `/etc/security/pscexpert/dodv2/fixpathvars` **Acción de conformidad** Asegura que el sistema cumpla los requisitos especificados. **Nota:** Este valor no cambia automáticamente cuando la política se restablece en la política predeterminada de AIX utilizando el archivo `DoDv2_to_AIXDefault.xml`. Debe cambiar manualmente este valor.
GEN000945	2	La vía de acceso de búsqueda de bibliotecas de la cuenta root debe ser el valor predeterminado de sistema y debe contener sólo vías de acceso absolutas.	**Ubicación** `/etc/security/pscexpert/dodv2/fixpathvars` **Acción de conformidad** Asegura que el sistema cumpla los requisitos especificados. **Nota:** Este valor no cambia automáticamente cuando la política se restablece en la política predeterminada de AIX utilizando el archivo `DoDv2_to_AIXDefault.xml`. Debe cambiar manualmente este valor.

Tabla 2. Requisitos generales de DoD (continuación)

ID de punto de comprobación de Department of Defense STIG	Categoría de la regla de STIG	Descripción	Ubicación del script donde se define la acción y los resultados de la acción que permite la conformidad
GEN000950	2	La lista de bibliotecas precargadas de la cuenta root debe estar vacía.	**Ubicación** `/etc/security/pscexpert/dodv2/fixpathvars` **Acción de conformidad** Asegura que el sistema cumpla los requisitos especificados. **Nota:** Este valor no cambia automáticamente cuando la política se restablece en la política predeterminada de AIX utilizando el archivo `DoDv2_to_AIXDefault.xml`. Debe cambiar manualmente este valor.
GEN000960 (relacionado con GEN003000, GEN003020, GEN003160, GEN003360, GEN003380)	2	La cuenta root no debe tener directorios grabables a nivel mundial en la vía de acceso de búsqueda ejecutable.	**Ubicación** `/etc/security/pscexpert/dodv2/rmwwpaths` **Acción de conformidad** Asegura que el sistema cumpla los requisitos especificados. **Nota:** Este valor no cambia automáticamente cuando la política se restablece en la política predeterminada de AIX utilizando el archivo `DoDv2_to_AIXDefault.xml`. Debe cambiar manualmente este valor.
GEN000980	2	El sistema debe impedir que la cuenta root inicie la sesión directamente, excepto desde la consola del sistema.	**Ubicación** `/etc/security/pscexpert/dodv2/chuserstanzadod` **Acción de conformidad** Asegura que el sistema cumpla los requisitos especificados.
GEN001000	2	Las consolas remotas deben inhabilitarse o protegerse del acceso no autorizado.	**Ubicación** `/etc/security/pscexpert/dodv2/remoteconsole` **Acción de conformidad** Asegura que se inhabiliten las consolas especificadas.
GEN001020	2	La cuenta root no debe utilizarse para el inicio de sesión directo.	**Ubicación** `/etc/security/pscexpert/dodv2/sshDoDconfig` **Acción de conformidad** Impide que la cuenta root inicie la sesión directamente.
GEN001060	2	El sistema debe registrar los intentos satisfactorios y no satisfactorios de acceso a la cuenta root.	**Ubicación** `/etc/security/pscexpert/dodv2/loginout` **Acción de conformidad** Asegura que el sistema cumpla los requisitos especificados.
GEN001100	1	Las contraseñas raíz nunca deben pasarse a través de una red en formato de texto.	**Ubicación** `/etc/security/pscexpert/dodv2/chuserstanzadod` **Acción de conformidad** Asegura que el sistema cumpla los requisitos especificados.
GEN001120	2	El sistema no debe permitir el inicio de sesión como root utilizando el protocolo `SSH`.	**Ubicación** `/etc/security/pscexpert/dodv2/sshDoDconfig` **Acción de conformidad** Inhabilita el inicio de sesión como root para `SSH`.

Tabla 2. Requisitos generales de DoD (continuación)

ID de punto de comprobación de Department of Defense STIG	Categoría de la regla de STIG	Descripción	Ubicación del script donde se define la acción y los resultados de la acción que permite la conformidad
GEN001440	3	A todos los usuarios interactivos se les debe asignar un directorio de inicio en el archivo `/etc/passwd`.	**Ubicación** `/etc/security/pscexpert/dodv2/grpusrpass_chk` **Acción de conformidad** Asegura que todos los usuarios interactivos tengan el directorio especificado.
GEN001475	2	El archivo `/etc/group` no debe contener ningún hash de contraseña de grupo.	**Ubicación** `/etc/security/pscexpert/dodv2/passwdhash` **Acción de conformidad** Asegura de que no haya ningún hash de contraseña de hash de contraseña en el archivo especificado. **Nota:** Este valor no cambia automáticamente cuando la política se restablece en la política predeterminada de AIX utilizando el archivo `DoDv2_to_AIXDefault.xml`. Debe cambiar manualmente este valor.
GEN001600	2	Las vías de acceso de búsqueda ejecutables de los scripts de control de ejecución sólo deben contener vías de acceso absolutas.	**Ubicación** `/etc/security/pscexpert/dodv2/fixpathvars` **Acción de conformidad** Asegura que el sistema cumpla los requisitos especificados. **Nota:** Este valor no cambia automáticamente cuando la política se restablece en la política predeterminada de AIX utilizando el archivo `DoDv2_to_AIXDefault.xml`. Debe cambiar manualmente este valor.
GEN001605	2	Las vías de acceso de búsqueda de biblioteca de los scripts de control de ejecución sólo deben contener vías de acceso absolutas.	**Ubicación** `/etc/security/pscexpert/dodv2/fixpathvars` **Acción de conformidad** Asegura que el sistema cumpla los requisitos especificados. **Nota:** Este valor no cambia automáticamente cuando la política se restablece en la política predeterminada de AIX utilizando el archivo `DoDv2_to_AIXDefault.xml`. Debe cambiar manualmente este valor.
GEN001610	2	Las listas de bibliotecas precargadas de los scripts de control de ejecución sólo deben contener vías de acceso absolutas.	**Ubicación** `/etc/security/pscexpert/dodv2/fixpathvars` **Acción de conformidad** Asegura que el sistema cumpla los requisitos especificados. **Nota:** Este valor no cambia automáticamente cuando la política se restablece en la política predeterminada de AIX utilizando el archivo `DoDv2_to_AIXDefault.xml`. Debe cambiar manualmente este valor.

Tabla 2. Requisitos generales de DoD (continuación)

ID de punto de comprobación de Department of Defense STIG	Categoría de la regla de STIG	Descripción	Ubicación del script donde se define la acción y los resultados de la acción que permite la conformidad
GEN001840	2	Las vías de acceso de búsqueda de ejecutables de todos los archivos de inicialización globales sólo deben contener vías de acceso absolutas.	**Ubicación** `/etc/security/pscexpert/dodv2/fixpathvars` **Acción de conformidad** Asegura que el sistema cumpla los requisitos especificados. **Nota:** Este valor no cambia automáticamente cuando la política se restablece en la política predeterminada de AIX utilizando el archivo `DoDv2_to_AIXDefault.xml`. Debe cambiar manualmente este valor.
GEN001845	2	Las vías de acceso de búsqueda de biblioteca de todos los archivos de inicialización globales sólo deben contener vías de acceso absolutas.	**Ubicación** `/etc/security/pscexpert/dodv2/fixpathvars` **Acción de conformidad** Asegura que el sistema cumpla los requisitos especificados. **Nota:** Este valor no cambia automáticamente cuando la política se restablece en la política predeterminada de AIX utilizando el archivo `DoDv2_to_AIXDefault.xml`. Debe cambiar manualmente este valor.
GEN001850	2	Las listas de bibliotecas precargadas de los archivos de inicialización globales deben contener sólo vías de acceso absolutas.	**Ubicación** `/etc/security/pscexpert/dodv2/fixpathvars` **Acción de conformidad** Asegura que el sistema cumpla los requisitos especificados. **Nota:** Este valor no cambia automáticamente cuando la política se restablece en la política predeterminada de AIX utilizando el archivo `DoDv2_to_AIXDefault.xml`. Debe cambiar manualmente este valor.
GEN001900	2	Las vías de acceso de búsqueda de ejecutables de todos los archivos de inicialización locales sólo deben contener vías de acceso absolutas.	**Ubicación** `/etc/security/pscexpert/dodv2/fixpathvars` **Acción de conformidad** Asegura que el sistema cumpla los requisitos especificados. **Nota:** Este valor no cambia automáticamente cuando la política se restablece en la política predeterminada de AIX utilizando el archivo `DoDv2_to_AIXDefault.xml`. Debe cambiar manualmente este valor.
GEN001901	2	Las vías de acceso de búsqueda de biblioteca de todos los archivos de inicialización locales sólo deben contener vías de acceso absolutas.	**Ubicación** `/etc/security/pscexpert/dodv2/fixpathvars` **Acción de conformidad** Asegura que el sistema cumpla los requisitos especificados. **Nota:** Este valor no cambia automáticamente cuando la política se restablece en la política predeterminada de AIX utilizando el archivo `DoDv2_to_AIXDefault.xml`. Debe cambiar manualmente este valor.

Tabla 2. Requisitos generales de DoD (continuación)

ID de punto de comprobación de Department of Defense STIG	Categoría de la regla de STIG	Descripción	Ubicación del script donde se define la acción y los resultados de la acción que permite la conformidad
GEN001902	2	Las listas de bibliotecas precargadas de todos los archivos de inicialización locales sólo deben contener vías de acceso absolutas.	**Ubicación** `/etc/security/pscexpert/dodv2/fixpathvars` **Acción de conformidad** Asegura que el sistema cumpla los requisitos especificados. **Nota:** Este valor no cambia automáticamente cuando la política se restablece en la política predeterminada de AIX utilizando el archivo `DoDv2_to_AIXDefault.xml`. Debe cambiar manualmente este valor.
GEN001940	2	Los archivos de inicialización de usuario no deben ejecutar programas grabables a nivel mundial.	**Ubicación** `/etc/security/pscexpert/dodv2/rmwwpaths` **Acción de conformidad** Asegura que el sistema cumpla los requisitos especificados.
GEN001980	2	Los archivos `.rhosts`, `.shosts`, `hosts.equiv`, `shosts.equiv`, `/etc/passwd`, `/etc/shadow` o `/etc/group` no deben contener un signo más (+) sin definir las entradas para grupos de red NIS+.	**Ubicación** `/etc/security/pscexpert/dodv2/dodv2netrules` **Acción de conformidad** Asegura que los archivos especificados cumplan los requisitos especificados.
GEN002000	2	No debe haber ningún archivo `.netrc` en el sistema.	**Ubicación** `/etc/security/pscexpert/dodv2/dodv2netrules` **Acción de conformidad** Asegura que no haya ninguno de los archivos especificados en el sistema. **Nota:** Este valor no cambia automáticamente cuando la política se restablece en la política predeterminada de AIX utilizando el archivo `DoDv2_to_AIXDefault.xml`. Debe cambiar manualmente este valor.
GEN002020	2	Todos los archivos `.rhosts`, `.shosts` o `hosts.equiv` sólo deben contener pares de host de confianza y usuario.	**Ubicación** `/etc/security/pscexpert/dodv2/dodv2netrules` **Acción de conformidad** Asegura que los archivos especificados cumplan este requisito.
GEN002040	1	Esta regla inhabilita los archivos `.rhosts`, `.shosts` y `hosts.equiv` o los archivos `shosts.equiv`.	**Ubicación** `/etc/security/pscexpert/dodv2/mvhostsfilesdod` **Acción de conformidad** Inhabilita los archivos especificados.

Tabla 2. Requisitos generales de DoD (continuación)

ID de punto de comprobación de Department of Defense STIG	Categoría de la regla de STIG	Descripción	Ubicación del script donde se define la acción y los resultados de la acción que permite la conformidad
GEN002120	1,2	Esta regla comprueba y configura shells de usuario.	**Ubicación** `/etc/security/pscexpert/dodv2/usershells` **Acción de conformidad** Crea los shells necesarios. **Nota:** Este valor no cambia automáticamente cuando la política se restablece en la política predeterminada de AIX utilizando el archivo `DoDv2_to_AIXDefault.xml`. Debe cambiar manualmente este valor.
GEN002140	1,2	Todos los shells referenciados en la lista `/etc/passwd` se deben listar en el archivo `/etc/shells`, excepto los shells que se especifican para impedir inicios de sesión.	**Ubicación** `/etc/security/pscexpert/dodv2/usershells` **Acción de conformidad** Asegura que los shells se listen en los archivos correctos. **Nota:** Este valor no cambia automáticamente cuando la política se restablece en la política predeterminada de AIX utilizando el archivo `DoDv2_to_AIXDefault.xml`. Debe cambiar manualmente este valor.
GEN002280	2	Los archivos y directorios de dispositivo sólo deben ser grabables por usuarios con una cuenta de sistema o como el sistema esté configurado por el proveedor.	**Ubicación** `/etc/security/pscexpert/dodv2/wwdevfiles` **Acción de conformidad** Visualiza archivos de dispositivos grabables a nivel mundial, directorios y otros archivos del sistema que están en directorios no públicos.
GEN002300	2	Los archivos de dispositivo que se utilizan para la copia de seguridad deben ser legibles y/o grabables sólo por el usuario root o el usuario de seguridad.	**Ubicación** `/etc/security/pscexpert/dodv2/wwdevfiles` **Acción de conformidad** Visualiza archivos de dispositivos grabables a nivel mundial, directorios y otros archivos del sistema que están en directorios no públicos.
GEN002400	2	El sistema debe comprobarse semanalmente para ver si hay archivos `setuid` no autorizados y modificación no autorizada en archivos `setuid` autorizados.	**Ubicación** `/etc/security/pscexpert/dodv2/trust` **Acción de conformidad** Comprueba semanalmente para identificar cambios en los archivos especificados. **Nota:** Compare los dos registros semanales más nuevos que se crean en el directorio `/var/security/pscexpert` para verificar que no había ninguna actividad no autorizada.

Tabla 2. Requisitos generales de DoD (continuación)

ID de punto de comprobación de Department of Defense STIG	Categoría de la regla de STIG	Descripción	Ubicación del script donde se define la acción y los resultados de la acción que permite la conformidad
GEN002420	2	Los soportes de almacenamiento extraíbles, los sistemas de archivo remotos y cualquier sistema de archivos que no contenga archivos `setuid` aprobados deben montarse utilizando la opción *nosuid*.	**Ubicación** `/etc/security/pscexpert/dodv2/fsmntoptions` **Acción de conformidad** Asegura que los sistemas de archivos montados de forma remota tengan las opciones especificadas. **Nota:** Este valor no cambia automáticamente cuando la política se restablece en la política predeterminada de AIX utilizando el archivo `DoDv2_to_AIXDefault.xml`. Debe cambiar manualmente este valor.
GEN002430	2	Los soportes de almacenamiento extraíbles, los sistemas de archivo remotos y cualquier sistema de archivos que no contenga archivos de dispositivo aprobados deben montarse utilizando la opción *nodev*.	**Ubicación** `/etc/security/pscexpert/dodv2/fsmntoptions` **Acción de conformidad** Asegura que los sistemas de archivos montados de forma remota tengan las opciones especificadas. **Nota:** Este valor no cambia automáticamente cuando la política se restablece en la política predeterminada de AIX utilizando el archivo `DoDv2_to_AIXDefault.xml`. Debe cambiar manualmente este valor.

GEN002480	2	Los directorios públicos deben ser los únicos directorios grabables a nivel mundial y los archivos grabables a nivel mundial deben estar sólo en directorios públicos.	**Ubicación**
			`/etc/security/pscexpert/dodv2/wwdevfiles`
			`/etc/security/pscexpert/dodv2/fpmdodfiles`
			Acción de conformidad
			Informa cuando los archivos grabables a nivel mundial no están en directorios públicos.

GEN002640	2	Las cuentas del sistema predeterminadas deben inhabilitarse o eliminarse.	**Ubicación**
			`/etc/security/pscexpert/dodv2/lockacc_rlogin`
			`/etc/security/pscexpert/dodv2/loginout`
			Acción de conformidad
			Inhabilita las cuentas de sistema predeterminadas.

GEN002660	2	Se debe habilitar la auditoría.	**Ubicación** `/etc/security/pscexpert/dodv2/dodaudit` **Acción de conformidad** Habilita el mandato `dodaudit`, que habilita la auditoría.
GEN002720	2	El sistema de auditoría debe configurarse para auditar los intentos fallidos de acceso a archivos y programas.	**Ubicación** `/etc/security/pscexpert/dodv2/dodaudit` **Acción de conformidad** Habilita automáticamente la auditoría especificada.
GEN002740	2	El sistema de auditoría debe configurarse para auditar supresiones de archivo.	**Ubicación** `/etc/security/pscexpert/dodv2/dodaudit` **Acción de conformidad** Habilita automáticamente la auditoría especificada.

Tabla 2. Requisitos generales de DoD (continuación)

ID de punto de comprobación de Department of Defense STIG	Categoría de la regla de STIG	Descripción	Ubicación del script donde se define la acción y los resultados de la acción que permite la conformidad
GEN002750	3	El sistema de auditoría debe configurarse para auditar la creación de cuentas.	**Ubicación** `/etc/security/pscexpert/dodv2/dodaudit` **Acción de conformidad** Habilita automáticamente la auditoría especificada.
GEN002751	3	El sistema de auditoría debe configurarse para auditar la modificación de cuentas.	**Ubicación** `/etc/security/pscexpert/dodv2/dodaudit` **Acción de conformidad** Habilita automáticamente la auditoría especificada.
GEN002752	3	El sistema de auditoría debe configurarse para auditar cuentas que están inhabilitadas.	**Ubicación** `/etc/security/pscexpert/dodv2/dodaudit` **Acción de conformidad** Habilita automáticamente la auditoría especificada.
GEN002753	3	El sistema de auditoría debe configurarse para auditar la terminación de cuentas.	**Ubicación** `/etc/security/pscexpert/dodv2/dodaudit` **Acción de conformidad** Habilita automáticamente la auditoría especificada.
GEN002760	2	El sistema de auditoría debe configurarse para auditar todas las acciones administrativas, con privilegios y de seguridad.	**Ubicación** `/etc/security/pscexpert/dodv2/dodaudit` **Acción de conformidad** Habilita automáticamente la auditoría especificada.
GEN002800	2	El sistema de auditoría debe configurarse para auditar el inicio de sesión, el cierre de sesión y la iniciación de sesión.	**Ubicación** `/etc/security/pscexpert/dodv2/dodaudit` **Acción de conformidad** Habilita automáticamente la auditoría especificada.
GEN002820	2	El sistema de auditoría debe configurarse para auditar todas las modificaciones de permisos de control de acceso discrecional.	**Ubicación** `/etc/security/pscexpert/dodv2/dodaudit` **Acción de conformidad** Habilita automáticamente la auditoría especificada.
GEN002825	2	El sistema de auditoría debe configurarse para auditar la carga y descarga de módulos de kernel dinámicos.	**Ubicación** `/etc/security/pscexpert/dodv2/dodaudit` **Acción de conformidad** Habilita automáticamente la auditoría especificada.
GEN002860	2	Los registros de auditoría deben rotar a diario.	**Ubicación** `/etc/security/pscexpert/dodv2/rotateauditdod` **Acción de conformidad** Asegura que se roten los registros de auditoría.

Tabla 2. Requisitos generales de DoD (continuación)

ID de punto de comprobación de Department of Defense STIG	Categoría de la regla de STIG	Descripción	Ubicación del script donde se define la acción y los resultados de la acción que permite la conformidad
GEN002960	2	El acceso al programa de utilidad `cron` se debe controlar utilizando el archivo `cron.allow` y/o el archivo `cron.deny`.	**Ubicación** `/etc/security/pscexpert/dodv2/limitsysacc` **Acción de conformidad** Asegura que estén habilitados los límites compatibles.
GEN003000 (relacionado con GEN000960, GEN003020, GEN003160, GEN003360, GEN003380)	2	`Cron` no debe ejecutar programas grabables a nivel de grupo o programas grabables a nivel mundial.	**Ubicación** `/etc/security/pscexpert/dodv2/rmwwpaths` **Acción de conformidad** Asegura que estén habilitados los límites compatibles. **Nota:** Este valor no cambia automáticamente cuando la política se restablece en la política predeterminada de AIX utilizando el archivo `DoDv2_to_AIXDefault.xml`. Debe cambiar manualmente este valor.
GEN003020 (relacionado con GEN000960, GEN003000, GEN003160, GEN003360, GEN003380)	2	`Cron` no debe ejecutar programas en directorios grabables a nivel mundial o subordinados a ellos.	**Ubicación** `/etc/security/pscexpert/dodv2/rmwwpaths` **Acción de conformidad** Elimina el permiso de grabación a nivel mundial de los directorios de programa `cron`. **Nota:** Este valor no cambia automáticamente cuando la política se restablece en la política predeterminada de AIX utilizando el archivo `DoDv2_to_AIXDefault.xml`. Debe cambiar manualmente este valor.
GEN003060	2	Las cuentas de sistema predeterminadas (excepto para root) no deben listarse en el archivo `cron.allow` o deben incluirse en el archivo `cron.deny` si el archivo `cron.allow` no existe.	**Ubicación** `cron.allow` o `cron.deny` **Acción de conformidad** Asegura que el sistema cumpla los requisitos especificados.
GEN003160 (relacionado con GEN000960, GEN003000, GEN003020, GEN003360, GEN003380)	2	El registro de `Cron` debe estar en ejecución.	**Ubicación** `/etc/security/pscexpert/dodv2/rmwwpaths` **Acción de conformidad** Asegura que el sistema cumpla los requisitos especificados.
GEN003280	2	El acceso al programa de utilidad `at` debe controlarse utilizando los archivos `at.allow` y `at.deny`.	**Ubicación** `/etc/security/pscexpert/dodv2/chcronfilesdod` **Acción de conformidad** Asegura que el sistema cumpla los requisitos especificados.
GEN003300	2	El archivo `at.deny` no debe estar vacío, si existe.	**Ubicación** `/etc/security/pscexpert/dodv2/chcronfilesdod` **Acción de conformidad** Asegura que el sistema cumpla los requisitos especificados.

Tabla 2. Requisitos generales de DoD (continuación)

ID de punto de comprobación de Department of Defense STIG	Categoría de la regla de STIG	Descripción	Ubicación del script donde se define la acción y los resultados de la acción que permite la conformidad
GEN003320	2	Las cuentas de sistema predeterminadas que no son root no deben listarse en el archivo `at.allow` o deben incluirse en el archivo `at.deny` si el archivo `at.allow` no existe.	**Ubicación** `/etc/security/pscexpert/dodv2/chcronfilesdod` **Acción de conformidad** Asegura que el sistema cumpla los requisitos especificados.
GEN003360 (relacionado con GEN000960, GEN003000, GEN003020, GEN003160, GEN003380)	2	El daemon `at` no debe ejecutar programas grabables a nivel de grupo o grabable a nivel mundial.	**Ubicación** `/etc/security/pscexpert/dodv2/rmwwpaths` **Acción de conformidad** Asegura que el sistema cumpla los requisitos especificados. **Nota:** Este valor no cambia automáticamente cuando la política se restablece en la política predeterminada de AIX utilizando el archivo `DoDv2_to_AIXDefault.xml`. Debe cambiar manualmente este valor.
GEN003380 (relacionado con GEN000960, GEN003000, GEN003020, GEN003160, GEN003360)	2	El daemon `at` no debe ejecutar programas en directorios grabables a nivel mundial o subordinados a ellos.	**Ubicación** `/etc/security/pscexpert/dodv2/rmwwpaths` **Acción de conformidad** Asegura que el sistema cumpla los requisitos especificados. **Nota:** Este valor no cambia automáticamente cuando la política se restablece en la política predeterminada de AIX utilizando el archivo `DoDv2_to_AIXDefault.xml`. Debe cambiar manualmente este valor.
GEN003510	2	Los volcados de núcleo de kernel deben estar inhabilitados a menos que sean necesarios.	**Ubicación** `/etc/security/pscexpert/dodv2/coredumpdev` **Acción de conformidad** Inhabilita los volcados de núcleo de kernel.
GEN003540	2	El sistema debe utilizar pilas de programa no ejecutables.	**Ubicación** `/etc/security/pscexpert/dodv2/sedconfigdod` **Acción de conformidad** Aplica el uso de pilas de programa no ejecutables.
GEN003600	2	El sistema no debe reenviar paquetes IPv4 direccionados de origen.	**Ubicación** `/etc/security/pscexpert/dodv2/ntwkoptsdod` **Acción de conformidad** Establece el valor de la opción de red `ipsrcforward` en *0*.
GEN003601	2	Los tamaños de colas de pendientes TCP debe establecerse adecuadamente.	**Ubicación** `/etc/security/pscexpert/dodv2/ntwkoptsdod` **Acción de conformidad** Establece el valor de la opción de red `clean_partial_conns` en *1*.

Tabla 2. Requisitos generales de DoD (continuación)

ID de punto de comprobación de Department of Defense STIG	Categoría de la regla de STIG	Descripción	Ubicación del script donde se define la acción y los resultados de la acción que permite la conformidad
GEN003603	2	El sistema no debe responder a los ecos de Internet Control Message Protocol versión 4 (ICMPv4) que se envían a una dirección de difusión.	**Ubicación** `/etc/security/pscexpert/dodv2/ntwkoptsdod` **Acción de conformidad** Establece el valor de la opción de red `bcastping` en *0*.
GEN003604	2	El sistema no debe responder a las solicitudes de indicación de fecha y hora de ICMP que se envían a una dirección de difusión.	**Ubicación** `/etc/security/pscexpert/dodv2/ntwkoptsdod` **Acción de conformidad** Establece el valor de la opción de red `bcastping` en *0*.
GEN003605	2	El sistema no debe aplicar el direccionamiento de origen inverso a las respuestas de TCP.	**Ubicación** `/etc/security/pscexpert/dodv2/ntwkoptsdod` **Acción de conformidad** Establece el valor de la opción de red `nonlocsrcroute` en *0*.
GEN003606	2	El sistema debe impedir que las aplicaciones locales generen paquetes direccionados de origen.	**Ubicación** `/etc/security/pscexpert/dodv2/ntwkoptsdod` **Acción de conformidad** Establece el valor de la opción de red `ipsrcroutesend` en *0*.
GEN003607	2	El sistema no debe aceptar paquetes IPv4 direccionados de origen.	**Ubicación** `/etc/security/pscexpert/dodv2/ntwkoptsdod` **Acción de conformidad** Inhabilita la capacidad de aceptar paquetes IPv4 de rutas de origen.
GEN003609	2	El sistema debe ignorar mensajes de redireccionamiento de ICMP IPv4.	**Ubicación** `/etc/security/pscexpert/dodv2/ntwkoptsdod` **Acción de conformidad** Establece el valor de la opción de red `ipignoreredirects` en *1*.
GEN003610	2	El sistema no debe enviar mensajes de redireccionamiento de ICMP IPv4.	**Ubicación** `/etc/security/pscexpert/dodv2/ntwkoptsdod` **Acción de conformidad** Establece el valor de la opción de red `ipsendredirects` en *0*.
GEN003612	2	El sistema debe configurarse para utilizar syncookies TCP cuando se produzca un desbordamiento de TCP SYN.	**Ubicación** `/etc/security/pscexpert/dodv2/ntwkoptsdod` **Acción de conformidad** Establece el valor de la opción de red `clean_partial_ _conns` en *1*.

Tabla 2. Requisitos generales de DoD (continuación)

ID de punto de comprobación de Department of Defense STIG	Categoría de la regla de STIG	Descripción	Ubicación del script donde se define la acción y los resultados de la acción que permite la conformidad
GEN003640	2	El sistema de archivos raíz debe utilizar el registro por diario u otro método para asegurar la coherencia del sistema de archivos.	**Ubicación** `/etc/security/pscexpert/dodv2/chkjournal` **Acción de conformidad** Habilita el registro por diario en el sistema de archivos raíz.
GEN003660	2	El sistema debe registrar datos informativos de autenticación.	**Ubicación** `/etc/security/pscexpert/dodv2/chsyslogdod` **Acción de conformidad** Habilita el registro de los datos `auth` e `info`.
GEN003700	2	`inetd` y `xinetd` deben inhabilitarse o eliminarse si no los utiliza ningún servicio de red.	**Ubicación** `/etc/security/pscexpert/dodv2/dodv2services` **Acción de conformidad** Asegura que el sistema cumpla los requisitos especificados.
GEN003810	2	Estos servicios `portmap` o `rpcbind` no deben estar en ejecución a menos que sean necesarios.	**Ubicación** `/etc/security/pscexpert/dodv2/dodv2services` **Acción de conformidad** Asegura que el sistema cumpla los requisitos especificados.
GEN003815	2	Los servicios `portmap` o `rpcbind` no deben instalarse a menos que se estén utilizando.	**Ubicación** `/etc/security/pscexpert/dodv2/dodv2services` **Acción de conformidad** Asegura que el sistema cumpla los requisitos especificados.
GEN003820-3860	1,2,3	Los daemons `rsh`, `rexexec` y `telnet` y el servicio `rlogind` no deben estar en ejecución.	**Ubicación** `/etc/security/pscexpert/dodv2/inetdservices` **Acción de conformidad** Inhabilita los daemons y servicios necesarios comentando las entradas en el archivo `/etc/inetd.conf`.
GEN003865	2	Las herramientas de análisis de red no deben estar instalados.	**Ubicación** `/etc/security/pscexpert/dodv2/dodv2services` **Acción de conformidad** Asegura que el sistema cumpla los requisitos especificados.
GEN003900	2	El archivo `hosts.lpd` (o equivalente) no debe contener un signo de suma (+).	**Ubicación** `/etc/security/pscexpert/dodv2/printers` **Acción de conformidad** Asegura que el sistema cumpla los requisitos especificados.

Tabla 2. Requisitos generales de DoD (continuación)

ID de punto de comprobación de Department of Defense STIG	Categoría de la regla de STIG	Descripción	Ubicación del script donde se define la acción y los resultados de la acción que permite la conformidad
GEN004220	1	Las cuentas administrativas no deben ejecutar un navegador web, excepto cuando sea necesario para la administración de servicio local.	**Ubicación** /etc/security/pscexpert/dodv2/dodv2cat1 **Acción de conformidad** Muestra los resultados de las pruebas de regla especificadas.
GEN004460	2	Esta regla registra los datos auth e info.	**Ubicación** /etc/security/pscexpert/dodv2/chsyslogdod **Acción de conformidad** Habilita el registro de los datos auth e info.
GEN004540	2	Esta regla inhabilita el mandato de ayuda sendmail.	**Ubicación** /etc/security/pscexpert/dodv2/sendmailhelp /etc/security/pscexpert/dodv2/dodv2cmntrows **Acción de conformidad** Inhabilita el mandato especificado.
GEN004580	2	El sistema no debe utilizar archivos .forward.	**Ubicación** /etc/security/pscexpert/dodv2/forward **Acción de conformidad** Inhabilita los archivos especificados. **Nota:** Este valor no cambia automáticamente cuando la política se restablece en la política predeterminada de AIX utilizando el archivo DoDv2_to_AIXDefault.xml. Debe cambiar manualmente este valor.
GEN004600	1	El servicio SMTP debe ser la versión más actual.	**Ubicación** /etc/security/pscexpert/dodv2/SMTP_ver **Acción de conformidad** Asegura que la última versión del servicio especificado esté en ejecución. **Nota:** Este valor no cambia automáticamente cuando la política se restablece en la política predeterminada de AIX utilizando el archivo DoDv2_to_AIXDefault.xml. Debe cambiar manualmente este valor.
GEN004620	2	El servidor sendmail debe tener la característica de depuración inhabilitada.	**Ubicación** /etc/security/pscexpert/dodv2/SMTP_ver **Acción de conformidad** Inhabilita la característica de depuración sendmail.
GEN004640	1	El servicio SMTP no debe tener un alias uudecode activo.	**Ubicación** /etc/security/pscexpert/dodv2/SMTPuucode **Acción de conformidad** Inhabilita el alias uudecode.
GEN004710	2	La transmisión de correo debe estar restringida.	**Ubicación** /etc/security/pscexpert/dodv2/sendmaildod **Acción de conformidad** Restringe la transmisión de correo.

Tabla 2. Requisitos generales de DoD (continuación)

ID de punto de comprobación de Department of Defense STIG	Categoría de la regla de STIG	Descripción	Ubicación del script donde se define la acción y los resultados de la acción que permite la conformidad
GEN004800	1,2,3	No se debe utilizar FTP no cifrado en el sistema.	**Ubicación** `/etc/security/pscexpert/dodv2/inetdservices` **Acción de conformidad** Inhabilita los daemons y servicios necesarios comentando las entradas en el archivo `/etc/inetd.conf`.
GEN004820	2	FTP anónimo no debe estar activo en el sistema a menos que esté autorizado.	**Ubicación** `/etc/security/pscexpert/dodv2/anonuser` **Acción de conformidad** Inhabilita el FTP anónimo en el sistema. **Nota:** Este valor no cambia automáticamente cuando la política se restablece en la política predeterminada de AIX utilizando el archivo `DoDv2_to_AIXDefault.xml`. Debe cambiar manualmente este valor.
GEN004840	2	Si el sistema es un servidor FTP anónimo, debe aislarse en la red de Zona desmilitarizada (DMZ).	**Ubicación** `/etc/security/pscexpert/dodv2/anonuser` **Acción de conformidad** Asegura que un FTP anónimo en el sistema esté en la red DMZ.
GEN004880	2	El archivo `ftpusers` debe existir.	**Ubicación** `/etc/security/pscexpert/dodv2/chdodftpusers` **Acción de conformidad** Asegura que el archivo especificado esté en el sistema.
GEN004900	2	El archivo `ftpusers` debe contener los nombres de cuenta a los que no se permite utilizar el protocolo FTP.	**Ubicación** `/etc/security/pscexpert/dodv2/chdodftpusers` **Acción de conformidad** Asegura que el archivo contiene los nombres de cuenta necesarios.
GEN005000	1	Las cuentas de FTP anónimo no deben tener un shell funcional.	**Ubicación** `/etc/security/pscexpert/dodv2/usershells` **Acción de conformidad** Elimina shells de las cuentas de FTP anónimo. **Nota:** Este valor no cambia automáticamente cuando la política se restablece en la política predeterminada de AIX utilizando el archivo `DoDv2_to_AIXDefault.xml`. Debe cambiar manualmente este valor.
GEN005080	1	El daemon `TFTP` debe funcionar en modalidad segura, que proporciona únicamente acceso a un directorio único en el sistema de archivos de host.	**Ubicación** `/etc/security/pscexpert/dodv2/tftpdod` **Acción de conformidad** Asegura que el daemon cumpla los requisitos especificados.

Tabla 2. Requisitos generales de DoD (continuación)

ID de punto de comprobación de Department of Defense STIG	Categoría de la regla de STIG	Descripción	Ubicación del script donde se define la acción y los resultados de la acción que permite la conformidad
GEN005120	2	El daemon TFTP se debe configurar según las especificaciones de proveedor, incluyendo una cuenta de usuario TFTP dedicada, un shell no de inicio de sesión, por ejemplo `/bin/false`, y un directorio de inicio que es propiedad del usuario TFTP.	**Ubicación** `/etc/security/pscexpert/dodv2/tftpdod` **Acción de conformidad** Asegura que el sistema cumpla los requisitos especificados.
GEN005140	1,2,3	Cualquier daemon TFTP activo debe estar autorizado y aprobado en el paquete de acreditación de sistema.	**Ubicación** `/etc/security/pscexpert/dodv2/inetdservices` **Acción de conformidad** Asegura que el daemon esté autorizado.
GEN005160	1,2	Cualquier host de sistema X Window debe grabar archivos `Xauthority`.	**Ubicación** `/etc/security/pscexpert/dodv2/dodv2disableX` **Acción de conformidad** Asegura que el host haya grabado los archivos especificados.
GEN005200	1,2	Las pantallas de sistema X Window no se pueden exportar públicamente.	**Ubicación** `/etc/security/pscexpert/dodv2/dodv2disableX` **Acción de conformidad** Inhabilita la diseminación de los programas especificados.
GEN005220	1,2	Se deben utilizar los archivos `.Xauthority` o `X*.hosts` (o equivalente) para restringir el acceso al servidor de sistema X Window.	**Ubicación** `/etc/security/pscexpert/dodv2/dodv2disableX` **Acción de conformidad** Asegura que los archivos especificados estén disponibles para restringir el acceso al servidor.
GEN005240	1,2	El programa de utilidad .Xauthority sólo debe permitir el acceso a los hosts autorizados.	**Ubicación** `/etc/security/pscexpert/dodv2/dodv2disableX` **Acción de conformidad** Asegura que el acceso esté limitado a hosts autorizados.
GEN005260	2	Esta regla inhabilita las conexiones de sistema X Window y el gestor de inicio de sesión XServer.	**Ubicación** `/etc/security/pscexpert/dodv2/dodv2cmntrows` **Acción de conformidad** Inhabilita las conexiones necesarias y el gestor de inicio de sesión.
GEN005280	1,2,3	El sistema no debe tener el servicio `UUCP` activo.	**Ubicación** `/etc/security/pscexpert/dodv2/inetdservices` **Acción de conformidad** Inhabilita los daemons y servicios necesarios comentando las entradas en el archivo `/etc/inetd.conf`.

Tabla 2. Requisitos generales de DoD (continuación)

ID de punto de comprobación de Department of Defense STIG	Categoría de la regla de STIG	Descripción	Ubicación del script donde se define la acción y los resultados de la acción que permite la conformidad
GEN005300	2	Las comunidades SNMP deben cambiarse respecto a los valores predeterminados.	**Ubicación** `/etc/security/pscexpert/dodv2/chsnmp` **Acción de conformidad** Asegura que el sistema cumpla los requisitos especificados.
GEN005305	2	El servicio SNMP sólo debe utilizar SNMPv3 o una versión posterior.	**Ubicación** `/etc/security/pscexpert/dodv2/chsnmp` **Acción de conformidad** Asegura que el sistema cumpla los requisitos especificados.
GEN005306	2	El servicio SNMP debe requerir el uso de un FIPS 140-2.	**Ubicación** `/etc/security/pscexpert/dodv2/chsnmp` **Acción de conformidad** Asegura que el sistema cumpla los requisitos especificados.
GEN005440	2	El sistema debe utilizar un servidor syslog remoto (host de registro).	**Ubicación** `/etc/security/pscexpert/dodv2/EnableTrustedLogging` **Acción de conformidad** Asegura que el sistema esté utilizando un servidor syslog remoto.
GEN005450	2	El sistema debe utilizar un servidor syslog remoto (host de registro).	**Ubicación** `/etc/security/pscexpert/dodv2/EnableTrustedLogging` **Acción de conformidad** Asegura que el sistema esté utilizando un servidor syslog remoto.
GEN005460	2	El sistema debe utilizar un servidor syslog remoto (host de registro).	**Ubicación** `/etc/security/pscexpert/dodv2/EnableTrustedLogging` **Acción de conformidad** Asegura que el sistema esté utilizando un servidor syslog remoto.
GEN005480	2	El sistema debe utilizar un servidor syslog remoto (host de registro).	**Ubicación** `/etc/security/pscexpert/dodv2/EnableTrustedLogging` **Acción de conformidad** Asegura que el sistema esté utilizando un servidor syslog remoto.
GEN005500	2	El daemon `SSH` debe estar configurado para utilizar sólo el protocolo Secure Shell versión 2 (SSHv2).	**Ubicación** `/etc/security/pscexpert/dodv2/sshDoDconfig` **Acción de conformidad** Asegura que el sistema cumpla los requisitos especificados.

Tabla 2. Requisitos generales de DoD (continuación)

ID de punto de comprobación de Department of Defense STIG	Categoría de la regla de STIG	Descripción	Ubicación del script donde se define la acción y los resultados de la acción que permite la conformidad
GEN005501	2	El cliente SSH debe estar configurado para utilizar sólo el protocolo SSHv2.	**Ubicación** /etc/security/pscexpert/dodv2/sshDoDconfig **Acción de conformidad** Asegura que el sistema cumpla los requisitos especificados.
GEN005504	2	El daemon SSH sólo debe escuchar en direcciones de red de gestión, a menos que esté autorizado para usos distintos de la gestión.	**Ubicación** /etc/security/pscexpert/dodv2/sshDoDconfig **Acción de conformidad** Asegura que el sistema cumpla los requisitos especificados.
GEN005505	2	El daemon SSH debe configurarse para utilizar sólo cifrados que cumplan con los estándares de Federal Information Processing Standards (FIPS) 140-2.	**Ubicación** /etc/security/pscexpert/dodv2/sshDoDconfig **Acción de conformidad** Asegura que el sistema cumpla los requisitos especificados.
GEN005506	2	El daemon SSH debe configurarse para utilizar sólo cifrados que se ajusten a los estándares de FIPS 140-2.	**Ubicación** /etc/security/pscexpert/dodv2/sshDoDconfig **Acción de conformidad** Asegura que el sistema cumpla los requisitos especificados.
GEN005507	2	El daemon SSH debe configurarse para utilizar sólo Códigos de autenticación de mensaje (MAC) con algoritmos hash criptográficos que se ajusten a los estándares FIPS 140-2.	**Ubicación** /etc/security/pscexpert/dodv2/sshDoDconfig **Acción de conformidad** Asegura que el sistema cumpla los requisitos especificados.
GEN005510	2	El cliente SSH debe configurarse para utilizar sólo los MAC con cifrados que cumplen con los estándares FIPS 140-2.	**Ubicación** /etc/security/pscexpert/dodv2/sshDoDconfig **Acción de conformidad** Asegura que el sistema cumpla los requisitos especificados.
GEN005511	2	El cliente SSH debe configurarse para utilizar sólo los MAC con cifrados que cumplen con los estándares FIPS 140-2.	**Ubicación** /etc/security/pscexpert/dodv2/sshDoDconfig **Acción de conformidad** Asegura que el sistema cumpla los requisitos especificados.
GEN005512	2	El daemon SSH debe configurarse para utilizar sólo los MAC con algoritmos hash criptográficos que se ajusten a los estándares FIPS 140-2.	**Ubicación** /etc/security/pscexpert/dodv2/sshDoDconfig **Acción de conformidad** Asegura que el sistema cumpla los requisitos especificados.

Tabla 2. Requisitos generales de DoD (continuación)

ID de punto de comprobación de Department of Defense STIG	Categoría de la regla de STIG	Descripción	Ubicación del script donde se define la acción y los resultados de la acción que permite la conformidad
GEN005521	2	El daemon SSH debe restringir el inicio de sesión a usuarios y/o grupos específicos.	**Ubicación** /etc/security/pscexpert/dodv2/sshDoDconfig **Acción de conformidad** Asegura que el sistema cumpla los requisitos especificados.
GEN005536	2	El daemon SSH debe realizar la comprobación en modalidad estricta de los archivos de configuración de directorio de inicio.	**Ubicación** /etc/security/pscexpert/dodv2/sshDoDconfig **Acción de conformidad** Asegura que el sistema cumpla los requisitos especificados.
GEN005537	2	El daemon SSH debe utilizar la separación de privilegios.	**Ubicación** /etc/security/pscexpert/dodv2/sshDoDconfig **Acción de conformidad** Asegura que el sistema cumpla los requisitos especificados.
GEN005538	2	El daemon SSH no debe permitir que rhosts se autentique utilizando el criptosistema Rivest-Shamir-Adleman (RSA).	**Ubicación** /etc/security/pscexpert/dodv2/sshDoDconfig **Acción de conformidad** Asegura que el sistema cumpla los requisitos especificados.
GEN005539	2	El daemon SSH no debe permitir la compresión o debe permitir la compresión sólo después de una autenticación satisfactoria.	**Ubicación** /etc/security/pscexpert/dodv2/sshDoDconfig **Acción de conformidad** Asegura que el sistema cumpla los requisitos especificados.
GEN005550	2	El daemon SSH debe configurarse con el banner de inicio de sesión DoD.	**Ubicación** /etc/security/pscexpert/dodv2/sshDoDconfig **Acción de conformidad** Asegura que el sistema cumpla los requisitos especificados.
GEN005560	2	Determinar si hay una pasarela predeterminada que esté configurada para IPv4.	**Ubicación** /etc/security/pscexpert/dodv2/chkgtway **Acción de conformidad** Asegura que el sistema cumpla los requisitos especificados. **Nota:** Este valor no cambia automáticamente cuando la política se restablece en la política predeterminada de AIX utilizando el archivo DoDv2_to_AIXDefault.xml. Debe cambiar manualmente este valor. **Nota:** Si el sistema está ejecutando el protocolo IPv6, asegúrese de que el valor *ipv6_enabled* en el archivo /etc/security/pscexpert/ipv6.conf se establece en el valor de yes. Si el sistema no está utilizando IPv6, asegúrese de que el valor *ipv6_enabled* se ha establecido en no.

Tabla 2. Requisitos generales de DoD (continuación)

ID de punto de comprobación de Department of Defense STIG	Categoría de la regla de STIG	Descripción	Ubicación del script donde se define la acción y los resultados de la acción que permite la conformidad
GEN005570	2	Determinar si hay una pasarela predeterminada que esté configurada para IPv6.	**Ubicación** `/etc/security/pscexpert/dodv2/chkgtway` **Acción de conformidad** Asegura que el sistema cumpla los requisitos especificados. **Nota:** Este valor no cambia automáticamente cuando la política se restablece en la política predeterminada de AIX utilizando el archivo `DoDv2_to_AIXDefault.xml`. Debe cambiar manualmente este valor. **Nota:** Si el sistema está ejecutando el protocolo IPv6, asegúrese de que el valor *ipv6_enabled* en el archivo `/etc/security/pscexpert/ipv6.conf` se establece en el valor de `yes`. Si el sistema no está utilizando IPv6, asegúrese de que el valor *ipv6_enabled* se ha establecido en `no`.
GEN005590	2	El sistema no debe estar ejecutando ningún daemon de protocolo de direccionamiento, a menos que el sistema sea un direccionador.	**Ubicación** `/etc/security/pscexpert/dodv2/dodv2cmntrows` **Acción de conformidad** Asegura que el sistema cumpla los requisitos especificados.
GEN005590	2	El sistema no debe estar ejecutando ningún daemon de protocolo de direccionamiento, a menos que el sistema sea un direccionador.	**Ubicación** `/etc/security/pscexpert/dodv2/dodv2cmntrows` **Acción de conformidad** Asegura que el sistema cumpla los requisitos especificados.
GEN005600	2	El reenvío de IP para IPv4 no debe habilitarse a menos que el sistema sea un direccionador.	**Ubicación** `/etc/security/pscexpert/dodv2/ntwkoptsdod` **Acción de conformidad** Establece el valor de la opción de red `ipforwarding` en *0*.
GEN005610	2	El sistema no debe tener el reenvío de IP para IPv6 habilitado a menos que el sistema sea un direccionador IPv6.	**Ubicación** `/etc/security/pscexpert/dodv2/ntwkoptsdod` **Acción de conformidad** Establece el valor de la opción de red `ip6forwarding` en *1*.
GEN005820	2	El UID y GID anónimos de NFS deben configurarse en valores sin permisos.	**Ubicación** `/etc/security/pscexpert/dodv2/nfsoptions` **Acción de conformidad** Asegura que los ID especificados no tengan permisos.
GEN005840	2	El servidor NFS debe estar configurado para restringir el acceso de sistema de archivos a los hosts locales.	**Ubicación** `/etc/security/pscexpert/dodv2/nfsoptions` **Acción de conformidad** Configura el servidor NFS para restringir el acceso a hosts locales.

Tabla 2. Requisitos generales de DoD (continuación)

ID de punto de comprobación de Department of Defense STIG	Categoría de la regla de STIG	Descripción	Ubicación del script donde se define la acción y los resultados de la acción que permite la conformidad
GEN005880	2	El servidor NFS no debe permitir el acceso de root remoto.	**Ubicación** `/etc/security/pscexpert/dodv2/nfsoptions` **Acción de conformidad** Inhabilita el acceso de root remoto en el servidor NFS.
GEN005900	2	La opción *nosuid* debe estar habilitada en todos los montajes de cliente NFS.	**Ubicación** `/etc/security/pscexpert/dodv2/nosuid` **Acción de conformidad** Habilita la opción *nosuid* en todos los montajes de cliente NFS.
GEN006060	2	El sistema no debe ejecutar `Samba` a menos que sea necesario.	**Ubicación** `/etc/security/pscexpert/dodv2/dodv2services` **Acción de conformidad** Asegura que el sistema cumpla los requisitos especificados.
GEN006380	1	El sistema no debe utilizar UDP para NIS o NIS+.	**Ubicación** `/etc/security/pscexpert/dodv2/dodv2cat1` **Acción de conformidad** Muestra los resultados de las pruebas de regla especificadas.
GEN006400	2	No se debe utilizar el protocolo Network Information System (NIS).	**Ubicación** `/etc/security/pscexpert/dodv2/nisplus` **Acción de conformidad** Inhabilita el protocolo especificado. **Nota:** Este valor no cambia automáticamente cuando la política se restablece en la política predeterminada de AIX utilizando el archivo `DoDv2_to_AIXDefault.xml`. Debe cambiar manualmente este valor.
GEN006420	2	Las correlaciones de NIS deben protegerse utilizando nombres de dominio difíciles de adivinar.	**Ubicación** `/etc/security/pscexpert/dodv2/nisplus` **Acción de conformidad** Asegura que los nombres de dominio no sean fáciles de determinar.
GEN006460	2	Cualquier servidor NIS+ debe funcionar en el nivel de seguridad 2.	**Ubicación** `/etc/security/pscexpert/dodv2/nisplus` **Acción de conformidad** Asegura que el servidor esté en el nivel de seguridad mínimo especificado. **Nota:** Este valor no cambia automáticamente cuando la política se restablece en la política predeterminada de AIX utilizando el archivo `DoDv2_to_AIXDefault.xml`. Debe cambiar manualmente este valor.

Tabla 2. Requisitos generales de DoD (continuación)

ID de punto de comprobación de Department of Defense STIG	Categoría de la regla de STIG	Descripción	Ubicación del script donde se define la acción y los resultados de la acción que permite la conformidad
GEN006480	2	El sistema debe comprobarse semanalmente para ver si hay archivos `setuid` no autorizados y modificación no autorizada en archivos `setuid` autorizados.	**Ubicación** `/etc/security/pscexpert/dodv2/trust` **Acción de conformidad** Comprueba semanalmente para identificar cambios en los archivos especificados.
GEN006560	2	El sistema debe comprobarse semanalmente para ver si hay archivos `setuid` no autorizados y modificación no autorizada en archivos `setuid` autorizados.	**Ubicación** `/etc/security/pscexpert/dodv2/trust` **Acción de conformidad** Comprueba semanalmente para identificar cambios en los archivos especificados.
GEN006580	2	El sistema debe utilizar un programa de control de accesos.	**Ubicación** `/etc/security/pscexpert/dodv2/checktcpd` **Acción de conformidad** Asegura que el sistema cumpla los requisitos especificados.
GEN006600	2	El programa de control de accesos del sistema debe registrar cada intento de acceso del sistema.	**Ubicación** `/etc/security/pscexpert/dodv2/chsyslogdod` **Acción de conformidad** Asegura que se registren los intentos de acceso.
GEN006620	2	El programa de control de accesos del sistema debe configurarse para otorgar o denegar el acceso del sistema a hosts específicos.	**Ubicación** `/etc/security/pscexpert/dodv2/chetchostsdod` **Acción de conformidad** Configura los archivos `hosts.deny` y `hosts.allow` en los valores necesarios.
GEN007020	2	El Protocolo de transmisión de control de corriente (SCTP) debe estar inhabilitado.	**Ubicación** `/etc/security/pscexpert/dodv2/dodv2netrules` **Acción de conformidad** Inhabilita el protocolo especificado.
GEN007700	2	El manejador de protocolo IPv6 no debe estar vinculado a la pila de red a menos que sea necesario.	**Ubicación** `/etc/security/pscexpert/dodv2/rminet6` **Acción de conformidad** Inhabilita el manejador de protocolo IPv6 de la pila de red, a menos que se especifique el manejador en el archivo `/etc/ipv6.conf`. **Nota:** Si el sistema está ejecutando el protocolo IPv6, asegúrese de que el valor *ipv6_enabled* en el archivo `/etc/security/pscexpert/ipv6.conf` se establece en el valor de `yes`. Si el sistema no está utilizando IPv6, asegúrese de que el valor *ipv6_enabled* se ha establecido en `no`.

Tabla 2. Requisitos generales de DoD (continuación)

ID de punto de comprobación de Department of Defense STIG	Categoría de la regla de STIG	Descripción	Ubicación del script donde se define la acción y los resultados de la acción que permite la conformidad
GEN007780	2	El sistema no debe tener túneles `6to4` habilitados.	**Ubicación** `/etc/security/pscexpert/dodv2/rmiface` **Acción de conformidad** Inhabilita los túneles especificados. **Nota:** Este valor no cambia automáticamente cuando la política se restablece en la política predeterminada de AIX utilizando el archivo `DoDv2_to_AIXDefault.xml`. Debe cambiar manualmente este valor.
GEN007820	2	El sistema no debe tener túneles IP configurados.	**Ubicación** `/etc/security/pscexpert/dodv2/rmtunnel` **Acción de conformidad** Inhabilita túneles IP. **Nota:** Este valor no cambia automáticamente cuando la política se restablece en la política predeterminada de AIX utilizando el archivo `DoDv2_to_AIXDefault.xml`. Debe cambiar manualmente este valor.
GEN007840	2	El cliente `DHCP` debe inhabilitarse si no se utiliza.	**Ubicación** `/etc/security/pscexpert/dodv2/dodv2services` **Acción de conformidad** Asegura que el sistema cumpla los requisitos especificados.
GEN007850	2	El cliente `DHCP` no debe enviar actualizaciones DNS dinámicas.	**Ubicación** `/etc/security/pscexpert/dodv2/dodv2services` **Acción de conformidad** Asegura que el sistema cumpla los requisitos especificados.
GEN007860	2	El sistema debe ignorar los mensajes de redireccionamiento de ICMP de IPv6.	**Ubicación** `/etc/security/pscexpert/dodv2/ntwkoptsdod` **Acción de conformidad** Establece el valor de la opción de red `ipignoreredirects` en *1*.
GEN007880	2	El sistema no debe enviar redirecciones de ICMP de IPv6.	**Ubicación** `/etc/security/pscexpert/dodv2/ntwkoptsdod` **Acción de conformidad** Establece el valor de la opción de red `ipsendredirects` en *0*.
GEN007900	2	El sistema debe utilizar un filtro de vía de acceso inversa adecuado para el tráfico de red IPv6, si el sistema utiliza IPv6.	**Ubicación** `/etc/security/pscexpert/dodv2/chuserstanzadod` **Acción de conformidad** Asegura que el sistema cumpla los requisitos especificados.
GEN007920	2	El sistema no debe reenviar paquetes IPv6 direccionados de origen.	**Ubicación** `/etc/security/pscexpert/dodv2/ntwkoptsdod` **Acción de conformidad** Establece el valor de la opción de red `ip6srcrouteforward` en *0*.

Tabla 2. Requisitos generales de DoD (continuación)

ID de punto de comprobación de Department of Defense STIG	Categoría de la regla de STIG	Descripción	Ubicación del script donde se define la acción y los resultados de la acción que permite la conformidad
GEN007940: GEN003607	2	El sistema no debe aceptar paquetes IPv4 o IPv6 direccionados de origen.	**Ubicación** `/etc/security/pscexpert/dodv2/ntwkoptsdod` **Acción de conformidad** Establece el valor de la opción de red `ipsrcrouterecv` en *0*.
GEN007950	2	El sistema no debe responder a las solicitudes de eco de ICMPv6 que se envían a una dirección de difusión.	**Ubicación** `/etc/security/pscexpert/dodv2/ntwkoptsdod` **Acción de conformidad** Establece el valor de la opción de red `bcastping` en *0*.
GEN008000	2	Si el sistema está utilizando Lightweight Directory Access Protocol (LDAP) para la información de autenticación o cuenta, los certificados que se utilizan para autenticar el servidor LDAP deben proporcionarse de la PKI de DoD o un método aprobado por DoD.	**Ubicación** `/etc/security/pscexpert/dodv2/ldap_config` **Acción de conformidad** Asegura que el sistema cumpla los requisitos especificados.
GEN008020	2	Si el sistema está utilizando LDAP para la información de autenticación o cuenta, la conexión de Seguridad de la capa de transporte (TLS) de LDAP debe requerir que el servidor proporcione un certificado con una vía de acceso de confianza válida.	**Ubicación** `/etc/security/pscexpert/dodv2/ldap_config` **Acción de conformidad** Asegura que el sistema cumpla los requisitos especificados.
GEN008050	2	Si el sistema está utilizando LDAP para la información de autenticación o cuenta, el archivo `/etc/ldap.conf` (o equivalente) no debe contener contraseñas.	**Ubicación** `/etc/security/pscexpert/dodv2/ldap_config` **Acción de conformidad** Asegura que el sistema cumpla los requisitos especificados.
GEN008380	2	El sistema debe comprobarse semanalmente para ver si hay archivos `setuid` no autorizados y modificación no autorizada en archivos `setuid` autorizados.	**Ubicación** `/etc/security/pscexpert/dodv2/trust` **Acción de conformidad** Comprueba semanalmente para identificar cambios en los archivos especificados.

Tabla 2. Requisitos generales de DoD (continuación)

ID de punto de comprobación de Department of Defense STIG	Categoría de la regla de STIG	Descripción	Ubicación del script donde se define la acción y los resultados de la acción que permite la conformidad
GEN008520	2	El sistema debe emplear un cortafuegos local que proteja el host frente a exploraciones de puerto. El cortafuegos debe evitar los puertos vulnerables durante 5 minutos para proteger el host frente a exploraciones de puerto.	**Ubicación** `/etc/security/pscexpert/dodv2/ipsecshunports` **Acción de conformidad** Asegura que el sistema cumpla los requisitos especificados.
GEN008540	2	El cortafuegos local del sistema debe implementar una política *deny-all, allow-by-exception*.	**Ubicación** `/etc/security/pscexpert/dodv2/ipsecshunhosthls` **Acción de conformidad** Asegura que el sistema cumpla los requisitos especificados. **Nota:** Puede especificar reglas de filtro adicionales en el archivo `/etc/security/aixpert/bin/filter.txt`. Estas reglas las integra el script `ipsecshunhosthls.sh` cuando se aplica el perfil. Las entradas deben estar en el formato siguiente: *número_puerto*`:`*dirección_IP*`:` *acción* donde los valores posibles para *acción* son `Allow` o `Deny`.
GEN008600	1	El sistema debe configurarse para iniciarse sólo desde la configuración de arranque del sistema.	**Ubicación** `/etc/security/pscexpert/dodv2/dodv2cat1` **Acción de conformidad** Asegura que el inicio del sistema sólo utilice la configuración de arranque del sistema.
GEN008640	1	El sistema no debe utilizar los medios extraíbles como el cargador de arranque.	**Ubicación** `/etc/security/pscexpert/dodv2/dodv2cat1` **Acción de conformidad** Asegura que el sistema no arranque desde una unidad extraíble.
GEN009140	1,2,3	El sistema no debe tener el servicio `chargen` activo.	**Ubicación** `/etc/security/pscexpert/dodv2/inetdservices` **Acción de conformidad** Inhabilita los daemons y servicios necesarios comentando las entradas en el archivo `/etc/inetd.conf`.
GEN009160	1,2,3	El sistema no debe tener el servicio `Calendar Management Service Daemon` (CMSD) activo.	**Ubicación** `/etc/security/pscexpert/dodv2/inetdservices` **Acción de conformidad** Inhabilita los daemons y servicios necesarios comentando las entradas en el archivo `/etc/inetd.conf`.

Tabla 2. Requisitos generales de DoD (continuación)

ID de punto de comprobación de Department of Defense STIG	Categoría de la regla de STIG	Descripción	Ubicación del script donde se define la acción y los resultados de la acción que permite la conformidad
GEN009180	1,2,3	El sistema no debe tener el servicio `tool-talk database server` (ttdbserver) activo.	**Ubicación** `/etc/security/pscexpert/dodv2/inetdservices` **Acción de conformidad** Inhabilita los daemons y servicios necesarios comentando las entradas en el archivo `/etc/inetd.conf`.
GEN009190	1,2,3	El sistema no debe tener el servicio `comsat` activo.	**Ubicación** `/etc/security/pscexpert/dodv2/inetdservices` **Acción de conformidad** Inhabilita los daemons y servicios necesarios comentando las entradas en el archivo `/etc/inetd.conf`.
GEN009200-9330	1,2,3	El sistema no puede tener otros servicios y daemons activos.	**Ubicación** `/etc/security/pscexpert/dodv2/inetdservices` **Acción de conformidad** Inhabilita los daemons y servicios necesarios comentando las entradas en el archivo `/etc/inetd.conf`.
GEN009210	2	El sistema no debe tener el servicio `discard` activo.	**Ubicación** `/etc/security/pscexpert/dodv2/inetdservices` **Acción de conformidad** Inhabilita los daemons y servicios necesarios comentando las entradas en el archivo `/etc/inetd.conf`.
GEN009220	2	El sistema no debe tener el servicio `dtspc` activo.	**Ubicación** `/etc/security/pscexpert/dodv2/inetdservices` **Acción de conformidad** Inhabilita los daemons y servicios necesarios comentando las entradas en el archivo `/etc/inetd.conf`.
GEN009230	2	El sistema no debe tener el servicio `echo` activo.	**Ubicación** `/etc/security/pscexpert/dodv2/inetdservices` **Acción de conformidad** Inhabilita los daemons y servicios necesarios comentando las entradas en el archivo `/etc/inetd.conf`.
GEN009240	2	El sistema no debe tener el servicio `IMAP (Internet Message Access Protocol)` activo.	**Ubicación** `/etc/security/pscexpert/dodv2/inetdservices` **Acción de conformidad** Inhabilita los daemons y servicios necesarios comentando las entradas en el archivo `/etc/inetd.conf`.
GEN009250	2	El sistema no debe tener el servicio `PostOffice Protocol (POP3)` activo.	**Ubicación** `/etc/security/pscexpert/dodv2/inetdservices` **Acción de conformidad** Inhabilita los daemons y servicios necesarios comentando las entradas en el archivo `/etc/inetd.conf`.

Tabla 2. Requisitos generales de DoD (continuación)

ID de punto de comprobación de Department of Defense STIG	Categoría de la regla de STIG	Descripción	Ubicación del script donde se define la acción y los resultados de la acción que permite la conformidad
GEN009260	2	El sistema no debe tener los servicios de talk o `ntalk` activos.	**Ubicación** `/etc/security/pscexpert/dodv2/inetdservices` **Acción de conformidad** Inhabilita los daemons y servicios necesarios comentando las entradas en el archivo `/etc/inetd.conf`.
GEN009270	2	El sistema no debe tener el servicio `netstat` activo en el proceso InetD.	**Ubicación** `/etc/security/pscexpert/dodv2/inetdservices` **Acción de conformidad** Inhabilita los daemons y servicios necesarios comentando las entradas en el archivo `/etc/inetd.conf`.
GEN009280	2	El sistema no debe tener el servicio `PCNFS` activo.	**Ubicación** `/etc/security/pscexpert/dodv2/inetdservices` **Acción de conformidad** Inhabilita los daemons y servicios necesarios comentando las entradas en el archivo `/etc/inetd.conf`.
GEN009290	2	El sistema no debe tener el servicio `systat` activo.	**Ubicación** `/etc/security/pscexpert/dodv2/inetdservices` **Acción de conformidad** Inhabilita los daemons y servicios necesarios comentando las entradas en el archivo `/etc/inetd.conf`.
GEN009300	2	El servicio `inetd time` no debe estar activo en el sistema en el daemon `inetd`.	**Ubicación** `/etc/security/pscexpert/dodv2/inetdservices` **Acción de conformidad** Inhabilita los daemons y servicios necesarios comentando las entradas en el archivo `/etc/inetd.conf`.
GEN009310	2	El sistema no debe tener el servicio `rusersd` activo.	**Ubicación** `/etc/security/pscexpert/dodv2/inetdservices` **Acción de conformidad** Inhabilita los daemons y servicios necesarios comentando las entradas en el archivo `/etc/inetd.conf`.
GEN009320	2	El sistema no debe tener el servicio `sprayd` activo.	**Ubicación** `/etc/security/pscexpert/dodv2/inetdservices` **Acción de conformidad** Inhabilita los daemons y servicios necesarios comentando las entradas en el archivo `/etc/inetd.conf`.
GEN009330	2	El sistema no debe tener el servicio `rstatd` activo.	**Ubicación** `/etc/security/pscexpert/dodv2/inetdservices` **Acción de conformidad** Inhabilita los daemons y servicios necesarios comentando las entradas en el archivo `/etc/inetd.conf`.

Tabla 2. Requisitos generales de DoD (continuación)

ID de punto de comprobación de Department of Defense STIG	Categoría de la regla de STIG	Descripción	Ubicación del script donde se define la acción y los resultados de la acción que permite la conformidad
GEN009340	2	Los gestores de inicio de sesión de servidor X no deben estar ejecutándose a menos que sean necesarios para la gestión de sesiones X11.	**Ubicación** `/etc/security/pscexpert/dodv2/dodv2cmntrows` **Acción de conformidad** Esta regla inhabilita las conexiones de sistema X Window y el gestor de inicio de sesión XServer.

Tabla 3. Requisitos de propiedad de DoD

ID de punto de comprobación de Department of Defense STIG	Descripción	Ubicación del script donde se define la acción y los resultados de la acción que permite la conformidad
AIX00085	El archivo `/etc/netsvc.conf` debe ser propiedad de root.	**Ubicación** `/etc/security/pscexpert/dodv2/chowndodfiles` **Acción de conformidad** Asegura que el archivo especificado sea propiedad de root.
AIX00090	El archivo `/etc/netsvc.conf` debe ser propiedad de grupo de bin, sys o system.	**Ubicación** `/etc/security/pscexpert/dodv2/chowndodfiles` **Acción de conformidad** Asegura que el archivo especificado sea propiedad de grupo de bin, sys o system.
AIX00320	El archivo `/etc/ftpaccess.ctl` debe ser propiedad de root.	**Ubicación** `/etc/security/pscexpert/dodv2/chowndodfiles` **Acción de conformidad** Asegura que el archivo especificado sea propiedad de root.
AIX00330	El archivo `/etc/ftpaccess.ctl` debe ser propiedad de grupo de bin, sys o system.	**Ubicación** `/etc/security/pscexpert/dodv2/chowndodfiles` **Acción de conformidad** Asegura que el archivo especificado sea propiedad de grupo de bin, sys o system.
GEN000250	El archivo de configuración de sincronización de tiempo (como `/etc/ntp.conf`) debe ser propiedad de root.	**Ubicación** `/etc/security/pscexpert/dodv2/chowndodfiles` **Acción de conformidad** Asegura que el archivo especificado sea propiedad de root.
GEN000251	El archivo de configuración de sincronización de tiempo (como, por ejemplo, `/etc/ntp.conf`) debe ser propiedad de grupo de bin, sys o system.	**Ubicación** `/etc/security/pscexpert/dodv2/chowndodfiles` **Acción de conformidad** Asegura que el archivo especificado sea propiedad de grupo de bin, sys o system.

Tabla 3. Requisitos de propiedad de DoD (continuación)

ID de punto de comprobación de Department of Defense STIG	Descripción	Ubicación del script donde se define la acción y los resultados de la acción que permite la conformidad
GEN001160	Todos los archivos y directorios debe tener un propietario válido.	**Ubicación** `/etc/security/pscexpert/dodv2/chowndodfiles` **Acción de conformidad** Asegura que todos los archivos y directorios tengan un propietario válido.
GEN001170	Todos los archivos y directorios deben tener un propietario de grupo válido.	**Ubicación** `/etc/security/pscexpert/dodv2/chowndodfiles` **Acción de conformidad** Asegura que todos los archivos y directorios tengan un propietario válido.
GEN001220	Todos los archivos, programas y directorios de sistema deben ser propiedad de una cuenta de sistema.	**Ubicación** `/etc/security/pscexpert/dodv2/chowndodfiles` **Acción de conformidad** Asegura que los archivos, programas y directorios de sistema sean propiedad de una cuenta de sistema.
GEN001240	Los archivos, programas y directorios de sistema deben ser propiedad de grupo de un grupo de sistema.	**Ubicación** `/etc/security/pscexpert/dodv2/chowndodfiles` **Acción de conformidad** Todos los archivos, programas y directorios de sistema son propiedad de grupo de un grupo de sistema.
GEN001320	Los archivos Network Information Systems (NIS)/NIS+/yp deben ser propiedad de root, sys o bin.	**Ubicación** `/etc/security/pscexpert/dodv2/chowndodfiles` **Acción de conformidad** Asegura que los archivos especificados sean propiedad de root, sys o bin.
GEN001340	Los archivos NIS/NIS+/yp deben ser propiedad de grupo de sys, bin, other o system.	**Ubicación** `/etc/security/pscexpert/dodv2/chowndodfiles` **Acción de conformidad** Asegura que los archivos especificados son propiedad de sys, bin, other o system.
GEN001362	El archivo `/etc/resolv.conf` debe ser propiedad de root.	**Ubicación** `/etc/security/pscexpert/dodv2/chowndodfiles` **Acción de conformidad** Asegura que el archivo especificado sea propiedad de root.

Tabla 3. Requisitos de propiedad de DoD (continuación)

ID de punto de comprobación de Department of Defense STIG	Descripción	Ubicación del script donde se define la acción y los resultados de la acción que permite la conformidad
GEN001363	El archivo `/etc/resolv.conf` debe ser propiedad de grupo de bin, sys o system.	**Ubicación** `/etc/security/pscexpert/dodv2/chowndodfiles` **Acción de conformidad** Asegura que el archivo especificado sea propiedad de grupo de bin, sys o system.
GEN001366	El archivo `/etc/hosts` debe ser propiedad de root.	**Ubicación** `/etc/security/pscexpert/dodv2/chowndodfiles` **Acción de conformidad** Asegura que el archivo especificado sea propiedad de root.
GEN001367	El archivo `/etc/hosts` debe ser propiedad de grupo de bin, sys o system.	**Ubicación** `/etc/security/pscexpert/dodv2/chowndodfiles` **Acción de conformidad** Asegura que el archivo especificado sea propiedad de grupo de bin, sys o system.
GEN001371	El archivo `/etc/nsswitch.conf` debe ser propiedad de root.	**Ubicación** `/etc/security/pscexpert/dodv2/chowndodfiles` **Acción de conformidad** Asegura que el archivo especificado sea propiedad de root.
GEN001372	El archivo `/etc/nsswitch.conf` debe ser propiedad de grupo de root, bin, sys o system.	**Ubicación** `/etc/security/pscexpert/dodv2/chowndodfiles` **Acción de conformidad** Asegura que el archivo especificado sea propiedad de grupo de root, bin, sys o system.
GEN001378	El archivo `/etc/passwd` debe ser propiedad de root.	**Ubicación** `/etc/security/pscexpert/dodv2/chowndodfiles` **Acción de conformidad** Asegura que el archivo especificado sea propiedad de root.
GEN001379	El archivo `/etc/passwd` debe ser propiedad de grupo de bin, security, sys o system.	**Ubicación** `/etc/security/pscexpert/dodv2/chowndodfiles` **Acción de conformidad** Asegura que el archivo especificado sea propiedad de grupo de bin, security, sys o system.

Tabla 3. Requisitos de propiedad de DoD (continuación)

ID de punto de comprobación de Department of Defense STIG	Descripción	Ubicación del script donde se define la acción y los resultados de la acción que permite la conformidad
GEN001391	El archivo `/etc/group` debe ser propiedad de root	**Ubicación** `/etc/security/pscexpert/dodv2/chowndodfiles` **Acción de conformidad** Asegura que el archivo especificado sea propiedad de root.
GEN001392	El archivo `/etc/group` debe ser propiedad de grupo de bin, security, sys o system.	**Ubicación** `/etc/security/pscexpert/dodv2/chowndodfiles` **Acción de conformidad** Asegura que el archivo especificado sea propiedad de grupo de bin, security, sys o system.
GEN001400	El archivo `/etc/security/passwd` debe ser propiedad de root.	**Ubicación** `/etc/security/pscexpert/dodv2/chowndodfiles` **Acción de conformidad** Asegura que el archivo especificado sea propiedad de root.
GEN001410	El archivo `/etc/security/passwd` debe ser propiedad de grupo de bin, security, sys o system.	**Ubicación** `/etc/security/pscexpert/dodv2/chowndodfiles` **Acción de conformidad** Asegura que el archivo especificado sea propiedad de grupo de bin, security, sys o system.
GEN001500	Los directorios de inicio de todos los usuarios interactivos deben ser propiedad de sus respectivos usuarios.	**Ubicación** `/etc/security/pscexpert/dodv2/chowndodfiles` **Acción de conformidad** Asegura que todos los directorios de inicio de los usuarios interactivos deban ser propiedad de sus respectivos usuarios.
GEN001520	Los directorios de inicio de todos los usuarios interactivos deben ser propiedad del grupo primario del propietario del directorio de inicio.	**Ubicación** `/etc/security/pscexpert/dodv2/chowndodfiles` **Acción de conformidad** Asegura que los directorios de inicio de todos los usuarios interactivos sean propiedad del grupo primario del propietario del directorio de inicio.
GEN001540	Todos los archivos y directorios que están contenidos en los directorios de inicio del usuario interactivo deben ser propiedad del propietario del directorio de inicio.	**Ubicación** `/etc/security/pscexpert/dodv2/chowndodfiles` **Acción de conformidad** Asegura que todos los archivos y directorios que están contenidos en los directorios de inicio del usuario interactivo sean propiedad del propietario del directorio de inicio.

Tabla 3. Requisitos de propiedad de DoD (continuación)

ID de punto de comprobación de Department of Defense STIG	Descripción	Ubicación del script donde se define la acción y los resultados de la acción que permite la conformidad
GEN001550	Todos los archivos y directorios que están contenidos en los directorios de inicio del usuario deben ser propiedad de un grupo del que el propietario del directorio de inicio sea miembro.	**Ubicación** `/etc/security/pscexpert/dodv2/chowndodfiles` **Acción de conformidad** Asegura que todos los archivos y directorios que están contenidos en los directorios de inicio del usuario deben ser propiedad de un grupo del que el propietario del directorio de inicio sea miembro.
GEN001660	Todos los archivos de inicio de sistema deben ser propiedad de root.	**Ubicación** `/etc/security/pscexpert/dodv2/chowndodfiles` **Acción de conformidad** Asegura que los archivos especificados sean propiedad de root.
GEN001680	Todos los archivos de inicio de sistema deben ser propiedad de grupo de sys, bin, other o system.	**Ubicación** `/etc/security/pscexpert/dodv2/chowndodfiles` **Acción de conformidad** Asegura que los archivos especificados sean propiedad de grupo de sys, bin, other o system.
GEN001740	Todos los archivos de inicialización globales deben ser propiedad de root.	**Ubicación** `/etc/security/pscexpert/dodv2/chowndodfiles` **Acción de conformidad** Asegura que los archivos especificados sean propiedad de root.
GEN001760	Todos los archivos de inicialización globales deben ser propiedad de grupo de sys, bin, system o security.	**Ubicación** `/etc/security/pscexpert/dodv2/chowndodfiles` **Acción de conformidad** Asegura que los archivos especificados sean propiedad de grupo de sys, bin, system o security.
GEN001820	Todos los archivos esquemáticos y directorios (normalmente en `/etc/skel`) deben ser propiedad de root o bin.	**Ubicación** `/etc/security/pscexpert/dodv2/chowndodfiles` **Acción de conformidad** Asegura que los archivos y directorios especificados sean propiedad de root o bin.
GEN001830	Todos los archivos esquemáticos (normalmente en `/etc/skel`) deben ser propiedad de grupo de security.	**Ubicación** `/etc/security/pscexpert/dodv2/chowndodfiles` **Acción de conformidad** Asegura que los archivos especificados sean propiedad de grupo de security.

Tabla 3. Requisitos de propiedad de DoD (continuación)

ID de punto de comprobación de Department of Defense STIG	Descripción	Ubicación del script donde se define la acción y los resultados de la acción que permite la conformidad
GEN001860	Todos los archivos de inicialización locales deben ser propiedad del usuario o root.	**Ubicación** `/etc/security/pscexpert/dodv2/chowndodfiles` **Acción de conformidad** Asegura que los archivos especificados sean propiedad del usuario o root.
GEN001870	Archivos de inicialización locales deben ser propiedad de grupo de root o del grupo primario del usuario.	**Ubicación** `/etc/security/pscexpert/dodv2/chowndodfiles` **Acción de conformidad** Asegura que los archivos de inicialización locales sean propiedad de grupo de root o del grupo primario del usuario.

GEN002060	Todos los archivos `.rhosts`, `.shosts`, `.netrc` o `hosts.equiv` deben ser accesible sólo por root o el propietario.	**Ubicación**
		`/etc/security/pscexpert/dodv2/chowndodfiles`
		`/etc/security/pscexpert/dodv2/fpmdodfiles`
		Acción de conformidad
		Asegura que sólo root o el propietario pueda acceder a los archivos especificados.

GEN002100	Pluggable Authentication Module (PAM) no debe soportar el archivo `.rhosts`.	**Ubicación** `/etc/security/pscexpert/dodv2/chowndodfiles` **Acción de conformidad** Asegura que el archivo especificado no esté disponible utilizando PAM.
GEN002200	Todos los archivos de shell deben ser propiedad de root o bin.	**Ubicación** `/etc/security/pscexpert/dodv2/chowndodfiles` **Acción de conformidad** Asegura que los archivos especificados sean propiedad de root o bin.
GEN002210	Todos los archivos de shell deben ser propiedad de grupo de root, bin, sys o system.	**Ubicación** `/etc/security/pscexpert/dodv2/chowndodfiles` **Acción de conformidad** Asegura que los archivos especificados sean propiedad de grupo de root, bin, sys o system.
GEN002340	Los dispositivos de audio deben ser propiedad de root.	**Ubicación** `/etc/security/pscexpert/dodv2/chowndodfiles` **Acción de conformidad** Asegura que todos los dispositivos de audio sean propiedad de root.

Tabla 3. Requisitos de propiedad de DoD (continuación)

ID de punto de comprobación de Department of Defense STIG	Descripción	Ubicación del script donde se define la acción y los resultados de la acción que permite la conformidad
GEN002360	Los dispositivos de audio deben ser propiedad de grupo de root, sys, bin o system.	**Ubicación** `/etc/security/pscexpert/dodv2/chowndodfiles` **Acción de conformidad** Asegura que todos los dispositivos de audio sean propiedad de grupo de root, sys, bin o system.
GEN002520	Todos los directorios públicos deben ser propiedad de root o una cuenta de aplicación.	**Ubicación** `/etc/security/pscexpert/dodv2/chowndodfiles` **Acción de conformidad** Asegura que todos los directorios públicos sean propiedad de root o una cuenta de aplicación.
GEN002540	Todos los directorios públicos deben ser propiedad de grupo de sistema o un grupo de aplicaciones.	**Ubicación** `/etc/security/pscexpert/dodv2/chowndodfiles` **Acción de conformidad** Asegura que todos los directorios públicos sean propiedad de grupo de sistema o un grupo de aplicaciones.
GEN002680	Los registros de auditoría de sistema deben ser propiedad de root.	**Ubicación** `/etc/security/pscexpert/dodv2/chowndodfiles` **Acción de conformidad** Asegura que los archivos especificados sean propiedad de root.
GEN002690	Los registros de auditoría de sistema deben ser propiedad de grupo de bin, sys o system.	**Ubicación** `/etc/security/pscexpert/dodv2/chowndodfiles` **Acción de conformidad** Asegura que los archivos especificados sean propiedad de grupo de bin, sys o system.
GEN003020	`Cron` no debe ejecutar programas en directorios grabables a nivel mundial o subordinados a ellos.	**Ubicación** `/etc/security/pscexpert/dodv2/chowndodfiles` **Acción de conformidad** Impide que `cron` ejecute programas en directorios grabables a nivel mundial o subordinados a ellos.
GEN003040	`Crontabs` debe ser propiedad de root o del creador de crontab.	**Ubicación** `/etc/security/pscexpert/dodv2/chowndodfiles` **Acción de conformidad** Asegura que los crontabs sean propiedad de root o del creador de crontab.

Tabla 3. Requisitos de propiedad de DoD (continuación)

ID de punto de comprobación de Department of Defense STIG	Descripción	Ubicación del script donde se define la acción y los resultados de la acción que permite la conformidad
GEN003050	Los archivos `Crontab` deben ser propiedad de grupo de system, cron o del grupo primario del creador de crontab.	**Ubicación** `/etc/security/pscexpert/dodv2/chowndodfiles` **Acción de conformidad** Asegura que los archivos `crontab` sean propiedad de grupo de system, cron o del grupo primario del creador de crontab.
GEN003110	Los directorios `cron` y `crontab` no deben tener listas de control de acceso ampliadas.	**Ubicación** `/etc/security/pscexpert/dodv2/chowndodfiles` **Acción de conformidad** Asegura que los directorios especificados no tengan listas de control de acceso ampliadas.
GEN003120	Los directorios `cron` y `crontab` deben ser propiedad de root o bin.	**Ubicación** `/etc/security/pscexpert/dodv2/chowndodfiles` **Acción de conformidad** Asegura que los directorios cron y crontab sean propiedad de root o bin.
GEN003140	Los directorios `cron` y `crontab` deben ser propiedad de grupo de system, sys, bin o cron.	**Ubicación** `/etc/security/pscexpert/dodv2/chowndodfiles` **Acción de conformidad** Asegura que los directorios especificados sean propiedad de grupo de system, sys, bin o cron.
GEN003160	Se debe implementar el registro de cron.	**Ubicación** `/etc/security/pscexpert/dodv2/chowndodfiles` **Acción de conformidad** Asegura que se implemente el registro de cron.
GEN003240	El archivo `cron.allow` debe ser propiedad de root, bin o sys.	**Ubicación** `/etc/security/pscexpert/dodv2/chowndodfiles` **Acción de conformidad** Asegura que el archivo especificado sea propiedad de root, bin o sys.
GEN003250	El archivo `cron.allow` debe ser propiedad de grupo de system, bin, sys o cron.	**Ubicación** `/etc/security/pscexpert/dodv2/chowndodfiles` **Acción de conformidad** Asegura que el archivo especificado sea propiedad de grupo de system, bin, sys o cron.

Tabla 3. Requisitos de propiedad de DoD (continuación)

ID de punto de comprobación de Department of Defense STIG	Descripción	Ubicación del script donde se define la acción y los resultados de la acción que permite la conformidad
GEN003260	El archivo `cron.deny` debe ser propiedad de root, bin o sys.	**Ubicación** `/etc/security/pscexpert/dodv2/chowndodfiles` **Acción de conformidad** Asegura que el archivo especificado sea propiedad de root, bin o sys.
GEN003270	El archivo `cron.deny` debe ser propiedad de grupo de system, bin, sys o cron.	**Ubicación** `/etc/security/pscexpert/dodv2/chowndodfiles` **Acción de conformidad** Asegura que el archivo especificado sea propiedad de grupo de system, bin, sys o cron.
GEN003420	El directorio `at` debe ser propiedad de root, bin, sys, daemon o cron.	**Ubicación** `/etc/security/pscexpert/dodv2/chowndodfiles` **Acción de conformidad** Asegura que el directorio especificado sea propiedad de root, sys, daemon o cron.
GEN003430	El directorio `at` debe ser propiedad de grupo de system, bin, sys o cron.	**Ubicación** `/etc/security/pscexpert/dodv2/chowndodfiles` **Acción de conformidad** Asegura que el directorio especificado sea propiedad de grupo de system, bin, sys o cron.
GEN003460	El archivo `at.allow` debe ser propiedad de root, bin o sys.	**Ubicación** `/etc/security/pscexpert/dodv2/chowndodfiles` **Acción de conformidad** Asegura que el archivo especificado sea propiedad de root, bin o sys.
GEN003470	El archivo `at.allow` debe ser propiedad de grupo de system, bin, sys o cron.	**Ubicación** `/etc/security/pscexpert/dodv2/chowndodfiles` **Acción de conformidad** Asegura que el archivo especificado sea propiedad de grupo de system, bin, sys o cron.
GEN003480	El archivo `at.deny` debe ser propiedad de root, bin o sys.	**Ubicación** `/etc/security/pscexpert/dodv2/chowndodfiles` **Acción de conformidad** Asegura que el archivo especificado sea propiedad de root, bin o sys.

Tabla 3. Requisitos de propiedad de DoD (continuación)

ID de punto de comprobación de Department of Defense STIG	Descripción	Ubicación del script donde se define la acción y los resultados de la acción que permite la conformidad
GEN003490	El archivo `at.deny` debe ser propiedad de grupo de system, bin, sys o cron.	**Ubicación** `/etc/security/pscexpert/dodv2/chowndodfiles` **Acción de conformidad** Asegura que el archivo especificado sea propiedad de grupo de system, bin, sys o cron.
GEN003720	El archivo `inetd.conf`, el archivo `xinetd.conf` y el directorio `xinetd.d` deben ser propiedad de root o bin.	**Ubicación** `/etc/security/pscexpert/dodv2/chowndodfiles` **Acción de conformidad** Asegura que los archivos y el directorio especificados sean propiedad de root o bin.
GEN003730	El archivo `inetd.conf`, el archivo `xinetd.conf` y el directorio `xinetd.d` deben ser propiedad de grupo de bin, sys o system.	**Ubicación** `/etc/security/pscexpert/dodv2/chowndodfiles` **Acción de conformidad** Asegura que los archivos y el directorio especificados sean propiedad de grupo de bin, sys o system.
GEN003760	El archivo `services` debe ser propiedad de root o bin.	**Ubicación** `/etc/security/pscexpert/dodv2/chowndodfiles` **Acción de conformidad** Asegura que el archivo especificado sea propiedad de root o bin.
GEN003770	El archivo `services` debe ser propiedad de grupo de bin, sys o system.	**Ubicación** `/etc/security/pscexpert/dodv2/chowndodfiles` **Acción de conformidad** Asegura que el archivo especificado sea propiedad de grupo de bin, sys o system.
GEN003920	El archivo `hosts.lpd` (o equivalente) debe ser propiedad de root, bin, sys o lp.	**Ubicación** `/etc/security/pscexpert/dodv2/chowndodfiles` **Acción de conformidad** Asegura que el archivo especificado sea propiedad de root, bin, sys o lp.
GEN003930	El archivo `hosts.lpd` (o equivalente) debe ser propiedad de grupo de bin, sys o system.	**Ubicación** `/etc/security/pscexpert/dodv2/chowndodfiles` **Acción de conformidad** Asegura que el archivo especificado sea propiedad de grupo de bin, sys o system.

Tabla 3. Requisitos de propiedad de DoD (continuación)

ID de punto de comprobación de Department of Defense STIG	Descripción	Ubicación del script donde se define la acción y los resultados de la acción que permite la conformidad
GEN003960	El propietario del mandato **traceroute** debe ser root.	**Ubicación** `/etc/security/pscexpert/dodv2/chowndodfiles` **Acción de conformidad** Asegura que el propietario del mandato sea root.
GEN003980	El mandato **traceroute** debe ser propiedad de grupo de sys, bin o system.	**Ubicación** `/etc/security/pscexpert/dodv2/chowndodfiles` **Acción de conformidad** Asegura que el mandato sea propiedad de grupo de sys, bin o system.
GEN004360	El archivo `alias` debe ser propiedad de root.	**Ubicación** `/etc/security/pscexpert/dodv2/chowndodfiles` **Acción de conformidad** Asegura que el archivo especificado sea propiedad de root.
GEN004370	El archivo `aliases` archivo debe ser propiedad de grupo de sys, bin o system.	**Ubicación** `/etc/security/pscexpert/dodv2/chowndodfiles` **Acción de conformidad** Asegura que el archivo especificado sea propiedad de grupo de sys, bin o system.
GEN004400	Los archivos que se ejecutan a través de un archivo `aliases` de correo deben ser propiedad de root y debe estar ubicados en un directorio que sea propiedad sólo de root y sea grabable sólo por root.	**Ubicación** `/etc/security/pscexpert/dodv2/chowndodfiles` **Acción de conformidad** Asegura que los archivos que se ejecutan a través de un archivo `aliases` de correo sean propiedad de root y se encuentren dentro de un directorio que sea propiedad sólo de root y sea grabable sólo por root.
GEN004410	Los archivos que se ejecutan a través de un archivo `aliases` de correo deben ser propiedad de grupo de root, bin, sys u otro. También deben encontrarse dentro de un directorio que sea propiedad de grupo de root, bin, sys u otro.	**Ubicación** `/etc/security/pscexpert/dodv2/chowndodfiles` **Acción de conformidad** Asegura que los archivos que se ejecutan a través de un archivo `aliases` de correo sean propiedad de grupo de root, bin, sys u otro y estén ubicados en un directorio que sea propiedad de grupo de root, bin, sys u otro.
GEN004480	El archivo de registro de servicio SMTP debe ser propiedad de root.	**Ubicación** `/etc/security/pscexpert/dodv2/chowndodfiles` **Acción de conformidad** Asegura que el archivo especificado sea propiedad de root.

Tabla 3. Requisitos de propiedad de DoD (continuación)

ID de punto de comprobación de Department of Defense STIG	Descripción	Ubicación del script donde se define la acción y los resultados de la acción que permite la conformidad
GEN004920	El archivo `ftpusers` debe ser propiedad de root.	**Ubicación** `/etc/security/pscexpert/dodv2/chowndodfiles` **Acción de conformidad** Asegura que el archivo especificado sea propiedad de root.
GEN004930	El archivo `ftpusers` debe ser propiedad de grupo de bin, sys o system.	**Ubicación** `/etc/security/pscexpert/dodv2/chowndodfiles` **Acción de conformidad** Asegura que el archivo especificado sea propiedad de grupo de bin, sys o system.
GEN005360	El archivo `snmpd.conf` debe ser propiedad de root.	**Ubicación** `/etc/security/pscexpert/dodv2/chowndodfiles` **Acción de conformidad** Asegura que el archivo especificado sea propiedad de root.
GEN005365	El archivo `snmpd.conf` debe ser propiedad de grupo de bin, sys o system.	**Ubicación** `/etc/security/pscexpert/dodv2/chowndodfiles` **Acción de conformidad** Asegura que el archivo especificado sea propiedad de grupo de bin, sys o system.
GEN005400	El archivo `/etc/syslog.conf` debe ser propiedad de root.	**Ubicación** `/etc/security/pscexpert/dodv2/chowndodfiles` **Acción de conformidad** Asegura que el archivo especificado sea propiedad de root.
GEN005420	El archivo `/etc/syslog.conf` debe ser propiedad de grupo de bin, sys o system.	**Ubicación** `/etc/security/pscexpert/dodv2/chowndodfiles` **Acción de conformidad** Asegura que el archivo especificado sea propiedad de grupo de bin, sys o system.
GEN005610	El sistema no debe tener el reenvío de IP para IPv6 habilitado, a menos que el sistema sea un direccionador IPv6.	**Ubicación** `/etc/security/pscexpert/dodv2/chowndodfiles` **Acción de conformidad** Asegura que el reenvío de IP para IPv6 no esté habilitado a menos que el sistema esté siendo utilizado como un direccionador IPv6.

Tabla 3. Requisitos de propiedad de DoD (continuación)

ID de punto de comprobación de Department of Defense STIG	Descripción	Ubicación del script donde se define la acción y los resultados de la acción que permite la conformidad
GEN005740	El archivo de configuración de exportación NFS debe ser propiedad de root.	**Ubicación** `/etc/security/pscexpert/dodv2/chowndodfiles` **Acción de conformidad** Asegura que el archivo especificado sea propiedad de root.
GEN005750	El archivo de configuración de exportación NFS debe ser propiedad de grupo de root, bin, sys o syxtem.	**Ubicación** `/etc/security/pscexpert/dodv2/chowndodfiles` **Acción de conformidad** Asegura que el archivo especificado sea propiedad de grupo de root, bin, sys o system.
GEN005800	Todos los archivos de sistema y directorios de sistema exportados por NFS deben ser propiedad de root.	**Ubicación** `/etc/security/pscexpert/dodv2/chowndodfiles` **Acción de conformidad** Asegura que el archivo especificado sea propiedad de root.
GEN005810	Todos los archivos de sistema y directorios de sistema exportados por NFS deben ser propiedad de grupo de root, bin, sys o system.	**Ubicación** `/etc/security/pscexpert/dodv2/chowndodfiles` **Acción de conformidad** Asegura que los archivos y directorios especificados son propiedad de grupo de root, bin, sys o system.
GEN006100	El archivo `/usr/lib/smb.conf` debe ser propiedad de root.	**Ubicación** `/etc/security/pscexpert/dodv2/chowndodfiles` **Acción de conformidad** Asegura que el archivo especificado sea propiedad de root.
GEN006120	El archivo `/usr/lib/smb.conf` debe ser propiedad de grupo de bin, sys o system.	**Ubicación** `/etc/security/pscexpert/dodv2/chowndodfiles` **Acción de conformidad** Asegura que el archivo especificado sea propiedad de grupo de bin, sys o system.
GEN006160	El archivo `/var/private/smbpasswd` debe ser propiedad de root.	**Ubicación** `/etc/security/pscexpert/dodv2/chowndodfiles` **Acción de conformidad** Asegura que el archivo especificado sea propiedad de root.

Tabla 3. Requisitos de propiedad de DoD (continuación)

ID de punto de comprobación de Department of Defense STIG	Descripción	Ubicación del script donde se define la acción y los resultados de la acción que permite la conformidad
GEN006180	El archivo /var/private/smbpasswd debe ser propiedad de grupo de sys o system.	**Ubicación** /etc/security/pscexpert/dodv2/chowndodfiles **Acción de conformidad** Asegura que el archivo especificado sea propiedad de grupo de sys o system.
GEN006340	Los archivos del directorio /etc/news deben ser propiedad de root o news.	**Ubicación** /etc/security/pscexpert/dodv2/chowndodfiles **Acción de conformidad** Asegura que el directorio especificado sea propiedad de root o news.
GEN006360	Los archivos de /etc/news deben ser propiedad de grupo de system o news.	**Ubicación** /etc/security/pscexpert/dodv2/chowndodfiles **Acción de conformidad** Asegura que los archivos especificados sean propiedad de grupo de system o news.
GEN008080	Si el sistema está utilizando LDAP para obtener información de autenticación o cuenta, el archivo /etc/ldap.conf (o equivalente) debe ser propiedad de root.	**Ubicación** /etc/security/pscexpert/dodv2/chowndodfiles **Acción de conformidad** Asegura que el archivo especificado sea propiedad de root.
GEN008100	Si el sistema está utilizando LDAP para obtener información de autenticación o cuenta, el archivo /etc/ldap.conf (o equivalente) debe ser propiedad de grupo de security, bin, sys o system.	**Ubicación** /etc/security/pscexpert/dodv2/chowndodfiles **Acción de conformidad** Asegura que el archivo especificado sea propiedad de grupo de bin, sys o system.
GEN008140	Si el sistema está utilizando LDAP para obtener información de autenticación o cuenta, el archivo o directorio de autoridad de certificado TLS debe ser propiedad de root.	**Ubicación** /etc/security/pscexpert/dodv2/chowndodfiles **Acción de conformidad** Asegura que el archivo especificado sea propiedad de root.
GEN008160	Si el sistema está utilizando LDAP para obtener información de autenticación o cuenta, el archivo o directorio de autoridad de certificado TLS debe ser propiedad de grupo de root, bin, sys o system.	**Ubicación** /etc/security/pscexpert/dodv2/chowndodfiles **Acción de conformidad** Asegura que el archivo especificado sea propiedad de grupo de bin, sys o system.

Tabla 4. Estándares de DoD para permisos de archivo

ID de punto de comprobación de Department of Defense STIG	Descripción	Ubicación del script donde se define la acción y los resultados de la acción que permite la conformidad
AIX00100	El archivo `/etc/netsvc.conf` debe tener la modalidad 0644 o una modalidad que sea menos permisiva.	**Ubicación** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Acción de conformidad** Asegura que el archivo se establezca en la modalidad de permiso especificada o en una que sea menos permisiva.
AIX00340	El archivo `/etc/ftpaccess.ctl` debe tener la modalidad 0640 o una modalidad que sea menos permisiva.	**Ubicación** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Acción de conformidad** Asegura que el archivo se establezca en la modalidad de permiso especificada o en una que sea menos permisiva.
GEN000252	El archivo de configuración de sincronización de tiempo (como, por ejemplo, `/etc/ntp.conf`) debe tener la modalidad 0640 o una modalidad que sea menos permisiva.	**Ubicación** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Acción de conformidad** Asegura que el archivo se establezca en la modalidad de permiso especificada o en una que sea menos permisiva.
GEN000920	El directorio de inicio de la cuenta root (distinto `/`) debe tener la modalidad 0700.	**Ubicación** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Acción de conformidad** Asegura que el directorio se establezca en la modalidad de permiso especificada o en una que sea menos permisiva.
GEN001140	Los archivos y directorios del sistema no deben tener permisos de acceso desiguales.	**Ubicación** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Acción de conformidad** Asegura que los permisos de acceso sean coherentes.
GEN001180	Los archivos de daemon de servicios de red deben tener la modalidad 0755 o una modalidad que sea menos permisiva.	**Ubicación** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Acción de conformidad** Asegura que los archivos se establezcan en la modalidad de permiso especificada en una que sea menos permisiva.
GEN001200	Todos los archivos de mandatos del sistema deben tener la modalidad 0755 o una modalidad que sea menos permisiva.	**Ubicación** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Acción de conformidad** Asegura que los archivos se establezcan en la modalidad de permiso especificada en una que sea menos permisiva.

Tabla 4. Estándares de DoD para permisos de archivo (continuación)

ID de punto de comprobación de Department of Defense STIG	Descripción	Ubicación del script donde se define la acción y los resultados de la acción que permite la conformidad
GEN001260	Los archivos de registro del sistema deben tener la modalidad 0640 o una modalidad que sea menos permisiva.	**Ubicación** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Acción de conformidad** Asegura que los archivos se establezcan en la modalidad de permiso especificada en una que sea menos permisiva.
GEN001280	Los archivos de página de manual deben tener la modalidad 0644 o una modalidad que sea menos permisiva.	**Ubicación** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Acción de conformidad** Asegura que los archivos se establezcan en la modalidad de permiso especificada en una que sea menos permisiva.
GEN001300	Los archivos de biblioteca deben tener la modalidad 0755 o una modalidad que sea menos permisiva.	**Ubicación** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Acción de conformidad** Asegura que los archivos se establezcan en la modalidad de permiso especificada en una que sea menos permisiva.
GEN001360	Los archivos NIS/NIS+/yp deben tener la modalidad 0755 o una modalidad que sea menos permisiva.	**Ubicación** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Acción de conformidad** Asegura que los archivos se establezcan en la modalidad de permiso especificada en una que sea menos permisiva.
GEN001364	El archivo `/etc/resolv.conf` debe tener la modalidad 0644 o una modalidad que sea menos permisiva.	**Ubicación** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Acción de conformidad** Asegura que el archivo se establezca en la modalidad de permiso especificada o en una que sea menos permisiva.
GEN001368	El archivo `/etc/hosts` debe tener la modalidad 0644 o una modalidad que sea menos permisiva.	**Ubicación** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Acción de conformidad** Asegura que el archivo se establezca en la modalidad de permiso especificada o en una que sea menos permisiva.
GEN001373	El archivo `/etc/nsswitch.conf` debe tener la modalidad 0644 o una modalidad que sea menos permisiva.	**Ubicación** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Acción de conformidad** Asegura que el archivo se establezca en la modalidad de permiso especificada o en una que sea menos permisiva.

Tabla 4. Estándares de DoD para permisos de archivo (continuación)

ID de punto de comprobación de Department of Defense STIG	Descripción	Ubicación del script donde se define la acción y los resultados de la acción que permite la conformidad
GEN001380	El archivo `/etc/passwd` debe tener la modalidad 0644 o una modalidad que sea menos permisiva.	**Ubicación** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Acción de conformidad** Asegura que el archivo se establezca en la modalidad de permiso especificada o en una que sea menos permisiva.
GEN001393	El archivo `/etc/group` debe tener la modalidad 0644 o una modalidad que sea menos permisiva.	**Ubicación** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Acción de conformidad** Asegura que el archivo se establezca en la modalidad de permiso especificada o en una que sea menos permisiva.
GEN001420	El archivo `/etc/security/passwd` debe tener la modalidad 0400.	**Ubicación** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Acción de conformidad** Asegura que el archivo se establezca en la modalidad de permiso especificada o en una que sea menos permisiva.
GEN001480	Todos los directorios de inicio de un usuario deben tener una modalidad de 0750 o menos permisiva.	**Ubicación** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Acción de conformidad** Asegura que el archivo se establezca en la modalidad de permiso especificada o en una que sea menos permisiva.
GEN001560	Todos los archivos y directorios que están contenidos en los directorios de inicio de un usuario deben tener la modalidad 0750 o una modalidad que sea menos permisiva.	**Ubicación** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Acción de conformidad** Asegura que los archivos se establezcan en la modalidad de permiso especificada en una que sea menos permisiva.
GEN001580	Todos los scripts de control de ejecución deben tener la modalidad 0755 o una modalidad que sea menos permisiva.	**Ubicación** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Acción de conformidad** Asegura que los archivos se establezcan en la modalidad de permiso especificada en una que sea menos permisiva.
GEN001640	Los scripts de control de ejecución no deben ejecutar programas o scripts grabables a nivel mundial.	**Ubicación** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Acción de conformidad** Comprueba en los programas, como `cron`, si hay programas o scripts grabables a nivel mundial.

Tabla 4. Estándares de DoD para permisos de archivo (continuación)

ID de punto de comprobación de Department of Defense STIG	Descripción	Ubicación del script donde se define la acción y los resultados de la acción que permite la conformidad
GEN001720	Todos los archivos de inicialización globales deben tener la modalidad 0644 o una modalidad que sea menos permisiva.	**Ubicación** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Acción de conformidad** Asegura que los archivos se establezcan en la modalidad de permiso especificada en una que sea menos permisiva.
GEN001800	Todos los archivos de esqueleto (por ejemplo, archivos en `/etc/skel`) deben tener la modalidad 0644 o una modalidad que sea menos permisiva.	**Ubicación** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Acción de conformidad** Asegura que los archivos se establezcan en la modalidad de permiso especificada en una que sea menos permisiva.
GEN001880	Todos los archivos de inicialización locales deben tener la modalidad 0740 o una modalidad que sea menos permisiva.	**Ubicación** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Acción de conformidad** Asegura que los archivos se establezcan en la modalidad de permiso especificada en una que sea menos permisiva.
GEN002220	Todos los archivos de shell deben tener la modalidad 0755 o una modalidad que sea menos permisiva.	**Ubicación** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Acción de conformidad** Asegura que los archivos se establezcan en la modalidad de permiso especificada en una que sea menos permisiva.
GEN002320	Los dispositivos de audio deben tener la modalidad 0660 o una modalidad que sea menos permisiva.	**Ubicación** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Acción de conformidad** Asegura que los dispositivos de audio estén establecidos en la modalidad de permiso especificada o una que sea menos permisiva.
GEN002560	El valor predeterminado de sistema y usuario **umask** debe ser 077.	**Ubicación** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Acción de conformidad** Asegura que los valores especificados sean *077*.
GEN002700	Los registros de auditoría del sistema deben tener la modalidad 0640 o una modalidad que sea menos permisiva.	**Ubicación** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Acción de conformidad** Asegura que los archivos se establezcan en la modalidad de permiso especificada en una que sea menos permisiva.

Tabla 4. Estándares de DoD para permisos de archivo (continuación)

ID de punto de comprobación de Department of Defense STIG	Descripción	Ubicación del script donde se define la acción y los resultados de la acción que permite la conformidad
GEN002717	Los archivos ejecutables de la herramienta de auditoría de sistema deben tener la modalidad 0750 o una modalidad que sea menos permisiva.	**Ubicación** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Acción de conformidad** Asegura que los archivos se establezcan en la modalidad de permiso especificada en una que sea menos permisiva.
GEN002980	El archivo `cron.allow` debe tener la modalidad 0600 o una modalidad que sea menos permisiva.	**Ubicación** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Acción de conformidad** Asegura que el archivo se establezca en la modalidad de permiso especificada o en una que sea menos permisiva.
GEN003080	Los archivos crontab deben tener la modalidad 0600 o una modalidad que sea menos permisiva.	**Ubicación** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Acción de conformidad** Asegura que los archivos se establezcan en la modalidad de permiso especificada en una que sea menos permisiva.
GEN003090	Los archivos `crontab` no deben tener listas de control de acceso (ACL) ampliadas.	**Ubicación** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Acción de conformidad** Asegura que los archivos especificados no tengan ACL ampliadas.
GEN003100	Los directorios cron y crontab deben tener la modalidad 0755 o una modalidad que sea menos permisiva.	**Ubicación** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Acción de conformidad** Asegura que los directorios especificados se establezcan en la modalidad de permisos especificada o en una que sea menos permisiva.
GEN003180	El archivo `cronlog` debe tener la modalidad 0600 o una modalidad que sea menos permisiva.	**Ubicación** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Acción de conformidad** Asegura que el archivo se establezca en la modalidad de permiso especificada o en una que sea menos permisiva.
GEN003200	El archivo `cron.deny` debe tener la modalidad 0600 o una modalidad que sea menos permisiva.	**Ubicación** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Acción de conformidad** Asegura que el archivo se establezca en la modalidad de permiso especificada o en una que sea menos permisiva.

Tabla 4. Estándares de DoD para permisos de archivo (continuación)

ID de punto de comprobación de Department of Defense STIG	Descripción	Ubicación del script donde se define la acción y los resultados de la acción que permite la conformidad
GEN003252	El archivo `at.deny` debe tener la modalidad 0640 o una modalidad que sea menos permisiva.	**Ubicación** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Acción de conformidad** Asegura que el archivo se establezca en la modalidad de permiso especificada o en una que sea menos permisiva.
GEN003340	El archivo `at.allow` debe tener la modalidad 0600 o una modalidad que sea menos permisiva.	**Ubicación** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Acción de conformidad** Asegura que el archivo se establezca en la modalidad de permiso especificada o en una que sea menos permisiva.
GEN003400	El directorio `at` debe tener la modalidad 0755 o una modalidad que sea menos permisiva.	**Ubicación** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Acción de conformidad** Asegura que el directorio se establezca en la modalidad de permiso especificada o en una que sea menos permisiva.
GEN003440	Los trabajos `At` no deben establecer el parámetro **`umask`** en un valor menos restrictivo que 077.	**Ubicación** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Acción de conformidad** Asegura que el parámetro se establezca en la modalidad de permiso especificada o en una que sea menos permisiva.
GEN003740	Los archivos `inetd.conf` y `xinetd.conf` deben tener la modalidad 0440 o una modalidad que sea menos permisiva.	**Ubicación** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Acción de conformidad** Asegura que los archivos se establezcan en la modalidad de permiso especificada en una que sea menos permisiva.
GEN003780	El archivo `services` debe tener la modalidad 0444 o una modalidad que sea menos permisiva.	**Ubicación** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Acción de conformidad** Asegura que el archivo se establezca en la modalidad de permiso especificada o en una que sea menos permisiva.
GEN003940	El archivo `hosts.lpd` (o equivalente) debe tener la modalidad 0644 o una modalidad que sea menos permisiva.	**Ubicación** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Acción de conformidad** Asegura que el archivo se establezca en la modalidad de permiso especificada o en una que sea menos permisiva.

Tabla 4. Estándares de DoD para permisos de archivo (continuación)

ID de punto de comprobación de Department of Defense STIG	Descripción	Ubicación del script donde se define la acción y los resultados de la acción que permite la conformidad
GEN004000	El archivo `traceroute` debe tener la modalidad 0700 o una modalidad que sea menos permisiva.	**Ubicación** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Acción de conformidad** Asegura que el archivo se establezca en la modalidad de permiso especificada o en una que sea menos permisiva.
GEN004380	El archivo `alias` debe tener la modalidad 0644 o una modalidad que sea menos permisiva.	**Ubicación** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Acción de conformidad** Asegura que el archivo se establezca en la modalidad de permiso especificada o en una que sea menos permisiva.
GEN004420	Los archivos que se ejecutan a través de un archivo `aliases` de correo deben tener la modalidad 0755 o una modalidad que sea menos permisiva.	**Ubicación** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Acción de conformidad** Asegura que los archivos se establezcan en la modalidad de permiso especificada en una que sea menos permisiva.
GEN004500	El archivo de registro de servicio SMTP debe tener la modalidad 0644 o una modalidad que sea menos permisiva.	**Ubicación** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Acción de conformidad** Asegura que el archivo se establezca en la modalidad de permiso especificada o en una que sea menos permisiva.
GEN004940	El archivo `ftpusers` debe tener la modalidad 0640 o una modalidad que sea menos permisiva.	**Ubicación** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Acción de conformidad** Asegura que el archivo se establezca en la modalidad de permiso especificada o en una que sea menos permisiva.
GEN005040	Todos los usuarios FTP deben tener un valor predeterminado de **`umask`** de 077.	**Ubicación** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Acción de conformidad** Asegura que el valor sea correcto.
GEN005100	El daemon `TFTP` debe tener la modalidad 0755 o una modalidad que sea menos permisiva.	**Ubicación** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Acción de conformidad** Asegura que el daemon se establezca en la modalidad especificada o en una que sea menos permisiva.

Tabla 4. Estándares de DoD para permisos de archivo (continuación)

ID de punto de comprobación de Department of Defense STIG	Descripción	Ubicación del script donde se define la acción y los resultados de la acción que permite la conformidad
GEN005180	Todos los archivos `.Xauthority` deben tener la modalidad 0600 o una modalidad que sea menos permisiva.	**Ubicación** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Acción de conformidad** Asegura que los archivos se establezcan en la modalidad de permiso especificada en una que sea menos permisiva.
GEN005320	El archivo `snmpd.conf` debe tener la modalidad 0600 o una modalidad que sea menos permisiva.	**Ubicación** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Acción de conformidad** Asegura que el archivo se establezca en la modalidad de permiso especificada o en una que sea menos permisiva.
GEN005340	Los archivos MIB (Management Information Base) deben tener la modalidad 0640 o una modalidad que sea menos permisiva.	**Ubicación** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Acción de conformidad** Asegura que los archivos se establezcan en la modalidad de permiso especificada en una que sea menos permisiva.
GEN005390	El archivo `/etc/syslog.conf` debe tener la modalidad 0640 o una modalidad que sea menos permisiva.	**Ubicación** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Acción de conformidad** Asegura que el archivo se establezca en la modalidad de permiso especificada o en una que sea menos permisiva.
GEN005522	Los archivos de claves de host públicas SSH deben tener la modalidad 0644 o una modalidad que sea menos permisiva.	**Ubicación** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Acción de conformidad** Asegura que los archivos se establezcan en la modalidad de permiso especificada en una que sea menos permisiva.
GEN005523	Los archivos de claves de host privadas SSH deben tener la modalidad 0600 o una modalidad que sea menos permisiva.	**Ubicación** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Acción de conformidad** Asegura que los archivos se establezcan en la modalidad de permiso especificada en una que sea menos permisiva.
GEN006140	El archivo `/usr/lib/smb.conf` debe tener la modalidad 0644 o una modalidad que sea menos permisiva.	**Ubicación** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Acción de conformidad** Asegura que el archivo se establezca en la modalidad de permiso especificada o en una que sea menos permisiva.

Tabla 4. Estándares de DoD para permisos de archivo (continuación)

ID de punto de comprobación de Department of Defense STIG	Descripción	Ubicación del script donde se define la acción y los resultados de la acción que permite la conformidad
GEN006200	El archivo `/var/private/smbpasswd` debe tener la modalidad 0600 o una modalidad que sea menos permisiva.	**Ubicación** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Acción de conformidad** Asegura que el archivo se establezca en la modalidad de permiso especificada o en una que sea menos permisiva.
GEN006260	El archivo `/etc/news/hosts.nntp` (o equivalente) debe tener la modalidad 0600 o una modalidad que sea menos permisiva.	**Ubicación** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Acción de conformidad** Asegura que el archivo se establezca en la modalidad de permiso especificada o en una que sea menos permisiva.
GEN006280	El archivo `/etc/news/hosts.nntp.nolimit` (o equivalente) debe tener la modalidad 0600 o una modalidad que sea menos permisiva.	**Ubicación** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Acción de conformidad** Asegura que el archivo se establezca en la modalidad de permiso especificada o en una que sea menos permisiva.
GEN006300	El archivo `/etc/news/nnrp.access` (o equivalente) debe tener la modalidad 0600 o una modalidad que sea menos permisiva.	**Ubicación** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Acción de conformidad** Asegura que el archivo se establezca en la modalidad de permiso especificada o en una que sea menos permisiva.
GEN006320	El archivo `/etc/news/passwd.nntp` (o equivalente) debe tener la modalidad 0600 o una modalidad que sea menos permisiva.	**Ubicación** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Acción de conformidad** Asegura que el archivo se establezca en la modalidad de permiso especificada o en una que sea menos permisiva.
GEN008060	Si el sistema está utilizando LDAP para obtener información de autenticación o cuenta, el archivo `/etc/ldap.conf` (o equivalente) debe tener la modalidad 0644 o una menos permisiva.	**Ubicación** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Acción de conformidad** Asegura que el archivo se establezca en la modalidad de permiso especificada o en una que sea menos permisiva.
GEN008180	Si el sistema está utilizando LDAP para obtener información de autenticación o cuenta, el archivo y/o directorio de autoridad de certificado TLS deben tener la modalidad 0644 (0755 para directorios) o una menos permisiva.	**Ubicación** `/etc/security/pscexpert/dodv2/fpmdodfiles` **Acción de conformidad** Asegura que el archivo especificado, los directorios o ambos se establezcan en la modalidad de permiso especificada o en una que sea menos permisiva.

Tabla 5. Requisitos de lista de control de acceso (ACL) de DoD

ID de punto de comprobación de Department of Defense STIG	Descripción	Ubicación del script donde se define la acción y los resultados de la acción que permite la conformidad
AIX00110	El archivo `/etc/netsvc.conf` no debe tener una lista de control de acceso (ACL) ampliada.	**Ubicación** `/etc/security/pscexpert/dodv2/acldodfiles` **Acción de conformidad** Inhabilita la ACL ampliada especificada. **Nota:** Este valor no cambia automáticamente cuando la política se restablece en la política predeterminada de AIX utilizando el archivo `DoDv2_to_AIXDefault.xml`. Debe cambiar manualmente este valor.
AIX00350	El archivo `/etc/ftpaccess.ctl` no debe tener una ACL ampliada.	**Ubicación** `/etc/security/pscexpert/dodv2/acldodfiles` **Acción de conformidad** Inhabilita la ACL ampliada especificada. **Nota:** Este valor no cambia automáticamente cuando la política se restablece en la política predeterminada de AIX utilizando el archivo `DoDv2_to_AIXDefault.xml`. Debe cambiar manualmente este valor.
GEN000253	El archivo de configuración de sincronización de tiempo (como `/etc/ntp.conf`) no debe tener una ACL ampliada.	**Ubicación** `/etc/security/pscexpert/dodv2/acldodfiles` **Acción de conformidad** Inhabilita la ACL ampliada especificada. **Nota:** Este valor no cambia automáticamente cuando la política se restablece en la política predeterminada de AIX utilizando el archivo `DoDv2_to_AIXDefault.xml`. Debe cambiar manualmente este valor.
GEN000930	El directorio de inicio de la cuenta root no debe tener una ACL ampliada.	**Ubicación** `/etc/security/pscexpert/dodv2/acldodfiles` **Acción de conformidad** Inhabilita la ACL ampliada especificada. **Nota:** Este valor no cambia automáticamente cuando la política se restablece en la política predeterminada de AIX utilizando el archivo `DoDv2_to_AIXDefault.xml`. Debe cambiar manualmente este valor.

Tabla 5. Requisitos de lista de control de acceso (ACL) de DoD (continuación)

ID de punto de comprobación de Department of Defense STIG	Descripción	Ubicación del script donde se define la acción y los resultados de la acción que permite la conformidad
GEN001190	Todos los archivos de daemon de servicios de red no deben tener ACL ampliadas.	**Ubicación** `/etc/security/pscexpert/dodv2/acldodfiles` **Acción de conformidad** Inhabilita la ACL ampliada especificada. **Nota:** Este valor no cambia automáticamente cuando la política se restablece en la política predeterminada de AIX utilizando el archivo `DoDv2_to_AIXDefault.xml`. Debe cambiar manualmente este valor.
GEN001210	Todos los archivos de mandatos del sistema no deben tener ACL ampliadas.	**Ubicación** `/etc/security/pscexpert/dodv2/acldodfiles` **Acción de conformidad** Inhabilita la ACL ampliada especificada. **Nota:** Este valor no cambia automáticamente cuando la política se restablece en la política predeterminada de AIX utilizando el archivo `DoDv2_to_AIXDefault.xml`. Debe cambiar manualmente este valor.
GEN001270	Los archivos de registro del sistema no deben tener ACL ampliadas, excepto cuando sea necesario para soportar el software autorizado.	**Ubicación** `/etc/security/pscexpert/dodv2/acldodfiles` **Acción de conformidad** Inhabilita la ACL ampliada especificada. **Nota:** Este valor no cambia automáticamente cuando la política se restablece en la política predeterminada de AIX utilizando el archivo `DoDv2_to_AIXDefault.xml`. Debe cambiar manualmente este valor.
GEN001310	Todos los archivos de biblioteca no deben tener ACL ampliadas.	**Ubicación** `/etc/security/pscexpert/dodv2/acldodfiles` **Acción de conformidad** Inhabilita la ACL ampliada especificada. **Nota:** Este valor no cambia automáticamente cuando la política se restablece en la política predeterminada de AIX utilizando el archivo `DoDv2_to_AIXDefault.xml`. Debe cambiar manualmente este valor.

Tabla 5. Requisitos de lista de control de acceso (ACL) de DoD (continuación)

ID de punto de comprobación de Department of Defense STIG	Descripción	Ubicación del script donde se define la acción y los resultados de la acción que permite la conformidad
GEN001361	Los archivos de mandato NIS/NIS+/yp no deben tener ACL ampliadas.	**Ubicación** `/etc/security/pscexpert/dodv2/acldodfiles` **Acción de conformidad** Inhabilita la ACL ampliada especificada. **Nota:** Este valor no cambia automáticamente cuando la política se restablece en la política predeterminada de AIX utilizando el archivo `DoDv2_to_AIXDefault.xml`. Debe cambiar manualmente este valor.
GEN001365	El archivo `/etc/resolv.conf` no debe tener una ACL ampliada.	**Ubicación** `/etc/security/pscexpert/dodv2/acldodfiles` **Acción de conformidad** Inhabilita la ACL ampliada especificada. **Nota:** Este valor no cambia automáticamente cuando la política se restablece en la política predeterminada de AIX utilizando el archivo `DoDv2_to_AIXDefault.xml`. Debe cambiar manualmente este valor.
GEN001369	El archivo `/etc/hosts` no debe tener una ACL ampliada.	**Ubicación** `/etc/security/pscexpert/dodv2/acldodfiles` **Acción de conformidad** Inhabilita la ACL ampliada especificada. **Nota:** Este valor no cambia automáticamente cuando la política se restablece en la política predeterminada de AIX utilizando el archivo `DoDv2_to_AIXDefault.xml`. Debe cambiar manualmente este valor.
GEN001374	El archivo `/etc/nsswitch.conf` no debe tener una ACL ampliada.	**Ubicación** `/etc/security/pscexpert/dodv2/acldodfiles` **Acción de conformidad** Inhabilita la ACL ampliada especificada. **Nota:** Este valor no cambia automáticamente cuando la política se restablece en la política predeterminada de AIX utilizando el archivo `DoDv2_to_AIXDefault.xml`. Debe cambiar manualmente este valor.

Tabla 5. Requisitos de lista de control de acceso (ACL) de DoD (continuación)

ID de punto de comprobación de Department of Defense STIG	Descripción	Ubicación del script donde se define la acción y los resultados de la acción que permite la conformidad
GEN001390	El archivo `/etc/passwd` no debe tener una ACL ampliada.	**Ubicación** `/etc/security/pscexpert/dodv2/acldodfiles` **Acción de conformidad** Inhabilita la ACL ampliada especificada. **Nota:** Este valor no cambia automáticamente cuando la política se restablece en la política predeterminada de AIX utilizando el archivo `DoDv2_to_AIXDefault.xml`. Debe cambiar manualmente este valor.
GEN001394	El archivo `/etc/group` no debe tener una ACL ampliada.	**Ubicación** `/etc/security/pscexpert/dodv2/acldodfiles` **Acción de conformidad** Inhabilita la ACL ampliada especificada. **Nota:** Este valor no cambia automáticamente cuando la política se restablece en la política predeterminada de AIX utilizando el archivo `DoDv2_to_AIXDefault.xml`. Debe cambiar manualmente este valor.
GEN001430	El archivo `/etc/security/passwd` no debe tener una ACL ampliada.	**Ubicación** `/etc/security/pscexpert/dodv2/acldodfiles` **Acción de conformidad** Inhabilita la ACL ampliada especificada. **Nota:** Este valor no cambia automáticamente cuando la política se restablece en la política predeterminada de AIX utilizando el archivo `DoDv2_to_AIXDefault.xml`. Debe cambiar manualmente este valor.
GEN001570	Todos los archivos y directorios que están contenidos en los directorios de inicio de usuario no deben tener ACL ampliadas.	**Ubicación** `/etc/security/pscexpert/dodv2/acldodfiles` **Acción de conformidad** Inhabilita la ACL ampliada especificada. **Nota:** Este valor no cambia automáticamente cuando la política se restablece en la política predeterminada de AIX utilizando el archivo `DoDv2_to_AIXDefault.xml`. Debe cambiar manualmente este valor.

Tabla 5. Requisitos de lista de control de acceso (ACL) de DoD (continuación)

ID de punto de comprobación de Department of Defense STIG	Descripción	Ubicación del script donde se define la acción y los resultados de la acción que permite la conformidad
GEN001590	Todos los scripts de control de ejecución no deben tener ACL ampliadas.	**Ubicación** `/etc/security/pscexpert/dodv2/acldodfiles` **Acción de conformidad** Inhabilita la ACL ampliada especificada. **Nota:** Este valor no cambia automáticamente cuando la política se restablece en la política predeterminada de AIX utilizando el archivo `DoDv2_to_AIXDefault.xml`. Debe cambiar manualmente este valor.
GEN001730	Todos los archivos de inicialización globales no deben tener ACL ampliadas.	**Ubicación** `/etc/security/pscexpert/dodv2/acldodfiles` **Acción de conformidad** Inhabilita la ACL ampliada especificada. **Nota:** Este valor no cambia automáticamente cuando la política se restablece en la política predeterminada de AIX utilizando el archivo `DoDv2_to_AIXDefault.xml`. Debe cambiar manualmente este valor.
GEN001810	Los archivos esquemáticos no deben tener ACL ampliadas.	**Ubicación** `/etc/security/pscexpert/dodv2/acldodfiles` **Acción de conformidad** Inhabilita la ACL ampliada especificada. **Nota:** Este valor no cambia automáticamente cuando la política se restablece en la política predeterminada de AIX utilizando el archivo `DoDv2_to_AIXDefault.xml`. Debe cambiar manualmente este valor.
GEN001890	Los archivos de inicialización locales no deben tener ACL ampliadas.	**Ubicación** `/etc/security/pscexpert/dodv2/acldodfiles` **Acción de conformidad** Inhabilita la ACL ampliada especificada. **Nota:** Este valor no cambia automáticamente cuando la política se restablece en la política predeterminada de AIX utilizando el archivo `DoDv2_to_AIXDefault.xml`. Debe cambiar manualmente este valor.

Tabla 5. Requisitos de lista de control de acceso (ACL) de DoD (continuación)

ID de punto de comprobación de Department of Defense STIG	Descripción	Ubicación del script donde se define la acción y los resultados de la acción que permite la conformidad
GEN002230	Todos los archivos de shell no deben tener ACL ampliadas	**Ubicación** `/etc/security/pscexpert/dodv2/acldodfiles` **Acción de conformidad** Inhabilita la ACL ampliada especificada. **Nota:** Este valor no cambia automáticamente cuando la política se restablece en la política predeterminada de AIX utilizando el archivo `DoDv2_to_AIXDefault.xml`. Debe cambiar manualmente este valor.
GEN002330	Los dispositivos de audio no deben tener ACL ampliadas.	**Ubicación** `/etc/security/pscexpert/dodv2/acldodfiles` **Acción de conformidad** Inhabilita la ACL ampliada especificada. **Nota:** Este valor no cambia automáticamente cuando la política se restablece en la política predeterminada de AIX utilizando el archivo `DoDv2_to_AIXDefault.xml`. Debe cambiar manualmente este valor.
GEN002710	Todos los archivos de auditoría del sistema no deben tener ACL ampliadas	**Ubicación** `/etc/security/pscexpert/dodv2/acldodfiles` **Acción de conformidad** Inhabilita la ACL ampliada especificada. **Nota:** Este valor no cambia automáticamente cuando la política se restablece en la política predeterminada de AIX utilizando el archivo `DoDv2_to_AIXDefault.xml`. Debe cambiar manualmente este valor.
GEN002990	Las ACL ampliadas deben inhabilitarse para los archivos `cron.allow` y `cron.deny`.	**Ubicación** `/etc/security/pscexpert/dodv2/acldodfiles` **Acción de conformidad** Inhabilita la ACL ampliada especificada. **Nota:** Este valor no cambia automáticamente cuando la política se restablece en la política predeterminada de AIX utilizando el archivo `DoDv2_to_AIXDefault.xml`. Debe cambiar manualmente este valor.

Tabla 5. Requisitos de lista de control de acceso (ACL) de DoD (continuación)

ID de punto de comprobación de Department of Defense STIG	Descripción	Ubicación del script donde se define la acción y los resultados de la acción que permite la conformidad
GEN003090	Los archivos crontab no deben tener ACL ampliadas.	**Ubicación** `/etc/security/pscexpert/dodv2/acldodfiles` **Acción de conformidad** Inhabilita la ACL ampliada especificada. **Nota:** Este valor no cambia automáticamente cuando la política se restablece en la política predeterminada de AIX utilizando el archivo `DoDv2_to_AIXDefault.xml`. Debe cambiar manualmente este valor.
GEN003110	Los directorios cron y crontab no deben tener ACL ampliadas.	**Ubicación** `/etc/security/pscexpert/dodv2/acldodfiles` **Acción de conformidad** Inhabilita la ACL ampliada especificada. **Nota:** Este valor no cambia automáticamente cuando la política se restablece en la política predeterminada de AIX utilizando el archivo `DoDv2_to_AIXDefault.xml`. Debe cambiar manualmente este valor.
GEN003190	Los archivos de registro cron no deben tener ACL ampliadas.	**Ubicación** `/etc/security/pscexpert/dodv2/acldodfiles` **Acción de conformidad** Inhabilita la ACL ampliada especificada. **Nota:** Este valor no cambia automáticamente cuando la política se restablece en la política predeterminada de AIX utilizando el archivo `DoDv2_to_AIXDefault.xml`. Debe cambiar manualmente este valor.
GEN003210	El archivo `cron.deny` no debe tener una ACL ampliada.	**Ubicación** `/etc/security/pscexpert/dodv2/acldodfiles` **Acción de conformidad** Inhabilita la ACL ampliada especificada. **Nota:** Este valor no cambia automáticamente cuando la política se restablece en la política predeterminada de AIX utilizando el archivo `DoDv2_to_AIXDefault.xml`. Debe cambiar manualmente este valor.

Tabla 5. Requisitos de lista de control de acceso (ACL) de DoD (continuación)

ID de punto de comprobación de Department of Defense STIG	Descripción	Ubicación del script donde se define la acción y los resultados de la acción que permite la conformidad
GEN003245	El archivo `at.allow` no debe tener una ACL ampliada.	**Ubicación** `/etc/security/pscexpert/dodv2/acldodfiles` **Acción de conformidad** Inhabilita la ACL ampliada especificada. **Nota:** Este valor no cambia automáticamente cuando la política se restablece en la política predeterminada de AIX utilizando el archivo `DoDv2_to_AIXDefault.xml`. Debe cambiar manualmente este valor.
GEN003255	El archivo `at.deny` no debe tener una ACL ampliada.	**Ubicación** `/etc/security/pscexpert/dodv2/acldodfiles` **Acción de conformidad** Inhabilita la ACL ampliada especificada. **Nota:** Este valor no cambia automáticamente cuando la política se restablece en la política predeterminada de AIX utilizando el archivo `DoDv2_to_AIXDefault.xml`. Debe cambiar manualmente este valor.
GEN003410	El directorio `at` no debe tener una ACL ampliada.	**Ubicación** `/etc/security/pscexpert/dodv2/acldodfiles` **Acción de conformidad** Inhabilita la ACL ampliada especificada. **Nota:** Este valor no cambia automáticamente cuando la política se restablece en la política predeterminada de AIX utilizando el archivo `DoDv2_to_AIXDefault.xml`. Debe cambiar manualmente este valor.
GEN003745	Los archivos `inetd.conf` y `xinetd.conf` no deben tener ACL ampliadas.	**Ubicación** `/etc/security/pscexpert/dodv2/acldodfiles` **Acción de conformidad** Inhabilita la ACL ampliada especificada. **Nota:** Este valor no cambia automáticamente cuando la política se restablece en la política predeterminada de AIX utilizando el archivo `DoDv2_to_AIXDefault.xml`. Debe cambiar manualmente este valor.

Tabla 5. Requisitos de lista de control de acceso (ACL) de DoD (continuación)

ID de punto de comprobación de Department of Defense STIG	Descripción	Ubicación del script donde se define la acción y los resultados de la acción que permite la conformidad
GEN003790	El archivo de servicios no debe tener una ACL ampliada.	**Ubicación** `/etc/security/pscexpert/dodv2/acldodfiles` **Acción de conformidad** Inhabilita la ACL ampliada especificada. **Nota:** Este valor no cambia automáticamente cuando la política se restablece en la política predeterminada de AIX utilizando el archivo `DoDv2_to_AIXDefault.xml`. Debe cambiar manualmente este valor.
GEN003950	El archivo `hosts.lpd` (o equivalente) no debe tener una ACL ampliada.	**Ubicación** `/etc/security/pscexpert/dodv2/acldodfiles` **Acción de conformidad** Inhabilita la ACL ampliada especificada. **Nota:** Este valor no cambia automáticamente cuando la política se restablece en la política predeterminada de AIX utilizando el archivo `DoDv2_to_AIXDefault.xml`. Debe cambiar manualmente este valor.
GEN004010	El archivo `traceroute` no debe tener una ACL ampliada.	**Ubicación** `/etc/security/pscexpert/dodv2/acldodfiles` **Acción de conformidad** Inhabilita la ACL ampliada especificada. **Nota:** Este valor no cambia automáticamente cuando la política se restablece en la política predeterminada de AIX utilizando el archivo `DoDv2_to_AIXDefault.xml`. Debe cambiar manualmente este valor.
GEN004390	El archivo `alias` no debe tener una ACL ampliada.	**Ubicación** `/etc/security/pscexpert/dodv2/acldodfiles` **Acción de conformidad** Inhabilita la ACL ampliada especificada. **Nota:** Este valor no cambia automáticamente cuando la política se restablece en la política predeterminada de AIX utilizando el archivo `DoDv2_to_AIXDefault.xml`. Debe cambiar manualmente este valor.

Tabla 5. Requisitos de lista de control de acceso (ACL) de DoD (continuación)

ID de punto de comprobación de Department of Defense STIG	Descripción	Ubicación del script donde se define la acción y los resultados de la acción que permite la conformidad
GEN004430	Los archivos que se ejecutan a través de un archivo `aliases` de correo no debe tener ACL ampliadas.	**Ubicación** `/etc/security/pscexpert/dodv2/acldodfiles` **Acción de conformidad** Inhabilita la ACL ampliada especificada. **Nota:** Este valor no cambia automáticamente cuando la política se restablece en la política predeterminada de AIX utilizando el archivo `DoDv2_to_AIXDefault.xml`. Debe cambiar manualmente este valor.
GEN004510	El archivo de registro de servicio SMTP no debe tener una ACL ampliada.	**Ubicación** `/etc/security/pscexpert/dodv2/acldodfiles` **Acción de conformidad** Inhabilita la ACL ampliada especificada. **Nota:** Este valor no cambia automáticamente cuando la política se restablece en la política predeterminada de AIX utilizando el archivo `DoDv2_to_AIXDefault.xml`. Debe cambiar manualmente este valor.
GEN004950	El archivo `ftpusers` no debe tener una ACL ampliada.	**Ubicación** `/etc/security/pscexpert/dodv2/acldodfiles` **Acción de conformidad** Inhabilita la ACL ampliada especificada. **Nota:** Este valor no cambia automáticamente cuando la política se restablece en la política predeterminada de AIX utilizando el archivo `DoDv2_to_AIXDefault.xml`. Debe cambiar manualmente este valor.
GEN005190	Los archivos `.Xauthority` no deben tener ACL ampliadas.	**Ubicación** `/etc/security/pscexpert/dodv2/acldodfiles` **Acción de conformidad** Inhabilita la ACL ampliada especificada. **Nota:** Este valor no cambia automáticamente cuando la política se restablece en la política predeterminada de AIX utilizando el archivo `DoDv2_to_AIXDefault.xml`. Debe cambiar manualmente este valor.

Tabla 5. Requisitos de lista de control de acceso (ACL) de DoD (continuación)

ID de punto de comprobación de Department of Defense STIG	Descripción	Ubicación del script donde se define la acción y los resultados de la acción que permite la conformidad
GEN005350	Los archivos MIB (Management Information Base) no deben tener archivos ACL ampliadas.	**Ubicación** `/etc/security/pscexpert/dodv2/acldodfiles` **Acción de conformidad** Inhabilita la ACL ampliada especificada. **Nota:** Este valor no cambia automáticamente cuando la política se restablece en la política predeterminada de AIX utilizando el archivo `DoDv2_to_AIXDefault.xml`. Debe cambiar manualmente este valor.
GEN005375	El archivo `snmpd.conf` no debe tener una ACL ampliada	**Ubicación** `/etc/security/pscexpert/dodv2/acldodfiles` **Acción de conformidad** Inhabilita la ACL ampliada especificada. **Nota:** Este valor no cambia automáticamente cuando la política se restablece en la política predeterminada de AIX utilizando el archivo `DoDv2_to_AIXDefault.xml`. Debe cambiar manualmente este valor.
GEN005395	El archivo `/etc/syslog.conf` no debe tener una ACL ampliada.	**Ubicación** `/etc/security/pscexpert/dodv2/acldodfiles` **Acción de conformidad** Inhabilita la ACL ampliada especificada. **Nota:** Este valor no cambia automáticamente cuando la política se restablece en la política predeterminada de AIX utilizando el archivo `DoDv2_to_AIXDefault.xml`. Debe cambiar manualmente este valor.
GEN006150	El archivo `/usr/lib/smb.conf` no debe tener una ACL ampliada.	**Ubicación** `/etc/security/pscexpert/dodv2/acldodfiles` **Acción de conformidad** Inhabilita la ACL ampliada especificada. **Nota:** Este valor no cambia automáticamente cuando la política se restablece en la política predeterminada de AIX utilizando el archivo `DoDv2_to_AIXDefault.xml`. Debe cambiar manualmente este valor.

Tabla 5. Requisitos de lista de control de acceso (ACL) de DoD (continuación)

ID de punto de comprobación de Department of Defense STIG	Descripción	Ubicación del script donde se define la acción y los resultados de la acción que permite la conformidad
GEN006210	El archivo `/var/private/smbpasswd` no debe tener una ACL ampliada.	**Ubicación** `/etc/security/pscexpert/dodv2/acldodfiles` **Acción de conformidad** Inhabilita la ACL ampliada especificada. **Nota:** Este valor no cambia automáticamente cuando la política se restablece en la política predeterminada de AIX utilizando el archivo `DoDv2_to_AIXDefault.xml`. Debe cambiar manualmente este valor.
GEN006270	El archivo `/etc/news/hosts.nntp` no debe tener una ACL ampliada.	**Ubicación** `/etc/security/pscexpert/dodv2/acldodfiles` **Acción de conformidad** Inhabilita la ACL ampliada especificada. **Nota:** Este valor no cambia automáticamente cuando la política se restablece en la política predeterminada de AIX utilizando el archivo `DoDv2_to_AIXDefault.xml`. Debe cambiar manualmente este valor.
GEN006290	El archivo `/etc/news/hosts.nntp.nolimit` no debe tener una ACL ampliada.	**Ubicación** `/etc/security/pscexpert/dodv2/acldodfiles` **Acción de conformidad** Inhabilita la ACL ampliada especificada. **Nota:** Este valor no cambia automáticamente cuando la política se restablece en la política predeterminada de AIX utilizando el archivo `DoDv2_to_AIXDefault.xml`. Debe cambiar manualmente este valor.
GEN006310	El archivo `/etc/news/nnrp.access` no debe tener una ACL ampliada.	**Ubicación** `/etc/security/pscexpert/dodv2/acldodfiles` **Acción de conformidad** Inhabilita la ACL ampliada especificada. **Nota:** Este valor no cambia automáticamente cuando la política se restablece en la política predeterminada de AIX utilizando el archivo `DoDv2_to_AIXDefault.xml`. Debe cambiar manualmente este valor.

Tabla 5. Requisitos de lista de control de acceso (ACL) de DoD (continuación)

ID de punto de comprobación de Department of Defense STIG	Descripción	Ubicación del script donde se define la acción y los resultados de la acción que permite la conformidad
GEN006330	El archivo `/etc/news/passwd.nntp` no debe tener una ACL ampliada.	**Ubicación** `/etc/security/pscexpert/dodv2/acldodfiles` **Acción de conformidad** Inhabilita la ACL ampliada especificada. **Nota:** Este valor no cambia automáticamente cuando la política se restablece en la política predeterminada de AIX utilizando el archivo `DoDv2_to_AIXDefault.xml`. Debe cambiar manualmente este valor.
GEN008120	Si el sistema está utilizando LDAP para obtener información de autenticación o cuenta, el archivo `/etc/ldap.conf` (o equivalente) no debe tener una lista de control de acceso (ACL) ampliada.	**Ubicación** `/etc/security/pscexpert/dodv2/acldodfiles` **Acción de conformidad** Asegura que los archivos especificados no tengan una ACL ampliada. **Nota:** Este valor no cambia automáticamente cuando la política se restablece en la política predeterminada de AIX utilizando el archivo `DoDv2_to_AIXDefault.xml`. Debe cambiar manualmente este valor.
GEN008200	Si el sistema está utilizando LDAP para obtener información de autenticación o cuenta, el archivo de autoridad de certificado TLS de LDAP o directorio (según corresponda) no debe tener una ACL ampliada.	**Ubicación** `/etc/security/pscexpert/dodv2/acldodfiles` **Acción de conformidad** Asegura que el directorio o archivo especificado no tenga una ACL ampliada. **Nota:** Este valor no cambia automáticamente cuando la política se restablece en la política predeterminada de AIX utilizando el archivo `DoDv2_to_AIXDefault.xml`. Debe cambiar manualmente este valor.

Información relacionada:

Conformidad con Department of Defense STIG

Conformidad con Payment Card Industry - Data Security Standard

Payment Card Industry - Data Security Standard (PCI - DSS) clasifica la seguridad de TI en 12 secciones que se denominan los 12 requisitos y procedimientos de evaluación de seguridad.

Los 12 requisitos y procedimientos de evaluación de la seguridad de TI definidos por PCI - DSS incluyen los siguientes elementos:

Requisito 1: Instalar y mantener una configuración de cortafuegos para proteger los datos del titular de la tarjeta.

Lista documentada de servicios y puertos necesarios para el negocio. Este requisito se implementa inhabilitando servicios innecesarios e inseguros.

Requisito 2: No utilizar valores predeterminados proporcionados por el proveedor para las contraseñas de sistema y otros parámetros de seguridad.

Cambiar siempre los valores predeterminados proporcionados por el proveedor antes de instalar un sistema en la red. Este requisito se implementa inhabilitando el daemon de Protocolo simple de gestión de red (SNMP).

Requisito 3: Proteger los datos almacenados del titular de la tarjeta.

Este requisito se implementa habilitando la característica Sistema de archivos cifrado (EFS) que se proporciona con el sistema operativo AIX.

Requisito 4: Cifrar los datos del titular de la tarjeta cuando los datos se transmiten a través de redes públicas abiertas.

Este requisito se implementa habilitando la característica de Seguridad IP (IPSEC) que se proporciona con el sistema operativo AIX.

Requisito 5: Utilizar y actualizar regularmente los programas de software antivirus.

Este requisito se implementa utilizando el programa de política Trusted Execution. Trusted Execution es el software antivirus recomendado y es nativo del sistema operativo AIX. PCI requiere que se capturan los registros del programa Trusted Execution habilitando la información de seguridad y gestión de sucesos (SIEM) para supervisar las alertas. Al ejecutar el programa Trusted Execution en modalidad de sólo registro, no se detienen las ejecuciones cuando se produce un error debido a una discrepancia de hash.

Requisito 6: Desarrollar y mantener sistemas y aplicaciones seguros.

Para implementar este requisito, debe instalar manualmente los parches necesarios para el sistema. Si ha adquirido PowerSC Standard Edition, puede utilizar la característica Trusted Network Connect (TNC).

Requisito 7: Restringir el acceso a los datos del titular de la tarjeta, por necesidad de conocimiento del negocio.

Puede implementar medidas de control de accesos fuertes utilizando la característica RBAC para permitir reglas y roles. RBAC no se puede automatizar porque para habilitarse necesita la entrada de un administrador.

`RbacEnablement` comprueba el sistema para determinar si existen en el sistema las propiedades isso, so y sa para los roles. Si estas propiedades no existen, el script las crea. Este script también se ejecuta como parte de las comprobaciones de pscexpert que se realizan cuando se ejecutan mandatos, como el mandato `pscxpert -c`.

Requisito 8: Asignar un ID exclusivo a cada persona que tiene acceso al sistema.

Puede implementar este requisito habilitando perfiles PCI. Se aplican las reglas siguientes al perfil de PCI:

- Cambiar contraseñas de usuario como mínimo cada 90 días.
- Solicitar una longitud mínima de contraseña de 7 caracteres.
- Utilizar una contraseña que contenga números y caracteres alfabéticos.
- No permitir que una persona envíe una contraseña nueva que sea igual que las cuatro contraseñas anteriores que se han utilizado.
- Limitar los intentos de acceso repetidos bloqueando el ID de usuario después de seis intentos incorrectos.
- Establecer la duración de bloqueo en 30 minutos o hasta que un administrador vuelve a habilitar el ID de usuario.
- Solicitar a un usuario que vuelva a entrar una contraseña para reactivar un terminal después de que esté desocupado durante 15 minutos o más.

Requisito 9: Restringir el acceso físico a los datos del titular de la tarjeta.

Almacenar repositorios que contienen datos confidenciales del titular de la tarjeta en una sala de acceso restringido.

Requisito 10: Realizar el seguimiento y supervisar todo el acceso a los recursos de red y a los datos del titular de la tarjeta.

Este requisito se implementa mediante el registro de acceso a los componentes del sistema habilitando los registros automáticos en los componentes del sistema.

Requisito 11: Probar con regularidad los sistemas y procesos de seguridad.

Este requisito se implementa utilizando la característica de Conformidad en tiempo real.

Requisito 12: Mantener una política de seguridad que incluya seguridad de información para los empleados y contratistas.

Activación de módems para los proveedores sólo cuando sea necesario para los proveedores con la desactivación inmediata después del uso. Este requisito se implementa inhabilitando el inicio de sesión root remoto, activándolo según las necesidades a través de un administrador del sistema y, a continuación, desactivándolo cuando ya no es necesario.

PowerSC Standard Edition reduce la gestión de configuración que es necesaria para satisfacer las directrices definidas por PCI DSS versión 2.0 y PCI DSS versión 3.0. Sin embargo, el proceso entero no se puede automatizar.

Por ejemplo, la restricción del acceso a los datos del titular de la tarjeta basándose en el requisito empresarial no se puede automatizar. El sistema operativo AIX proporciona sólidas tecnologías de seguridad como, por ejemplo, el Control de acceso basado en rol (RBAC); sin embargo, PowerSC Standard Edition no puede automatizar esta configuración porque no puede determinar las personas que necesitan acceso y las personas que no. IBM Compliance Expert puede automatizar la configuración de otros valores de seguridad que sean compatibles con los requisitos de PCI.

Cuando se aplica el perfil PCI a un entorno de base de datos, varios puertos TCP y UDP utilizados por la pila de software se inhabilitan por las restricciones. Debe habilitar estos puertos y inhabilitar la función Trusted Execution para ejecutar la aplicación y la carga de trabajo. Ejecute los mandatos siguientes para eliminar las restricciones en los puertos y inhabilitar la función Trusted Execution:

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

Nota: Todos los archivos de script personalizados que se proporcionan para mantener la conformidad PCI - DSS están en el directorio `/etc/security/pscexpert/bin`.

La tabla siguiente muestra cómo PowerSC Standard Edition se encarga de los requisitos del estándar PCI DSS utilizando las funciones del programa de utilidad AIX Security Expert:

Tabla 6. Valores relacionados con los estándares de conformidad de PCI DSS versión 2.0 y versión 3.0

Implementa estos estándares de PCI DSS	Especificación de implementación	Implementación de AIX Security Expert	Ubicación del script que modifica el valor
2.1	Cambiar siempre los valores predeterminados proporcionados por el proveedor antes de instalar un sistema en la red. Por ejemplo, incluye contraseñas, cadenas de comunidad de protocolo de gestión de red simple y eliminar cuentas innecesarias.	Establece el número mínimo de semanas que deben pasar antes de poder cambiar una contraseña a 0 semanas estableciendo el parámetro **minage** en un valor de 0.	`/etc/security/pscexpert/bin/chusrattr`

Tabla 6. Valores relacionados con los estándares de conformidad de PCI DSS versión 2.0 y versión 3.0 (continuación)

Implementa estos estándares de PCI DSS	Especificación de implementación	Implementación de AIX Security Expert	Ubicación del script que modifica el valor
PCI versión 2 8.5.9 **PCI versión 3** 8.2.4	Cambiar contraseñas de usuario como mínimo cada 90 días.	Establece el número máximo de semanas que una contraseña es válida en 13 semanas estableciendo el parámetro **maxage** en un valor de 13.	/etc/security/pscexpert/bin/chusrattr
2.1	Cambiar siempre los valores predeterminados proporcionados por el proveedor antes de instalar un sistema en la red. Por ejemplo, incluye contraseñas, cadenas de comunidad de protocolo de gestión de red simple y eliminar cuentas innecesarias.	Establece el número de semanas que una cuenta con una contraseña caducada permanece en el sistema en 8 semanas estableciendo el parámetro **maxexpired** en un valor de 8.	/etc/security/pscexpert/bin/chusrattr
PCI versión 2 8.5.10 **PCI versión 3** 8.2.3	Solicitar una longitud mínima de contraseña de 7 caracteres al menos.	Establece la longitud mínima de contraseña en 7 caracteres estableciendo el parámetro **minlen** en un valor de 7.	/etc/security/pscexpert/bin/chusrattr
PCI versión 2 8.5.11 **PCI versión 3** 8.2.3	Utilizar contraseñas que contienen los caracteres numéricos y alfabéticos.	Establece el número mínimo de caracteres alfabéticos que se necesitan en una contraseña en 1. Este valor asegura que la contraseña contiene caracteres alfabéticos estableciendo el parámetro **minalpha** en un valor de 1.	/etc/security/pscexpert/bin/chusrattr
PCI versión 2 8.5.11 **PCI versión 3** 8.2.3	Utilizar contraseñas que contienen los caracteres numéricos y alfabéticos.	Establece el número mínimo de caracteres no alfabéticos que se necesitan en una contraseña en 1. Este valor asegura que la contraseña contiene caracteres no alfabéticos estableciendo el parámetro **minother** en un valor de 1.	/etc/security/pscexpert/bin/chusrattr
PCI versión 2 2.1 **PCI versión 3** 8.2.2	Cambiar siempre los valores predeterminados proporcionados por el proveedor antes de instalar un sistema en la red. Por ejemplo, incluye contraseñas, cadenas de comunidad de protocolo de gestión de red simple y eliminar cuentas innecesarias.	Establece el número máximo de veces que un carácter puede repetirse en una contraseña en 8 estableciendo el parámetro **maxrepeats** en un valor de 8. Este valor indica que un carácter de una contraseña puede repetirse un número ilimitado de veces cuando se ajusta a las demás limitaciones de contraseña.	/etc/security/pscexpert/bin/chusrattr
PCI versión 2 8.5.12 **PCI versión 3** 8.2.5	No permitir que una persona envíe una contraseña nueva que sea igual que alguna de las cuatro últimas contraseñas que ha utilizado.	Establece el número de semanas antes de que se pueda volver a utilizar una contraseña en 52 estableciendo el parámetro **histexpire** en un valor de 52.	/etc/security/pscexpert/bin/chusrattr

Tabla 6. Valores relacionados con los estándares de conformidad de PCI DSS versión 2.0 y versión 3.0 (continuación)

Implementa estos estándares de PCI DSS	Especificación de implementación	Implementación de AIX Security Expert	Ubicación del script que modifica el valor
PCI versión 2 8.5.12 **PCI versión 3** 8.2.5	No permitir que una persona envíe una contraseña nueva que sea igual que alguna de las cuatro últimas contraseñas que ha utilizado.	Establece en 4 el número de contraseñas anteriores que no se pueden volver a utilizar estableciendo el parámetro **histsize** en un valor de 4.	/etc/security/pscexpert/bin/chusrattr
PCI versión 2 8.5.13 **PCI versión 3** 8.1.6	Limitar los intentos de acceso repetidos bloqueando el ID de usuario después de no más de seis intentos.	Establece el número de intentos de inicio de sesión no satisfactorios consecutivos que inhabilita una cuenta en 6 intentos para cada cuenta no root estableciendo el parámetro **loginentries** en un valor de 6.	/etc/security/pscexpert/bin/chusrattr
PCI versión 2 8.5.13 **PCI versión 3** 8.1.6	Limitar los intentos de acceso repetidos bloqueando el ID de usuario después de no más de seis intentos.	Establece el número de intentos de inicio de sesión no satisfactorios consecutivos que inhabilita un puerto a 6 intentos estableciendo el parámetro **logindisable** en un valor de 6.	• /etc/security/pscexpert/bin/chdefstanza • /etc/security/login.cfg
PCI versión 2 8.5.14 **PCI versión 3** 8.1.7	Establecer la duración de bloqueo en un mínimo de 30 minutos o hasta que el administrador habilite el ID de usuario.	Establece en 30 minutos el periodo de tiempo que un puerto está bloqueado después de que el atributo *logindisable* lo haya inhabilitado estableciendo el parámetro **loginreenable** en un valor de 30.	• /etc/security/pscexpert/bin/chdefstanza • /etc/security/login.cfg
12.3.9	Activación de tecnologías de acceso remoto para proveedores y business partners sólo cuando éstos las necesiten, con la desactivación inmediata después de su uso.	Inhabilita la función de inicio de sesión como root remoto estableciendo el valor en false. El administrador del sistema puede activar la función de inicio de sesión remoto como sea necesario y, a continuación, desactivarlo cuando se complete la tarea.	• /etc/security/pscexpert/bin/chuserstanza • /etc/security/user
8.1.1	Asignar a todos los usuarios un ID exclusivo antes de permitirles acceder a los componentes del sistema o los datos del titular de la tarjeta.	Habilita la función que garantiza que todos los usuarios tengan un nombre de usuario exclusivo antes de poder acceder a los componentes de sistema o a los datos del titular de la tarjeta estableciendo dicha función de un valor de true.	• /etc/security/pscexpert/bin/chuserstanza • /etc/security/user
10.2	Habilitar la auditoría en el sistema.	Habilita la auditoría de los archivos binarios en el sistema.	/etc/security/pscexpert/bin/pciaudit
PCI versión 2 1.1.5 2.2.2 **PCI versión 3** 2.2.2	Inhabilitar servicios innecesarios y no seguros, que incluyen Common Desktop Environment (CDE).	Inhabilita la función CDE cuando no se ha configurado LFT (Layer Four Traceroute).	/etc/security/pscexpert/bin/comntrows

Tabla 6. Valores relacionados con los estándares de conformidad de PCI DSS versión 2.0 y versión 3.0 (continuación)

Implementa estos estándares de PCI DSS	Especificación de implementación	Implementación de AIX Security Expert	Ubicación del script que modifica el valor
PCI versión 2 1.1.5 2.2.2 **PCI versión 3** 2.2.2	Inhabilitar servicios innecesarios y no seguros, que incluyen el daemon `timed`.	Detiene el daemon `timed` y comenta la entrada correspondiente en el archivo `/etc/rc.tcpip` que inicia automáticamente el daemon.	`/etc/security/pscexpert/bin/rctcpip`
PCI versión 2 1.1.5 2.2.2 **PCI versión 3** 2.2.2	Inhabilitar servicios innecesarios y no seguros, que incluyen el daemon `rwhod`.	Detiene el daemon `rwhod` y comenta la entrada correspondiente en el archivo `/etc/rc.tcpip` que inicia automáticamente el daemon.	`/etc/security/pscexpert/bin/rctcpip`
PCI versión 2 2.1 **PCI versión 3** 2.1.1	Cambiar los valores predeterminados proporcionados por el proveedor antes de instalar un sistema en la red, lo que incluye inhabilitar el daemon `SNMP`.	Detiene el daemon `SNMP` y comenta la entrada correspondiente en el archivo `/etc/rc.tcpip` que inicia automáticamente el daemon.	`/etc/security/pscexpert/bin/rctcpip`
PCI versión 2 2.1 **PCI versión 3** 2.1.1	Cambiar los valores predeterminados proporcionados por el proveedor antes de instalar un sistema en la red, que incluye inhabilitar el daemon `SNMPMIBD`.	Inhabilita el daemon `SNMPMIBD` comentando la entrada correspondiente en el archivo `/etc/rc.tcpip` que inicia automáticamente el daemon.	`/etc/security/pscexpert/bin/rctcpip`
2.1	Cambiar los valores predeterminados proporcionados por el proveedor antes de instalar un sistema en la red, lo que incluye inhabilitar el daemon `AIXMIBD`.	Inhabilita el daemon `AIXMIBD` comentando la entrada correspondiente en el archivo `/etc/rc.tcpip` que inicia automáticamente el daemon.	`/etc/security/pscexpert/bin/rctcpip`
2.1	Cambiar los valores predeterminados proporcionados por el proveedor antes de instalar un sistema en la red, lo que incluye inhabilitar el daemon `HOSTMIBD`.	Inhabilita el daemon `HOSTMIBD` comentando la entrada correspondiente en el archivo `/etc/rc.tcpip` que inicia automáticamente el daemon.	`/etc/security/pscexpert/bin/rctcpip`
PCI versión 2 1.1.5 2.2.2 **PCI versión 3** 2.2.2	Inhabilitar servicios innecesarios y no seguros, que incluyen el daemon `DPID2`.	Detiene el daemon `DPID2` y comenta la entrada correspondiente en el archivo `/etc/rc.tcpip` que inicia automáticamente el daemon.	`/etc/security/pscexpert/bin/rctcpip`

Tabla 6. Valores relacionados con los estándares de conformidad de PCI DSS versión 2.0 y versión 3.0 (continuación)

Implementa estos estándares de PCI DSS	Especificación de implementación	Implementación de AIX Security Expert	Ubicación del script que modifica el valor
PCI versión 2 2.1 **PCI versión 3** 2.2.2	Cambiar los valores predeterminado proporcionados por el proveedor antes de instalar un sistema en la red, que incluye detener el servidor DHCP.	Inhabilita el servidor DHCP.	/etc/security/pscexpert/bin/rctcpip
PCI versión 2 1.1.5 2.2.2 **PCI versión 3** 2.2.2	Inhabilitar servicios innecesarios y no seguros, que incluyen el agente DHCP.	Detiene e inhabilita el agente de relé DHCP y comenta la entrada correspondiente en el archivo /etc/rc.tcpip que inicia automáticamente el agente.	/etc/security/pscexpert/bin/rctcpip
PCI versión 2 1.1.5 2.2.2 **PCI versión 3** 2.2.2	Inhabilitar servicios innecesarios y no seguros, que incluyen el daemon rshd.	Detiene e inhabilita todas las instancias del daemon rshd y el servicio de shell y comenta las entradas correspondientes en el archivo /etc/inetd.conf que inicia automáticamente las instancias.	/etc/security/pscexpert/bin/cominetdconf
PCI versión 2 1.1.5 2.2.2 **PCI versión 3** 2.2.2	Inhabilitar servicios innecesarios y no seguros, que incluyen el daemon rlogind.	Detiene e inhabilita todas las instancias del daemon rlogind y el servicio rlogin. El programa de utilidad AIX Security Expert también comenta las entradas correspondientes en el archivo /etc/inetd.conf que inician automáticamente las instancias.	/etc/security/pscexpert/bin/cominetdconf
PCI versión 2 1.1.5 2.2.2 **PCI versión 3** 2.2.2	Inhabilitar servicios innecesarios y no seguros, que incluyen el daemon rexecd.	Detiene e inhabilita todas las instancias del daemon rexecd. El programa de utilidad AIX Security Expert también comenta la entrada correspondiente en el archivo /etc/inetd.conf que inicia automáticamente el daemon.	/etc/security/pscexpert/bin/cominetdconf
PCI versión 2 1.1.5 2.2.2 **PCI versión 3** 2.2.2	Inhabilitar servicios innecesarios y no seguros, que incluyen el daemon comsat.	Detiene e inhabilita todas las instancias del daemon comsat. El programa de utilidad AIX Security Expert también comenta la entrada correspondiente en el archivo /etc/inetd.conf que inicia automáticamente el daemon.	/etc/security/pscexpert/bin/cominetdconf
PCI versión 2 1.1.5 2.2.2 **PCI versión 3** 2.2.2	Inhabilitar servicios innecesarios y no seguros, que incluyen el daemon fingerd.	Detiene e inhabilita todas las instancias del daemon fingerd. El programa de utilidad AIX Security Expert también comenta la entrada correspondiente en el archivo /etc/inetd.conf que inicia automáticamente el daemon.	/etc/security/pscexpert/bin/cominetdconf

Tabla 6. Valores relacionados con los estándares de conformidad de PCI DSS versión 2.0 y versión 3.0 (continuación)

Implementa estos estándares de PCI DSS	Especificación de implementación	Implementación de AIX Security Expert	Ubicación del script que modifica el valor
PCI versión 2 1.1.5 2.2.2 **PCI versión 3** 2.2.2	Inhabilitar servicios innecesarios y no seguros, que incluyen el daemon `systat`.	Detiene e inhabilita todas las instancias del daemon `systat`. El programa de utilidad AIX Security Expert también comenta la entrada correspondiente en el archivo `/etc/inetd.conf` que inicia automáticamente el daemon.	`/etc/security/pscexpert/bin/cominetdconf`
2.1	Cambiar los valores predeterminados proporcionados por el proveedor antes de instalar un sistema en la red, que incluye inhabilitar el mandato `netstat`.	Inhabilita el mandato `netstat` comentando la entrada correspondiente en el archivo `/etc/inetd.conf`.	`/etc/security/pscexpert/bin/cominetdconf`
PCI versión 2 1.1.5 2.2.2 **PCI versión 3** 2.2.3	Inhabilitar servicios innecesarios y no seguros, que incluyen el daemon `tftp`.	Detiene e inhabilita todas las instancias del daemon `tftp`. El programa de utilidad AIX Security Expert también comenta la entrada correspondiente en el archivo `/etc/inetd.conf` que inicia automáticamente el daemon.	`/etc/security/pscexpert/bin/cominetdconf`
PCI versión 2 1.1.5 2.2.2 **PCI versión 3** 2.2.2	Inhabilitar servicios innecesarios y no seguros, que incluyen el daemon `talkd`.	Detiene e inhabilita todas las instancias del daemon `talkd`. El programa de utilidad AIX Security Expert también comenta la entrada correspondiente en el archivo `/etc/inetd.conf` que inicia automáticamente el daemon.	`/etc/security/pscexpert/bin/cominetdconf`
PCI versión 2 1.1.5 2.2.2 **PCI versión 3** 2.2.2	Inhabilitar servicios innecesarios y no seguros, que incluyen el daemon `rquotad`.	Detiene e inhabilita todas las instancias del daemon `rquotad`. El programa de utilidad AIX Security Expert también comenta la entrada correspondiente en el archivo `/etc/inetd.conf` que inicia automáticamente el daemon.	`/etc/security/pscexpert/bin/cominetdconf`
PCI versión 2 1.1.5 2.2.2 **PCI versión 3** 2.2.2	Inhabilitar servicios innecesarios y no seguros, que incluyen el daemon `rstatd`.	Detiene e inhabilita todas las instancias del daemon `rstatd`. El programa de utilidad AIX Security Expert también comenta la entrada correspondiente en el archivo `/etc/inetd.conf` que inicia automáticamente el daemon.	`/etc/security/pscexpert/bin/cominetdconf`
PCI versión 2 1.1.5 2.2.2 **PCI versión 3** 2.2.2	Inhabilitar servicios innecesarios y no seguros, que incluyen el daemon `rusersd`.	Detiene e inhabilita todas las instancias del daemon `rusersd`. El programa de utilidad AIX Security Expert también comenta la entrada correspondiente en el archivo `/etc/inetd.conf` que inicia automáticamente el daemon.	`/etc/security/pscexpert/bin/cominetdconf`

Tabla 6. Valores relacionados con los estándares de conformidad de PCI DSS versión 2.0 y versión 3.0 (continuación)

Implementa estos estándares de PCI DSS	Especificación de implementación	Implementación de AIX Security Expert	Ubicación del script que modifica el valor
PCI versión 2 1.1.5 2.2.2 **PCI versión 3** 2.2.2	Inhabilitar servicios innecesarios y no seguros, que incluyen el daemon `rwalld`.	Detiene e inhabilita todas las instancias del daemon `rwalld`. El programa de utilidad AIX Security Expert también comenta la entrada correspondiente en el archivo `/etc/inetd.conf` que inicia automáticamente el daemon.	`/etc/security/pscexpert/bin/cominetdconf`
PCI versión 2 1.1.5 2.2.2 **PCI versión 3** 2.2.2	Inhabilitar servicios innecesarios y no seguros, que incluyen el daemon `sprayd`.	Detiene e inhabilita todas las instancias del daemon `sprayd`. El programa de utilidad AIX Security Expert también comenta la entrada correspondiente en el archivo `/etc/inetd.conf` que inicia automáticamente el daemon.	`/etc/security/pscexpert/bin/cominetdconf`
PCI versión 2 1.1.5 2.2.2 **PCI versión 3** 2.2.2	Inhabilitar servicios innecesarios y no seguros, que incluyen el daemon `pcnfsd`.	Detiene e inhabilita todas las instancias del daemon `pcnfsd`. El programa de utilidad AIX Security Expert también comenta la entrada correspondiente en el archivo `/etc/inetd.conf` que inicia automáticamente el daemon.	`/etc/security/pscexpert/bin/cominetdconf`
PCI versión 2 1.1.5 2.2.2 **PCI versión 3** 2.2.2	Inhabilitar servicios innecesarios y no seguros, que incluyen el servicio `TCP echo`.	Detiene e inhabilita todas las instancias del servicio `echo(tcp)`. El programa de utilidad AIX Security Expert también comenta la entrada correspondiente en el archivo `/etc/inetd.conf` que inicia automáticamente el servicio.	`/etc/security/pscexpert/bin/cominetdconf`
PCI versión 2 1.1.5 2.2.2 **PCI versión 3** 2.2.2	Inhabilitar servicios innecesarios y no seguros, que incluyen el servicio `TCP discard`.	Detiene e inhabilita todas las instancias del servicio `discard(tcp)`. El programa de utilidad AIX Security Expert también comenta la entrada correspondiente en el archivo `/etc/inetd.conf` que inicia automáticamente el servicio.	`/etc/security/pscexpert/bin/cominetdconf`
PCI versión 2 1.1.5 2.2.2 **PCI versión 3** 2.2.2	Inhabilitar servicios innecesarios y no seguros, que incluyen el servicio `TCP chargen`.	Detiene e inhabilita todas las instancias del servicio `chargen(tcp)`. El programa de utilidad AIX Security Expert también comenta la entrada correspondiente en el archivo `/etc/inetd.conf` que inicia automáticamente el servicio.	`/etc/security/pscexpert/bin/cominetdconf`
PCI versión 2 1.1.5 2.2.2 **PCI versión 3** 2.2.2	Inhabilitar servicios innecesarios y no seguros, que incluyen el servicio `TCP daytime`.	Detiene e inhabilita todas las instancias del servicio `daytime(tcp)`. El programa de utilidad AIX Security Expert también comenta la entrada correspondiente en el archivo `/etc/inetd.conf` que inicia automáticamente el servicio.	`/etc/security/pscexpert/bin/cominetdconf`

Tabla 6. Valores relacionados con los estándares de conformidad de PCI DSS versión 2.0 y versión 3.0 (continuación)

Implementa estos estándares de PCI DSS	Especificación de implementación	Implementación de AIX Security Expert	Ubicación del script que modifica el valor
PCI versión 2 1.1.5 2.2.2 **PCI versión 3** 2.2.2	Inhabilitar servicios innecesarios y no seguros, que incluyen el servicio `TCP time`.	Detiene e inhabilita todas las instancias del servicio `timed(tcp)`. El programa de utilidad AIX Security Expert también comenta la entrada correspondiente en el archivo `/etc/inetd.conf` que inicia automáticamente el servicio.	`/etc/security/pscexpert/bin/cominetdconf`
PCI versión 2 1.1.5 2.2.2 **PCI versión 3** 2.2.2	Inhabilitar servicios innecesarios y no seguros, que incluyen el servicio `UDP echo`.	Detiene e inhabilita todas las instancias del servicio `echo(udp)`. El programa de utilidad AIX Security Expert también comenta la entrada correspondiente en el archivo `/etc/inetd.conf` que inicia automáticamente el servicio.	`/etc/security/pscexpert/bin/cominetdconf`
PCI versión 2 1.1.5 2.2.2 **PCI versión 3** 2.2.2	Inhabilitar servicios innecesarios y no seguros, que incluyen el servicio `UDP discard`.	Detiene e inhabilita todas las instancias del servicio `discard(udp)`. El programa de utilidad AIX Security Expert también comenta la entrada correspondiente en el archivo `/etc/inetd.conf` que inicia automáticamente el servicio.	`/etc/security/pscexpert/bin/cominetdconf`
PCI versión 2 1.1.5 2.2.2 **PCI versión 3** 2.2.2	Inhabilitar servicios innecesarios y no seguros, que incluyen el servicio UDP `chargen`.	Detiene e inhabilita todas las instancias del servicio `chargen(udp)`. El programa de utilidad AIX Security Expert también comenta la entrada correspondiente en el archivo `/etc/inetd.conf` que inicia automáticamente el servicio.	`/etc/security/pscexpert/bin/cominetdconf`
PCI versión 2 1.1.5 2.2.2 **PCI versión 3** 2.2.2	Inhabilitar servicios innecesarios y no seguros, que incluyen el servicio `UDP daytime`.	Detiene e inhabilita todas las instancias del servicio `daytime(udp)`. El programa de utilidad AIX Security Expert también comenta la entrada correspondiente en el archivo `/etc/inetd.conf` que inicia automáticamente el servicio.	`/etc/security/pscexpert/bin/cominetdconf`
PCI versión 2 1.1.5 2.2.2 **PCI versión 3** 2.2.2	Inhabilitar servicios innecesarios y no seguros, que incluyen el servicio `UDP time`.	Detiene e inhabilita todas las instancias del servicio `timed(udp)`. El programa de utilidad AIX Security Expert también comenta la entrada correspondiente en el archivo `/etc/inetd.conf` que inicia automáticamente el servicio.	`/etc/security/pscexpert/bin/cominetdconf`
PCI versión 2 1.1.5 2.2.2 **PCI versión 3** 2.2.3	Inhabilitar servicios innecesarios y no seguros, que incluyen el servicio `FTP`.	Detiene e inhabilita todas las instancias del daemon `ftpd`. El programa de utilidad AIX Security Expert también comenta la entrada correspondiente en el archivo `/etc/inetd.conf` que inicia automáticamente el daemon.	`/etc/security/pscexpert/bin/cominetdconf`

Tabla 6. Valores relacionados con los estándares de conformidad de PCI DSS versión 2.0 y versión 3.0 (continuación)

Implementa estos estándares de PCI DSS	Especificación de implementación	Implementación de AIX Security Expert	Ubicación del script que modifica el valor
PCI versión 2 1.1.5 2.2.2 **PCI versión 3** 2.2.3	Inhabilitar servicios innecesarios y no seguros, que incluyen el servicio `telnet`.	Detiene e inhabilita todas las instancias del daemon `telnetd`. El programa de utilidad AIX Security Expert también comenta la entrada correspondiente en el archivo `/etc/inetd.conf` que inicia automáticamente el daemon.	`/etc/security/pscexpert/bin/cominetdconf`
PCI versión 2 1.1.5 2.2.2 **PCI versión 3** 2.2.2	Inhabilitar servicios innecesarios y no seguros, que incluyen `dtspc`.	Detiene e inhabilita todas las instancias del daemon `dtspc`. AIX Security Expert también comenta la entrada correspondiente en el archivo `/etc/inittab` que inicia automáticamente el daemon cuando LFT no está configurado y CDE está inhabilitado en el archivo `/etc/inittab`.	`/etc/security/pscexpert/bin/cominetdconf`
PCI versión 2 1.1.5 2.2.2 **PCI versión 3** 2.2.2	Inhabilitar servicios innecesarios y no seguros, que incluyen el servicio `ttdbserver`.	Detiene e inhabilita todas las instancias del servicio `ttdbserver`. El programa de utilidad AIX Security Expert también comenta la entrada correspondiente en el archivo `/etc/inetd.conf` que inicia automáticamente el servicio.	`/etc/security/pscexpert/bin/cominetdconf`
PCI versión 2 1.1.5 2.2.2 **PCI versión 3** 2.2.2	Inhabilitar servicios innecesarios y no seguros, que incluyen el servicio `cmsd`.	Detiene e inhabilita todas las instancias del servicio `cmsd`. El programa de utilidad AIX Security Expert también comenta la entrada correspondiente en el archivo `/etc/inetd.conf` que inicia automáticamente el servicio.	`/etc/security/pscexpert/bin/cominetdconf`
PCI versión 2 2.2.3 **PCI versión 3** 2.2.4	Configurar los parámetros de sistema de seguridad para impedir el uso incorrecto.	Elimina los mandatos de ID de usuario de conjunto (SUID) comentando la entrada correspondiente en el archivo `/etc/inetd.conf` que habilita automáticamente los mandatos.	`/etc/security/pscexpert/bin/rmsuidfrmrcmds`
PCI versión 2 2.2.3 **PCI versión 3** 2.2.4	Configurar los parámetros de sistema de seguridad para impedir el uso incorrecto.	Habilita el nivel de seguridad más bajo para el Gestor de permisos de archivo.	`/etc/security/pscexpert/bin/filepermgr`
PCI versión 2 2.2.3 **PCI versión 3** 2.2.4	Configurar los parámetros de sistema de seguridad para impedir el uso incorrecto.	Modifica el protocolo de sistema de archivos de red con valores restringidos que cumplen los requisitos de seguridad de PCI. Estos valores restringidos incluyen inhabilitar el acceso de root remoto y el acceso de UID y GID anónimo.	`/etc/security/pscexpert/bin/nfsconfig`

Tabla 6. Valores relacionados con los estándares de conformidad de PCI DSS versión 2.0 y versión 3.0 (continuación)

Implementa estos estándares de PCI DSS	Especificación de implementación	Implementación de AIX Security Expert	Ubicación del script que modifica el valor
PCI versión 2 2.2.2 **PCI versión 3** 2.2.3	Habilitar sólo servicios, protocolos, daemons, etc. necesarios y seguros, según sea necesario para el funcionamiento correcto del sistema. Implemente características de seguridad para los servicios, protocolos o daemons necesarios que se consideren inseguros.	Inhabilita los daemons `rlogind`, `rshd` y `tftpd`, que no son seguros.	`/etc/security/pscexpert/bin/disrmtdmns`
PCI versión 2 2.2.2 **PCI versión 3** 2.2.3	Habilitar sólo servicios, protocolos, daemons, etc. necesarios y seguros, según sea necesario para el funcionamiento correcto del sistema. Implemente características de seguridad para los servicios, protocolos o daemons necesarios que se consideren inseguros.	Inhabilita los daemons `rlogind`, `rshd` y `tftpd`, que no son seguros.	`/etc/security/pscexpert/bin/rmrhostsnetrc`
PCI versión 2 2.2.2 **PCI versión 3** 2.2.3	Habilitar sólo servicios, protocolos, daemons, etc. necesarios y seguros, según sea necesario para el funcionamiento correcto del sistema. Implemente características de seguridad para los servicios, protocolos o daemons necesarios que se consideren inseguros.	Inhabilita los daemons `logind`, `rshd` y `tftpdpci_rmetchostsequiv`, que no son seguros.	`/etc/security/pscexpert/bin/rmetchostsequiv`
PCI versión 2 1.3.6 **PCI versión 3** 2.2.3	Implementar inspección con estado o filtro de paquete, en el que sólo se permiten conexiones establecidas en la red.	Habilita la opción **`clean_partial_conns`** de red estableciendo el valor en 1.	`/etc/security/pscexpert/bin/ntwkopts`
PCI versión 2 2.2.2 **PCI versión 3** 2.2.3	Implementar inspección con estado o filtro de paquete, en el que sólo se permiten conexiones establecidas en la red.	Habilita la seguridad de TCP estableciendo la opción **`tcp_tcpsecure`** de red en un valor de 7. Este valor proporciona protección contra los ataques a datos, restablecimiento (RST) y solicitud de conexión TCP (SYN).	`/etc/security/pscexpert/bin/ntwkopts`

Tabla 6. Valores relacionados con los estándares de conformidad de PCI DSS versión 2.0 y versión 3.0 (continuación)

Implementa estos estándares de PCI DSS	Especificación de implementación	Implementación de AIX Security Expert	Ubicación del script que modifica el valor
1.2	Proteger el acceso no autorizado a puertos no utilizados.	Configura el sistema para rechazar los hosts durante 5 minutos para evitar que otros sistemas accedan a puertos no utilizados.	`/etc/security/pscexpert/bin/ipsecshunhosthls` **Nota:** Puede especificar reglas de filtro adicionales en el archivo `/etc/security/aixpert/bin/filter.txt`. Estas reglas las integra el script `ipsecshunhosthls.sh` cuando se aplica el perfil. Las entradas deben estar en el formato siguiente: *`número_puerto`*`:`*`dirección_IP`*`:` *`acción`* donde los valores posibles para *acción* son `Allow` o `Deny`.
1.2	Proteger el host frente a las exploraciones de puertos.	Configura el sistema para que rechace los puertos vulnerables durante 5 minutos, lo que impide las exploraciones de puerto.	`/etc/security/pscexpert/bin/ipsecshunports` **Nota:** Puede especificar reglas de filtro adicionales en el archivo `/etc/security/aixpert/bin/filter.txt`. Estas reglas las integra el script `ipsecshunhosthls.sh` cuando se aplica el perfil. Las entradas deben estar en el formato siguiente: *`número_puerto`*`:`*`dirección_IP`*`:` *`acción`* donde los valores posibles para *acción* son `Allow` o `Deny`.
7.1.1	Limitar permisos de creación de objetos.	Establece los permisos de creación de objetos predeterminados en 22 estableciendo el parámetro **`umask`** en un valor de 22.	`/etc/security/pscexpert/bin/chusrattr`
7.1.1	Limitar el acceso al sistema.	Asegura que el ID de root sea el único que se lista en el archivo `cron.allow` y elimina el archivo `cron.deny` del sistema.	`/etc/security/pscexpert/bin/limitsysacc`
6.5.8	Eliminar punto de la vía de acceso root.	Elimina los puntos de la variable de entorno PATH en los archivos siguientes que se encuentran en el directorio de inicio de root: • .cshrc • .kshrc • .login • .profile	`/etc/security/pscexpert/bin/rmdotfrmpathroot`
6.5.8	Eliminar punto de la vía de acceso no root:	Elimina los puntos de la variable de entorno *PATH* en los archivos siguientes que están en el directorio de inicio de usuario: • .cshrc • .kshrc • .login • .profile	`/etc/security/pscexpert/bin/rmdotfrmpathnroot`

Tabla 6. Valores relacionados con los estándares de conformidad de PCI DSS versión 2.0 y versión 3.0 (continuación)

Implementa estos estándares de PCI DSS	Especificación de implementación	Implementación de AIX Security Expert	Ubicación del script que modifica el valor
2.2.3	Limitar el acceso al sistema.	Añade la capacidad de usuario root y el nombre de usuario en el archivo `/etc/ftpusers`.	`/etc/security/pscexpert/bin/chetcftpusers`
2.1	Elimine la cuenta de invitado.	Elimina la cuenta de invitado y sus archivos.	`/etc/security/pscexpert/bin/execmds`
6.5.2	Impedir el inicio de programas en el espacio de contenido.	Habilita la característica de inhabilitación de ejecución de pila (SED).	`/etc/security/pscexpert/bin/sedconfig`
8.2	Asegúrese de que la contraseña de root no es débil.	Inicia una comprobación de integridad de contraseña de root con la contraseña de root, garantizando de este modo una contraseña de root fuerte.	`/etc/security/pscexpert/bin/chuserstanza`
PCI versión 2 8.5.15 **PCI versión 3** 8.1.8	Limitar el acceso al sistema estableciendo el tiempo de inactividad de sesión.	Establece el límite de tiempo de inactividad en 15 minutos. Si la sesión está desocupada durante más de 15 minutos, debe entrar de nuevo la contraseña.	`/etc/security/pscexpert/bin/autologoff`
1.3.5	Limitar el acceso de tráfico a la información del titular de la tarjeta.	Establece la regulación de tráfico de TCP en el valor alto, que aplica la mitigación de denegación de servicio en los puertos.	`/etc/security/pscexpert/bin/tcptr_pscexpert`
1.3.5	Mantener una conexión segura al migrar datos.	Habilita la creación de túnel de seguridad IP (IPSec) automatizada entre Virtual I/O Servers durante la migración de partición activa.	`/etc/security/pscexpert/bin/cfgsecmig`
1.3.5	Limitar los paquetes de orígenes desconocidos.	Permite los paquetes de la consola de gestión de hardware.	`/etc/security/pscexpert/bin/ipsecpermithostorport`
5.1.1	Mantener el software antivirus.	Mantiene la integridad del sistema mediante la detección, eliminación y protección frente a tipos conocidos de software malicioso.	`/etc/security/pscexpert/bin/manageITsecurity`
PCI versión 2 Sección 7 **PCI versión 3** Sección 7	Mantener el acceso según las necesidades.	Habilitar el control de acceso basado en roles (RBAC) creando roles de usuario de operador de sistema, administrador de sistema y responsable de seguridad de sistema de información con los permisos necesarios.	`/etc/security/pscexpert/bin/EnableRbac`

Tabla 6. Valores relacionados con los estándares de conformidad de PCI DSS versión 2.0 y versión 3.0 (continuación)

Implementa estos estándares de PCI DSS	Especificación de implementación	Implementación de AIX Security Expert	Ubicación del script que modifica el valor
PCI versión 2 No incluido en el perfil de la versión 2, añadido en la versión 3. **PCI versión 3** 2.3	Implementar más características de seguridad para los servicios, protocolos o daemons necesarios que se consideran no seguros.	Utiliza tecnologías seguras como SSH (Secure Shell), S-FTP (SSH File Transfer Protocol - Protocolo de transferencia de archivos SSH), SSL (Secure Sockets Layer - Capa de sockets seguros) o IPsec VPN (Internet Protocol Security Virtual Private Network - Red privada virtual de seguridad de protocolo de Internet) para proteger los servicios no seguros como NetBIOS, compartición de archivos, Telnet y FTP. También configura el daemon SSH para utilizar sólo el protocolo SSHv2.	`/etc/security/pscexpert/bin/sshPCIconfig`
PCI versión 2 No incluido en el perfil de la versión 2, añadido en la versión 3. **PCI versión 3** 2.3	El cliente SSH debe configurarse para utilizar sólo el protocolo SSHv2.	Configura el cliente SSH para utilizar el protocolo SSHv2.	`/etc/security/pscexpert/bin/sshPCIconfig`
PCI versión 2 No incluido en el perfil de la versión 2, añadido en la versión 3. **PCI versión 3** 2.3	El daemon SSH solo debe escuchar direcciones de red de gestión a menos que esté autorizado para usos distintos de la gestión.	Asegura que el daemon SSH esté configurado sólo para escuchar.	`/etc/security/pscexpert/bin/sshPCIconfig`
PCI versión 2 No incluido en el perfil de la versión 2, añadido en la versión 3. **PCI versión 3** 2.3	El daemon SSH debe configurarse para utilizar sólo cifrados aprobados FIPS 140-2	Asegura que el daemon SSH utilice sólo los cifrados FIPS 140-2.	`/etc/security/pscexpert/bin/sshPCIconfig`
PCI versión 2 No incluido en el perfil de la versión 2, añadido en la versión 3. **PCI versión 3** 2.3	El daemon SSH debe configurarse para utilizar sólo códigos de autenticación de mensajes (MAC) que emplean algoritmos hash criptográficos aprobados de FIPS 140-2.	Asegura que los MAC estén ejecutando los algoritmos aprobados.	`/etc/security/pscexpert/bin/sshPCIconfig`

Tabla 6. Valores relacionados con los estándares de conformidad de PCI DSS versión 2.0 y versión 3.0 (continuación)

Implementa estos estándares de PCI DSS	Especificación de implementación	Implementación de AIX Security Expert	Ubicación del script que modifica el valor
PCI versión 2 No incluido en el perfil de la versión 2, añadido en la versión 3. **PCI versión 3** 2.3	El daemon SSH debe restringir la posibilidad de inicio de sesión a usuarios o grupos específicos.	Restringe el inicio de sesión en el sistema a usuarios y grupos específicos.	`/etc/security/pscexpert/bin/sshPCIconfig`
PCI versión 2 No incluido en el perfil de la versión 2, añadido en la versión 3. **PCI versión 3** 2.3	El sistema debe mostrar la fecha y hora del último inicio de sesión de cuenta satisfactorio al iniciar la sesión.	Mantiene la información del último inicio de sesión satisfactorio y la visualiza después del siguiente inicio de sesión satisfactorio.	`/etc/security/pscexpert/bin/sshPCIconfig`
PCI versión 2 No incluido en el perfil de la versión 2, añadido en la versión 3. **PCI versión 3** 2.3	El daemon SSH debe realizar la comprobación de modalidad estricta de los archivos de configuración del directorio de inicio.	Asegura que los archivos de configuración de directorio de inicio se establezcan en las modalidades correctas.	`/etc/security/pscexpert/bin/sshPCIconfig`
PCI versión 2 No incluido en el perfil de la versión 2, añadido en la versión 3. **PCI versión 3** 2.3	El daemon SSH debe utilizar la separación de privilegios.	Asegura que el daemon SSH tenga la cantidad correcta de separación de sus privilegios.	`/etc/security/pscexpert/bin/sshPCIconfig`
PCI versión 2 No incluido en el perfil de la versión 2, añadido en la versión 3. **PCI versión 3** 2.3	El daemon SSH no debe permitir que los rhosts tengan autenticación RSA.	Inhabilita la autenticación RSA para los rhosts cuando se utiliza el daemon SSH.	`/etc/security/pscexpert/bin/sshPCIconfig`
PCI versión 2 1.1.5 2.2.2 **PCI versión 3** 10.4	Examine los estándares y procesos de configuración para verificar que la tecnología de sincronización de tiempo se implementa y mantiene actual según los requisitos de PCI DSS 6.1 y 6.2.	Habilita el daemon ntp.	`/etc/security/pscexpert/bin/rctcpip`

Tabla 6. Valores relacionados con los estándares de conformidad de PCI DSS versión 2.0 y versión 3.0 (continuación)

Implementa estos estándares de PCI DSS	Especificación de implementación	Implementación de AIX Security Expert	Ubicación del script que modifica el valor
PCI versión 2 No incluido en el perfil de la versión 2, añadido en la versión 3. **PCI versión 3** 8.1.5	Inhabilitar una cuenta de usuario cuando no se está utilizando.	Inhabilita las cuentas de usuario después de 35 días de inactividad.	`/etc/security/pscexpert/bin/disableacctpci`
PCI versión 3 2.2.3	Inhabilitar Secure Sockets Layer (SSL) v3 y Transport Layer Security (TLS) v1.0 en las aplicaciones.	Inhabilite las versiones SSLv3 y TLS v1.0 en la configuración de servidor Courier POP3 (Pop3d).	`/etc/security/pscexpert/bin/disableSSL`
PCI versión 3 2.2.3	Inhabilitar SSL v3 y TLS v1.0 en las aplicaciones.	Inhabilite SSLV3 y TLS v1.0 en el servidor Courier IMAP (imapd).	`/etc/security/pscexpert/bin/disableSSL`
PCI versión 3 8.2.1	Inhabilitar SSL v3 y TLS v1.0 en las aplicaciones.	Compruebe el archivo de configuración de NTP (Network Time Protocol - Protocolo de hora en red) para TLS 1.1 o la adopción de seguridad posterior.	`/etc/security/pscexpert/bin/checkNTP`
PCI versión 3 2.2.3	Inhabilitar SSL v3 y TLS v1.0 en las aplicaciones.	Compruebe el archivo de configuración de FTPD (File Transfer Protocol Daemon - Daemon de protocolo de transferencia de archivos) para TLS 1.1 o la adopción de seguridad posterior.	`/etc/security/pscexpert/bin/secureFTP`
PCI versión 3 2.2.3	Inhabilitar SSL v3 y TLS v1.0 en las aplicaciones.	Compruebe el archivo de configuración de FTP (File Transfer Protocol - Protocolo de transferencia de archivos) para TLS 1.1 o la adopción de seguridad posterior.	`/etc/security/pscexpert/bin/secureFTP`
PCI versión 3 2.2.3	Inhabilitar SSL v3 y TLS v1.0 en las aplicaciones.	Inhabilitar SSLv3 y TLS v1.0 en la configuración de sendmail.	`/etc/security/pscexpert/bin/sendmailPCIConfig`
PCI versión 3 2.2.3	Inhabilitar SSL v3 y TLS v1.0 en las aplicaciones.	Compruebe si la versión de SSL en AIX es posterior a 1.0.2.	`/etc/security/pscexpert/bin/sslversion`
PCI versión 3 8.2.1	Aplicar la autenticación de dos factores.	Aplicar la autenticación de dos factores como SHA-256 o SHA-512.	`/etc/security/pscexpert/bin/pwdalgchk`

Información relacionada:

Conformidad con Payment Card Industry - Data Security Standard

Conformidad con la ley Sarbanes-Oxley y COBIT

La ley Sarbanes-Oxley (SOX) de 2002 que se basa en el 107º congreso de los Estados Unidos de América supervisa la auditoría de las empresas públicas que están sujetas a las leyes de valores y asuntos relacionados, con el fin de proteger los intereses de los inversores.

La sección 404 de SOX requiere la evaluación de gestión en los controles internos. Para la mayoría de las organizaciones, los controles internos abarcan los sistemas de tecnología de la información, que procesan e informan de los datos financieros de la empresa. La Ley SOX proporciona detalles específicos sobre TI y la seguridad de TI. Muchos auditores de SOX dependen de los estándares, como por ejemplo COBIT, como un método para evaluar y auditar el gobierno y control de TI adecuados. La opción de configuración XML de SOX/COBIT de PowerSC Standard Edition proporciona la configuración de seguridad de los sistemas AIX y Virtual I/O Server (VIOS que se necesita para cumplir con las directrices de conformidad de COBIT.

IBM Compliance Expert Express Edition se ejecuta en la siguiente versión del sistema operativo AIX:

- AIX 6.1
- AIX 7.1
- AIX 7.2

La conformidad con los estándares externos es una responsabilidad de la carga de trabajo del administrador de sistema AIX. IBM Compliance Expert Express Edition se ha diseñado para simplificar la gestión de los valores de sistema operativo y los informes que son necesarios para la conformidad de estándares.

Los perfiles de conformidad preconfigurados que se entregan con IBM Compliance Expert Express Edition reduce la carga de trabajo administrativa de interpretar la documentación de conformidad y de implementar esos estándares como parámetros de configuración de sistema específicos.

Las capacidades de IBM Compliance Expert Express Edition están diseñadas para ayudar a los clientes a gestionar eficazmente los requisitos del sistema, que están asociados con la conformidad de estándares externos que puede reducir potencialmente los costes al mismo tiempo que mejora la conformidad. Todos los estándares de seguridad externos incluyen aspectos distintos de los valores de configuración de sistema. El uso de IBM Compliance Expert Express Edition no puede asegurar la conformidad de estándares. Compliance Expert está diseñado para simplificar la gestión del valor de configuración de sistemas que ayuda a los administradores a centrarse en otros aspectos de la conformidad de los estándares.

Información relacionada:

Conformidad con COBIT

Health Insurance Portability and Accountability Act (HIPAA)

Health Insurance Portability and Accountability Act (HIPAA) es un perfil de seguridad que se centra en la protección de Información sanitaria protegida electrónicamente (Electronically Protected Health Information - EPHI).

La regla de seguridad de HIPAA se centra específicamente en la protección de EPHI y sólo un subconjunto de los organismos están sujetos a la regla de seguridad de HIPAA basándose en las funciones y el uso de EPHI.

Todas las entidades cubiertas por HIPAA, similares a algunos de los organismos federales, deben cumplir con la regla de seguridad de HIPAA.

La regla de seguridad de HIPAA se centra en la protección de la confidencialidad, integridad y disponibilidad de EPHI, tal como se define en la regla de seguridad.

La EPHI que una entidad cubierta crea, recibe, mantiene o transmite se debe proteger de las amenazas anticipadas, los riesgos y los usos y declaraciones inadmisibles.

Los requisitos, las normas y las especificaciones de implementación de la regla de seguridad de HIPAA se aplican a las siguientes entidades cubiertas:

- Proveedores de asistencia médica
- Seguros médicos
- Clearinghouses de asistencia médica
- Recetas de seguro médico para personas mayores y patrocinadores de tarjetas de fármacos

La tabla siguiente detalla la diversas secciones de la regla de seguridad de HIPAA y cada sección incluye varios estándares y especificaciones de implementación.

Nota: Todos los archivos de script personalizados que se proporcionan para mantener la conformidad de HIPAA están en el directorio `/etc/security/pscexpert/bin`.

Tabla 7. Reglas de HIPAA y detalles de implementación

Secciones de regla de seguridad de HIPAA	Especificación de implementación	Implementación de aixpert	Mandatos y valores de retorno
164.308 (a) (1) (ii) (D) 164.308 (a) (5) (ii) (C) 164.312 (b)	Implementa los procedimientos para revisar regularmente los registros de la actividad del sistema de información, como registros de auditoría, informes de acceso e informes de incidencias de seguridad.	Determina si la auditoría está habilitada en el sistema.	**Mandato**: **#audit query**. **Valor de retorno**: Si se ejecuta de forma satisfactoria, este mandato sale con un valor de 0. Si no es satisfactorio, el mandato sale con un valor de 1.
164.308 (a) (1) (ii) (D) 164.308 (a) (5) (ii) (C) 166.312 (b)	Implementa los procedimientos para revisar regularmente los registros de la actividad del sistema de información, como registros de auditoría, informes de acceso e informes de incidencias de seguridad.	Habilita la auditoría en el sistema. Además, configura los sucesos que se deben capturar.	**Mandato**: **# audit start >/dev/null 2>&1**. **Valor de retorno**: Si se ejecuta de forma satisfactoria, este mandato sale con un valor de 0. Si no es satisfactorio, el mandato sale con un valor de 1. Se auditan los siguientes sucesos: **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)	Cifrado y descifrado (A):Implementa un mecanismo para cifrar y descifrar la EPHI.	Determina si el sistema de archivos cifrado (EFS) está habilitado en el sistema.	**Mandato**: **# efskeymgr -V >/dev/null 2>&1**. **Valor de retorno**: Si EFS ya está habilitado, este mandato sale con un valor de 0. Si EFS no está habilitado, este mandato sale con un valor de 1.

Tabla 7. Reglas de HIPAA y detalles de implementación (continuación)

Secciones de regla de seguridad de HIPAA	Especificación de implementación	Implementación de aixpert	Mandatos y valores de retorno
164.312 (a) (2) (iii)	Cierre de sesión automático (A): Implementa los procedimientos electrónicos para finalizar una sesión electrónica después de un intervalo predefinido de inactividad.	Configura el sistema para cerrar la sesión de procesos interactivos tras 15 minutos de inactividad.	**Mandato**: **grep TMOUT= /etc/security /.profile > /dev/null 2>&1** **echo "TMOUT=900 ; TIMEOUT=900; export TMOUT TIMEOUT**. **Valor de retorno**: Si el mandato no puede encontrar el valor **TMOUT=15**, el script sale con un valor de 1. De lo contrario, el mandato sale con un valor de 0.
164.308 (a) (5) (ii) (D) 164.312 (a) (2) (i)	Gestión de contraseñas (A):Implementa los procedimientos para crear, cambiar y proteger contraseñas.	Asegura que todas las contraseñas contengan un mínimo de 14 caracteres.	**Mandato**: **chsec -f /etc/security/user -s user -a minlen=8**. **Valor de retorno**: Si se ejecuta de forma satisfactoria, este script sale con un valor de 0. Si no es satisfactorio, el script sale con un código de error de 1.
164.308 (a) (5) (ii) (D) 164.312 (a) (2) (i)	Gestión de contraseñas (A):Implementa los procedimientos para crear, cambiar y proteger contraseñas.	Asegura que todas las contraseñas incluyan al menos dos caracteres alfabéticos, uno de los cuales debe estar en mayúsculas.	**Mandato**: **chsec -f /etc/security/user -s user –a minalpha=4**. **Valor de retorno**: Si se ejecuta de forma satisfactoria, este script sale con un valor de 0. Si no es satisfactorio, el mandato sale con un código de error de 1.
164.308 (a) (5) (ii) (D) 164.312 (a) (2) (i)	Gestión de contraseñas (A):Implementa los procedimientos para crear, cambiar y proteger contraseñas.	Especifica que el número mínimo de caracteres no alfabéticos de una contraseña sea 2.	**Mandato**: **#chsec –f /etc/security/user –s user –a minother=2**. **Valor de retorno**: Si se ejecuta de forma satisfactoria, este script sale con un valor de 0. Si no es satisfactorio, el mandato sale con un código de error de 1.
164.308 (a) (5) (ii) (D) 164.312 (a) (2) (i)	Gestión de contraseñas (A):Implementa los procedimientos para crear, cambiar y proteger contraseñas.	Asegúrese de que ninguna de las contraseñas contiene caracteres repetitivos.	**Mandato**: **#chsec –f /etc/security/user –s user –a maxrepeats=1**. **Valor de retorno**: Si se ejecuta de forma satisfactoria, este script sale con un valor de 0. Si no es satisfactorio, el mandato sale con un código de error de 1.
164.308 (a) (5) (ii) (D) 164.312 (a) (2) (i)	Gestión de contraseñas (A):Implementa los procedimientos para crear, cambiar y proteger contraseñas.	Asegúrese de que la contraseña no se reutiliza en los últimos cinco cambios.	**Mandato**: **#chsec –f /etc/security/user –s user –a histsize=5**. **Valor de retorno**: Si se ejecuta de forma satisfactoria, este script sale con un valor de 0. Si no es satisfactorio, el mandato sale con un código de error de 1.

Tabla 7. Reglas de HIPAA y detalles de implementación (continuación)

Secciones de regla de seguridad de HIPAA	Especificación de implementación	Implementación de aixpert	Mandatos y valores de retorno
164.308 (a) (5) (ii) (D) 164.312 (a) (2) (i)	Gestión de contraseñas (A):Implementa los procedimientos para crear, cambiar y proteger contraseñas.	Especifica el número máximo de semanas en 13 semanas, para que la contraseña siga siendo válida.	**Mandato**: **#chsec –f /etc/security/user –s user –a maxage=8**. **Valor de retorno**: Si se ejecuta de forma satisfactoria, este script sale con un valor de 0. Si no es satisfactorio, el mandato sale con un código de error de 1.
164.308 (a) (5) (ii) (D) 164.312 (a) (2) (i)	Gestión de contraseñas (A):Implementa los procedimientos para crear, cambiar y proteger contraseñas.	Elimina cualquier número mínimo de requisitos de semana antes de que se pueda cambiar una contraseña.	**Mandato**: **#chsec –f /etc/security/user –s user –a minage=2**. **Valor de retorno**: Si se ejecuta de forma satisfactoria, este script sale con un valor de 0. Si no es satisfactorio, el mandato sale con un código de error de 1.
164.308 (a) (5) (ii) (D) 164.312 (a) (2) (i)	Gestión de contraseñas (A):Implementa los procedimientos para crear, cambiar y proteger contraseñas.	Especifica el número máximo de semanas en 4 semanas, para cambiar una contraseña caducada, después de que caduque el valor del parámetro **maxage** establecido por el usuario.	**Mandato**: **#chsec –f /etc/security/user –s user –a maxexpired=4**. **Valor de retorno**: Si se ejecuta de forma satisfactoria, este script sale con un valor de 0. Si no es satisfactorio, el mandato sale con un código de error de 1.
164.308 (a) (5) (ii) (D) 164.312 (a) (2) (i)	Gestión de contraseñas (A):Implementa los procedimientos para crear, cambiar y proteger contraseñas.	Especifica que el número mínimo de caracteres que no se pueden repetir de la contraseña antigua es de 4 caracteres.	**Mandato**: **#chsec –f /etc/security/user –s user –a mindiff=4**. **Valor de retorno**: Si se ejecuta de forma satisfactoria, este script sale con un valor de 0. Si no es satisfactorio, el mandato sale con un código de error de 1.
164.308 (a) (5) (ii) (D) 164.312 (a) (2) (i)	Gestión de contraseñas (A):Implementa los procedimientos para crear, cambiar y proteger contraseñas.	Especifica que el número de días a esperar antes de que el sistema emita un aviso de que se necesita un cambio de contraseña es 5.	**Mandato**: **#chsec –f /etc/security/user –s user –a pwdwarntime = 5**. **Valor de retorno**: Si se ejecuta de forma satisfactoria, este script sale con un valor de 0. Si no es satisfactorio, el mandato sale con un código de error de 1.
164.308 (a) (5) (ii) (D) 164.312 (a) (2) (i)	Gestión de contraseñas (A):Implementa los procedimientos para crear, cambiar y proteger contraseñas.	Verifica si las definiciones de usuario son correctas y arregla los errores.	**Mandato**: **/usr/bin/usrck -y ALL** **/usr/bin/usrck –n ALL**. **Valor de retorno**: El mandato no devuelve un valor. El mandato comprueba y arregla los errores, si hay alguno.

Tabla 7. Reglas de HIPAA y detalles de implementación (continuación)

Secciones de regla de seguridad de HIPAA	Especificación de implementación	Implementación de aixpert	Mandatos y valores de retorno
164.308 (a) (5) (ii) (D) 164.312 (a) (2) (i)	Gestión de contraseñas (A):Implementa los procedimientos para crear, cambiar y proteger contraseñas.	Bloquea la cuenta después de tres intentos de inicio de sesión fallidos consecutivos.	**Mandato**: **#chsec –f /etc/security/user –s user –a loginretries=3**. **Valor de retorno**: Si se ejecuta de forma satisfactoria, este script sale con un valor de 0. Si no es satisfactorio, el mandato sale con un código de error de 1.
164.308 (a) (5) (ii) (D) 164.312 (a) (2) (i)	Gestión de contraseñas (A):Implementa los procedimientos para crear, cambiar y proteger contraseñas.	Especifica el retardo entre un inicio de sesión no satisfactorio y el otro como 5 segundos.	**Mandato**: **chsec -f /etc/security/login.cfg -s default -a logindelay=5**. **Valor de retorno**: Si se ejecuta de forma satisfactoria, este script sale con un valor de 0. Si no es satisfactorio, el mandato sale con un código de error de 1.
164.308 (a) (5) (ii) (D) 164.312 (a) (2) (i)	Gestión de contraseñas (A):Implementa los procedimientos para crear, cambiar y proteger contraseñas.	Establece en 10 el número de intentos de inicio de sesión no satisfactorios en un puerto, antes de que se bloquee el puerto.	**Mandato**: **chsec -f /etc/security/lastlog -s username -a \ unsuccessful_login_count=10**. **Valor de retorno**: Si se ejecuta de forma satisfactoria, este script sale con un valor de 0. Si no es satisfactorio, el mandato sale con un código de error de 1.
164.308 (a) (5) (ii) (D) 164.312 (a) (2) (i)	Gestión de contraseñas (A):Implementa los procedimientos para crear, cambiar y proteger contraseñas.	Establece en 60 segundos el intervalo de tiempo en un puerto para los intentos de inicio de sesión no satisfactorios antes de que se inhabilite el puerto.	**Mandato**: **#chsec -f /etc/security/lastlog -s user –a time_last_unsuccessful_ login=60**. **Valor de retorno**: Si se ejecuta de forma satisfactoria, este script sale con un valor de 0. Si no es satisfactorio, el mandato sale con un código de error de 1.
164.308 (a) (5) (ii) (D) 164.312 (a) (2) (i)	Gestión de contraseñas (A):Implementa los procedimientos para crear, cambiar y proteger contraseñas.	Establece en 30 minutos el intervalo de tiempo tras el cual se desbloquea un puerto y después de inhabilitarlo.	**Mandato**: **#chsec -f /etc/security/login.cfg -s default -a loginreenable = 30**. **Valor de retorno**: Si se ejecuta de forma satisfactoria, este script sale con un valor de 0. Si no es satisfactorio, el mandato sale con un código de error de 1.
164.308 (a) (5) (ii) (D) 164.312 (a) (2) (i)	Gestión de contraseñas (A):Implementa los procedimientos para crear, cambiar y proteger contraseñas.	Establece el intervalo de tiempo para escribir una contraseña en 30 segundos.	**Mandato**: **chsec -f /etc/security/login.cfg -s usw -a logintimeout=30**. **Valor de retorno**: Si se ejecuta de forma satisfactoria, este script sale con un valor de 0. Si no es satisfactorio, el mandato sale con un código de error de 1.

Tabla 7. Reglas de HIPAA y detalles de implementación (continuación)

Secciones de regla de seguridad de HIPAA	Especificación de implementación	Implementación de aixpert	Mandatos y valores de retorno
164.308 (a) (5) (ii) (D) 164.312 (a) (2) (i)	Gestión de contraseñas (A):Implementa los procedimientos para crear, cambiar y proteger contraseñas.	Asegúrese de que las cuentas están bloqueadas tras 35 días de inactividad.	**Mandato**: **grep TMOUT= /etc/security /.profile > /dev/null 2>&1if TMOUT = (35x24x60x60){#chsec -f /etc/security/user -s user -aaccount_locked = true}**. **Valor de retorno**: Si el mandato no puede establecer el valor de **account_locked** en **true**, el script sale con un valor de 1. De lo contrario, el mandato sale con un valor de 0.
164.312 (c) (1)	Implementa las políticas y los procedimientos para proteger la EPHI de la alteración incorrecta o la destrucción.	Establezca las políticas de Trusted Execution (TE) en activadas (ON).	**Mandato**: Activa **CHKEXEC, CHKSHLIB, CHKSCRIPT, CHKKERNEXT, STOP_ON_CHKFAIL,TE=ON Por ejemplo, trustchk –p TE=ON CHKEXEC = ON, CHKSHLIB,=ON, CHKSCRIPT=ON, CHKKERNEXT = ON**. **Valor de retorno**: Si se produce una anomalía, el script sale con un valor de 1.
164.312 (e) (1)	Implementa las medidas de seguridad técnicas para impedir el acceso no autorizado a la EPHI que se transmite a través de una red de comunicación electrónica.	Determina si los conjuntos de archivos **ssh** están instalados. En caso negativo, visualiza un mensaje de error.	**Mandato**: **# lslpp –l | grep openssh > /dev/null 2>&1**. **Valor de retorno**: Si el código de retorno para este mandato es 0, el script sale con un valor de 0. Si los conjuntos de archivos ssh no están instalados, el script sale con un valor de 1 y muestra el mensaje de error `Instalar conjuntos de archivos ssh para la transmisión segura`.

La tabla siguiente detalla las diversas funciones de la regla de seguridad de HIPAA y cada función incluye varios estándares y especificaciones de implementación.

Tabla 8. Funciones de HIPAA y detalles de implementación

Funciones de HIPAA	Especificación de implementación	Implementación de aixpert	Mandatos y valores de retorno
Registro de errores	Consolida los errores de diferentes registros y envía correos electrónicos el administrador.	Determina si existen errores de hardware. Determina si existen errores irrecuperables del archivo **trcfile** en la ubicación, `/var/adm/ras/trcfile`. Envía los errores a **root@<nombre_host>**.	**Mandato**: **errpt -d H**. **Valor de retorno**: Si se ejecuta de forma satisfactoria, este mandato sale con un valor de 0. Si no es satisfactorio, el mandato sale con un valor de 1.
Habilitación de FPM	Cambia los permisos de archivo.	Cambia el permiso de archivos de una lista de permisos y archivos utilizando el mandato **fpm**.	**Mandato**: **# fpm -1 <nivel> -f <archivo de mandatos>**. **Valor de retorno**: Si se ejecuta de forma satisfactoria, este mandato sale con un valor de 0. Si no es satisfactorio, el mandato sale con un valor de 1.

Tabla 8. Funciones de HIPAA y detalles de implementación (continuación)

Funciones de HIPAA	Especificación de implementación	Implementación de aixpert	Mandatos y valores de retorno
Habilitación de RBAC	Crea usuarios **isso**, **so** y **sa** y asigna roles adecuados a los usuarios.	Sugiere que cree usuarios **isso**, **so** y **sa**. Asigna roles adecuados a los usuarios.	**Mandato**: **/etc/security/pscexpert/bin/RbacEnablement**.

Información relacionada:

Health Insurance Portability and Accountability Act (HIPAA)

Conformidad con North American Electric Reliability Corporation

North American Electric Reliability Corporation (NERC) es una corporación sin fines de lucro que desarrolla el estándar para la industria de los sistemas de energía eléctrica. PowerSC Standard Edition contiene un perfil NERC preconfigurado, que proporciona estándares de seguridad que se pueden utilizar para proteger sistemas de energía eléctrica críticos.

El perfil de NERC sigue los estándares de CIP (Critical Infrastructure Protection - Protección de infraestructura crucial).

El perfil de NERC se encuentra en `/etc/security/aixpert/custom/NERC.xml`. Puede restablecer los requisitos de CIP que se aplican al perfil de NERC al estado predeterminado aplicando el perfil NERC_to_AIXDefault.xml que se encuentra en el directorio `/etc/security/aixpert/custom`. Este proceso no es igual que la operación de deshacer del perfil de NERC.

La tabla siguiente proporciona información sobre los estándares de CIP que se aplican al sistema operativo AIX y cómo PowerSC Standard Edition maneja los estándares de CIP:

Tabla 9. Estándares de CIP para PowerSC Standard Edition

Estándar de CIP	Implementación de AIX Security Expert	Ubicación del script que modifica el valor
CIP-003-3 R5.1	Configura los parámetros de seguridad de sistema para evitar problemas eliminando los atributos de identificación de usuario establecido (SUID) y de identificación de grupo establecido (SGID) de los archivos binarios.	• `/etc/security/pscexpert/bin/filepermgr` • `/etc/security/pscexpert/bin/rmsuidfrmrcmds`
CIP-003-3 R5.1.1	Habilita el control de acceso basado en roles (RBAC) creando roles de usuario operador del sistema, administrador del sistema y responsable de seguridad del sistema de información con los permisos necesarios.	`/etc/security/pscexpert/bin/EnableRbac`
CIP-005-3a R2.1-R2.4	Habilita Secure Shell (SSH) para el acceso de seguridad.	`/etc/security/pscexpert/bin/sshstart`
CIP-005-3a R2.5 CIP-007-5 R1.1	Inhabilita los siguientes servicios no necesarios y no seguros: • Daemon **lpd** • Common Desktop Environment (CDE)	`/etc/security/pscexpert/bin/comntrows`

Tabla 9. Estándares de CIP para PowerSC Standard Edition (continuación)

Estándar de CIP	Implementación de AIX Security Expert	Ubicación del script que modifica el valor
CIP-005-3a R2.5 CIP-007-5 R1.1	Inhabilita los siguientes servicios no necesarios y no seguros: • Daemon **timed** • Daemon **NTP** • Daemon **rwhod** • Daemon **DPID2** • Agente DHCP	`/etc/security/pscexpert/bin/rctcpip`
CIP-005-3a R2.5 CIP-007-5 R1.1	Inhabilita los siguientes servicios no necesarios y no seguros: • 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** • Servicio cmsd • Servicio ttdbserver • Servicio echo de TCP • Servicio discard de TCP • Servicio chargen de TCP • Servicio daytime de TCP • Servicio time de TCP • Servicio echo de UDP • Servicio discard de UDP • Servicio chargen de UDP • Servicio daytime de UDP • Servicio time de UDP	`/etc/security/pscexpert/bin/cominetdconf`
CIP-005-3a R2.5 CIP-007-5 R1.1	Aplica la denegación de solicitud de servicio para los puertos de mitigación.	`/etc/security/pscexpert/bin/tcptr_aixpert`
CIP-005-3a R3 CIP-007-3a R5, R6.5 CIP-007-5 R4.4	Habilita la auditoría de los archivos binarios en el sistema.	`/etc/security/pscexpert/bin/pciaudit`
CIP-007-3a R3 CIP-007-5 R2.1	Visualiza un mensaje para habilitar Trusted Network Connect (TNC).	`/etc/security/pscexpert/bin/GeneralMsg`

Tabla 9. Estándares de CIP para PowerSC Standard Edition (continuación)

Estándar de CIP	Implementación de AIX Security Expert	Ubicación del script que modifica el valor
CIP-007-3a R4 CIP-007-5 R3.3	Mantiene la integridad del sistema mediante la detección, eliminación y protección frente a tipos conocidos de software malicioso.	`/etc/security/pscexpert/bin/manageITsecurity`
CIP-007-3a R5.2.1	Permite cambiar la contraseña en el primer inicio de sesión para todas las cuentas de usuarios predeterminadas que no están bloqueadas.	`/etc/security/pscexpert/bin/pwdchg`
CIP-007-3a R5.2.2-R5.2.3	Bloquea todas las cuentas de usuario predeterminadas.	`/etc/security/pscexpert/dodv2/lockacc_rlogin`
CIP-007-3a R5.3.1	Establece cada contraseña en un mínimo de 6 caracteres.	`/etc/security/pscexpert/bin/chusrattr`
CIP-007-5 R5.5.1	Establece cada contraseña en un mínimo de 8 caracteres.	`/etc/security/pscexpert/bin/chusrattr`
CIP-007-3a R5.3.2 CIP-007-5 R5.5.2	Establece cada contraseña en una combinación de caracteres alfabéticos, numéricos y especiales.	`/etc/security/pscexpert/bin/chusrattr`
CIP-007-3a R5.3.3 CIP-007-5 R5.6	Cambia cada contraseña cada año.	`/etc/security/pscexpert/bin/chusrattr`
CIP-007-3a R7	Visualiza un mensaje para habilitar el Sistema de archivos cifrado (EFS).	`/etc/security/pscexpert/bin/GeneralMsg`
CIP-007-5 R5.7	Limita el número de intentos de autenticación no satisfactorios.	`/etc/security/pscexpert/bin/chusrattr`
CIP-010-1 CIP-010-2 R2.1	Visualiza un mensaje para habilitar Conformidad en tiempo real (RTC).	`/etc/security/pscexpert/bin/GeneralMsg`

Información relacionada:

Conformidad con North American Electric Reliability Corporation

Gestión de la automatización de la seguridad y conformidad

Conozca el proceso de planificación y despliegue de los perfiles de automatización de la seguridad y conformidad de PowerSC en un grupo de sistemas de acuerdo con los procedimientos de conformidad y gobierno de TI.

Como parte de la conformidad y el gobierno de TI, los sistemas que ejecutan clases de datos de seguridad y carga de trabajo similares se deben gestionar y configurar de forma coherente. Para planificar y desplegar la conformidad en los sistemas, realice las tareas siguientes:

Identificación de los grupos de trabajo del sistema

Las directrices de conformidad y de gobierno de TI afirman que los sistemas que se ejecutan en clases de datos de carga de trabajo y seguridad similares deben gestionarse y configurarse de forma coherente. Por lo tanto, debe identificar todos los sistemas en un grupo de trabajo similar.

Utilización de un sistema para pruebas que no es de producción para la configuración inicial

Aplicar el perfil de conformidad de PowerSC adecuado al sistema para pruebas.

Tenga en cuenta los ejemplos siguientes para aplicar perfiles de conformidad en el sistema operativo AIX.

Ejemplo 1: Aplicación de `DoD.xml`

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

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

En este ejemplo, no hay reglas anómalas, es decir, `Failedrules=0`. Esto significa que todas las reglas se aplican correctamente y la fase de prueba se puede iniciar. Si hay anomalías, se genera salida detallada.

Ejemplo 2: Aplicación de `PCI.xml` con una anomalía

```
# 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
```

La anomalía de la regla `pci_grpck` se debe resolver. Las posibles causas de la anomalía incluyen las siguientes razones:

- La regla no se aplica al entorno y debe eliminarse.
- Hay un problema en el sistema que se debe arreglar.

Investigación de una regla anómala

En la mayoría de los casos, no hay ningún error cuando se aplica un perfil de seguridad y conformidad de PowerSC. Sin embargo, el sistema puede tener requisitos previos relacionados con la instalación que faltan u otras cuestiones que requieren la atención del administrador.

La causa de la anomalía puede investigarse utilizando el ejemplo siguiente:

Vea el archivo `/etc/security/aixpert/custom/PCI.xml` y localice la regla anómala. En este ejemplo la regla es `pci_grpck`. Ejecute el mandato **fgrep**, busque la regla anómala `pci_grpck` y vea la regla XML asociada.

```
fgrep -p pci_grpck /etc/security/aixpert/custom/PCI.xml
<AIXPertEntry name="pci_grpck" function="grpck"
<AIXPertRuleType type="DLS"/
<AIXPertDescription&gt;Implementa partes de PCI Sección 8.2,
Comprobar definiciones de grupo: Verifica si las definiciones de grupo son correctas y arregla los errores
</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
Definiciones de sistema y contraseña de grupo de usuarios</AIXPertGroup
</AIXPertEntry
```

En la regla `pci_grpck`, se puede ver el mandato `/usr/sbin/grpck`.

Actualización de la regla anómala

Al aplicar un perfil de seguridad y conformidad de PowerSC, puede detectar errores.

El sistema puede tener requisitos previos de instalación que faltan y otros problemas que requieren la atención del administrador. Después de determinar el mandato subyacente de la regla anómala, examine el sistema para conocer el mandato de configuración que está fallando. Es posible que el sistema tenga un problema de seguridad. También puede ser que una regla determinada no sea aplicable al entorno del sistema. A continuación, se debe crear un perfil de seguridad personalizado.

Creación de perfil de configuración de seguridad personalizada

Si una regla no es aplicable al entorno específico del sistema, la mayoría de las organizaciones de conformidad permiten excepciones documentadas.

Para eliminar una regla y crear una política de seguridad y un archivo de configuración personalizados, realice los pasos siguientes:

1. Copie el contenido de los archivos siguientes en un único archivo denominado `/etc/security/aixpert/custom/<mi_política_seguridad>.xml`:

   `/etc/security/aixpert/custom/[PCI.xml|DoD.xml|SOX-COBIT.xml]`
2. Edite el archivo `<mi_política_seguridad>.xml` eliminando la regla que no es aplicable de la etiqueta XML de apertura`<AIXPertEntry name...` a la etiqueta XML de finalización `</AIXPertEntry`.

Puede insertar reglas de configuración adicionales por seguridad. Inserte las reglas adicionales en el esquema `AIXPertSecurityHardening` de XML. No puede cambiar los perfiles de PowerSC directamente, pero puede personalizar los perfiles.

Para la mayoría de entornos, debe crear una política XML personalizada. Para distribuir un perfil de cliente a otros sistemas, debe copiar de forma segura la política XML personalizada en el sistema que necesita la misma configuración. Se utiliza un protocolo seguro, como protocolo de transferencia de archivos seguro (SFTP), para distribuir una política XML personalizada a otros sistemas y el perfil se almacena en una ubicación segura `/etc/security/aixpert/custom/<my_security_policy.xml>/etc/security/aixpert/custom/`

Inicie la sesión en el sistema donde se debe crear un perfil personalizado y ejecute el mandato siguiente:

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

Prueba de las aplicaciones con el AIX Profile Manager

Las configuraciones de seguridad pueden afectar a las aplicaciones y la forma en que se accede al sistema y éste se gestiona. Es importante probar las aplicaciones y los métodos de gestión esperados del sistema antes de desplegar el sistema en un entorno de producción.

Los estándares de conformidad con la normativa imponen una configuración de seguridad que es más estricta que una configuración lista para usar. Para probar el sistema, realice los pasos siguientes:

1. Seleccione **Ver y gestionar perfiles** en el panel derecho de la página de bienvenida de AIX Profile Manager.
2. Seleccione el perfil utilizado por la plantilla para desplegarlo en los sistemas que se deben supervisar.
3. Pulse **Comparar**.
4. Seleccione el grupo gestionado o seleccione sistemas individuales dentro del grupo y pulse **Añadir**, para añadirlos que el recuadro seleccionado.
5. Pulse **Aceptar**.

La operación de comparación se inicia.

Supervisión de sistemas para la conformidad continuada con AIX Profile Manager

Las configuraciones de seguridad pueden afectar a las aplicaciones y la forma en que se accede al sistema y éste se gestiona. Es importante supervisar las aplicaciones y los métodos de gestión esperados del sistema cuando se despliega el sistema en un entorno de producción.

Para utilizar AIX Profile Manager para supervisar un sistema AIX, siga los pasos siguientes:

1. Seleccione **Ver y gestionar perfiles** en el panel derecho de la página de bienvenida de AIX Profile Manager.
2. Seleccione el perfil utilizado por la plantilla para desplegarlo en los sistemas que se deben supervisar.
3. Pulse **Comparar**.
4. Seleccione el grupo gestionado o seleccione sistemas individuales en el grupo y añádalos al recuadro seleccionado.
5. Pulse **Aceptar**.

La operación de comparación se inicia.

Configuración de la Automatización de la seguridad y conformidad de PowerSC

Conozca el procedimiento para configurar PowerSC para la Automatización de la seguridad y conformidad desde la línea de mandatos y utilizando AIX Profile Manager.

Configuración de valores de opciones de conformidad de PowerSC

Conozca los aspectos básicos de la característica de Automatización de la seguridad y conformidad de PowerSC, pruebe la configuración de sistemas de prueba que no son de producción y planifique y despliegue los valores. Cuando se aplica una configuración de conformidad, los valores cambian numerosos valores de configuración en el sistema operativo.

Nota: Algunos perfiles y estándares de conformidad inhabilitan Telnet, porque Telnet utiliza contraseñas de texto simple. Por lo tanto, debe tener Open SSH instalado, configurado y en funcionamiento. Puede utilizar cualquier otro medio de comunicación con el sistema que se está configurando. Estos estándares de conformidad requieren que se inhabilite el inicio de sesión `root`. Configure uno o varios usuarios no root antes de continuar aplicando los cambios de configuración. Esta configuración no habilita root y puede iniciar la sesión como usuario no root y ejecutar el mandato **su** para root. Pruebe si puede establecer la conexión SSH con el sistema, iniciar la sesión como el usuario no root y ejecutar el mandato `root`.

Para acceder a los perfiles de configuración de DoD, PCI, SOX o COBIT, utilice el directorio siguiente:

- Los perfiles del sistema operativo AIX se colocan en el directorio `/etc/security/aixpert/custom`.
- Los perfiles de Virtual I/O Server (VIOS) se colocan en el directorio `/etc/security/aixpert/core`.

Configuración de la conformidad de PowerSC desde la línea de mandatos

Implementar o comprobar el perfil de conformidad utilizando el mandato **pscxpert** en el sistema AIX y el mandato **viosecure** en el Virtual I/O Server (VIOS).

Para aplicar los perfiles de conformidad de PowerSC en un sistema AIX, escriba uno de los mandatos siguientes, lo que depende del nivel de conformidad de seguridad que desea aplicar.

Tabla 10. Mandatos PowerSC para AIX

Mandato	Estándar de conformidad
% pscxpert -f /etc/security/aixpert/custom/DoD.xml	*US Department of Defense UNIX Security Technical Implementation Guide*
% pscxpert -f /etc/security/aixpert/custom/Hipaa.xml	*Heath Insurance Portability and Accountability Act*
% pscxpert -f /etc/security/aixpert/custom/PCI.xml	*Payment Card Industry Data Security Standard*
% pscxpert -f /etc/security/aixpert/custom/SOX-COBIT.xml	*Ley Sarbanes-Oxley de 2002 – Gobierno de COBIT IT*

Para aplicar los perfiles de conformidad de PowerSC en un sistema VIOS, especifique uno de los mandatos siguientes para el nivel de conformidad de seguridad que desea aplicar.

Tabla 11. Mandatos de PowerSC para el Virtual I/O Server

Mandato	Estándar de conformidad
% viosecure -file /etc/security/aixpert/custom/DoD.xml	*US Department of Defense UNIX Security Technical Implementation Guide*
% viosecure -file /etc/security/aixpert/custom/Hipaa.xml	*Heath Insurance Portability and Accountability Act*
% viosecure -file /etc/security/aixpert/custom/PCI.xml	*Payment Card Industry Data Security Standard*
% viosecure -file /etc/security/aixpert/custom/SOX-COBIT.xml	*Ley Sarbanes-Oxley de 2002 – Gobierno de COBIT IT*

El mandato **pscxpert** en el sistema AIX y el mandato **viosecure** en VIOS pueden tomar tiempo para ejecutarse porque comprueban o establecen el sistema completo y hacen cambios de configuración relacionados con la seguridad. La salida es similar al ejemplo siguiente:

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

Sin embargo, algunas normas fallan en función del entorno AIX, el conjunto de instalación y la configuración anterior.

Por ejemplo, una regla de requisito previo puede fallar porque el sistema no tiene el conjunto de archivos de instalación necesario. Es necesario comprender cada error y resolverlo antes de desplegar los perfiles de conformidad por el centro de datos.

Conceptos relacionados:

"Gestión de la automatización de la seguridad y conformidad" en la página 103
Conozca el proceso de planificación y despliegue de los perfiles de automatización de la seguridad y conformidad de PowerSC en un grupo de sistemas de acuerdo con los procedimientos de conformidad y gobierno de TI.

Configuración de la conformidad de PowerSC con AIX Profile Manager

Conozca el procedimiento para configurar los perfiles de seguridad y conformidad de PowerSC y para desplegar la configuración en un sistema gestionado AIX utilizando AIX Profile Manager.

Para configurar los perfiles de seguridad y conformidad de PowerSC utilizando AIX Profile Manager, realice los pasos siguientes:

1. Inicie la sesión en IBM Systems Director y seleccione AIX Profile Manager.
2. Cree una plantilla que se base en uno de los perfiles de seguridad y conformidad de PowerSC realizando los pasos siguientes:
   a. Pulse **Ver y gestionar plantillas** en el panel derecho de la página de bienvenida de AIX Profile Manager.
   b. Pulse **Crear**.
   c. Pulse **Sistema operativo** en la lista **Tipo de plantilla**.
   d. Proporcione un nombre para la plantilla en el campo **Nombre de plantilla de configuración**.

e. Pulse **Continuar** > **Guardar**.

3. Seleccione el perfil a utilizar con la plantilla seleccionando **Examinar** en la opción **Seleccionar qué perfil utilizar para esta plantilla**. Los perfiles visualizan los elementos siguientes:
   - `ice_DLS.xml` es el nivel de seguridad predeterminado del sistema operativo AIX.
   - `ice_DoD.xml` es la publicación Department of Defense Security and Implementation Guide para los valores de UNIX.
   - `ice_HLS.xml` es una seguridad genérica de algo nivel para los valores de AIX.
   - `ice_LLS.xml` es la seguridad bajo nivel para los valores de AIX.
   - `ice_MLS.xml` es la seguridad de nivel medio para los valores de AIX.
   - `ice_PCI.xml` es el valor de Payment Card Industry para el sistema operativo AIX.
   - `ice_SOX.xml` son los valores de SOX o COBIT para el sistema operativo AIX.
4. Elimine cualquier perfil del recuadro seleccionado.
5. Seleccione **Añadir** para mover el perfil necesario al recuadro seleccionado.
6. Pulse **Guardar**.

Para desplegar la configuración en un sistema gestionado AIX, siga los pasos siguientes:

1. Seleccione **Ver y gestionar plantillas** en el panel derecho de la página de bienvenida de AIX Profile Manager.
2. Seleccione la plantilla necesaria que se debe desplegar.
3. Pulse **Desplegar**.
4. Seleccione los sistemas en los que desplegar el perfil y pulse **Añadir** para mover el perfil necesario al recuadro seleccionado.
5. Pulse **Aceptar** para desplegar la plantilla de configuración. El sistema se configura de acuerdo con la plantilla seleccionada del perfil.

Para que el despliegue se realice satisfactoriamente para DoD, PCI o SOX, PowerSC Standard Edition se debe instalar en el punto final del sistema AIX. Si el sistema que se está desplegando no tiene instalado PowerSC, el despliegue falla. IBM Systems Director despliega la plantilla de configuración en los puntos finales de sistema AIX seleccionados y los configura de acuerdo con los requisitos de conformidad.

Información relacionada:

Gestor de perfiles de AIX

IBM Systems Director

PowerSC Conformidad en tiempo real

La característica PowerSC Conformidad en tiempo real supervisa continuamente los sistemas AIX habilitados para asegurarse de que están configurados de forma coherente y segura.

La característica PowerSC Conformidad en tiempo real funciona con las políticas de Automatización de conformidad de PowerSC y AIX Security Expert para proporcionar una nofiticación cuando se producen violaciones de conformidad o cuando cambia un archivo supervisado. Cuando se viola la política de configuración de seguridad de un sistema, la característica PowerSC Conformidad en tiempo real envía un correo electrónico o un mensaje de texto para alertar al administrador de sistema.

La característica PowerSC Conformidad en tiempo real es una característica de seguridad pasiva que soporta perfiles de conformidad cambiados o predefinidos que incluyen Department of Defense Security Technical Implementation Guide, Payment Card Industry Data Security Standard, la Ley Sarbanes-Oxley y la conformidad de COBIT. Se proporciona una lista predeterminada de archivos para supervisar los cambios, pero puede añadir archivos a la lista.

Instalación de PowerSC Conformidad en tiempo real

La característica PowerSC Conformidad en tiempo real se instala con PowerSC Standard Edition versión 1.1.4, o posterior, y no forma parte del sistema operativo AIX base.

Para instalar PowerSC Standard Edition, complete los pasos siguientes:

1. Asegúrese de que está ejecutando uno de los siguientes sistemas operativos AIX en el sistema donde está instalando la característica PowerSC Standard Edition:
   - IBM AIX 6 con el nivel de tecnología 7, o posteriores, con AIX Event Infrastructure para AIX y clústeres AIX (bos.ahafs 6.1.7.0), o posteriores
   - IBM AIX 7 con el nivel de tecnología 1, o posteriores, con AIX Event Infrastructure para AIX y clústeres AIX (bos.ahafs 7.1.1.0), o posteriores
   - AIX Versión 7.2, o posteriores, con AIX Event Infrastructure para AIX y clústeres AIX (bos.ahafs 7.2.0.0), o posteriores
2. Para actualizar o instalar el conjunto de archivos de la característica PowerSC Standard Edition, instale el conjunto de archivos `powerscStd.rtc` del paquete de instalación para PowerSC Standard Edition versión 1.1.4, o posteriores.

Configuración de PowerSC Conformidad en tiempo real

Puede configurar PowerSC Conformidad en tiempo real para enviar alertas cuando se producen violaciones de un perfil de conformidad o cambios en un archivo supervisado. Algunos ejemplos de los perfiles incluyen Department of Defense Security Technical Implementation Guide, Payment Card Industry Data Security Standard, la ley Sarbanes-Oxley y COBIT.

Puede configurar PowerSC Conformidad en tiempo real utilizando uno de los métodos siguientes:

- Escriba el mandato **mkrtc**.
- Ejecute la herramienta SMIT especificando el mandato siguiente:

  ```
  smit RTC
  ```

Identificación de archivos supervisados por la característica PowerSC Conformidad en tiempo real

La característica PowerSC Conformidad en tiempo real supervisa en una lista predeterminada de archivos de los valores de seguridad de alto nivel los cambios, que se pueden personalizar añadiendo o eliminando archivos de la lista de archivos del archivo `/etc/security/rtc/rtcd_policy.conf`.

Hay dos métodos para identificar la plantilla de conformidad que se aplica en un sistema. Un método es utilizar el mandato **pscxpert** y el otro es utilizar Gestor de perfiles de AIX con IBM Systems Director.

Cuando se identifica el perfil de conformidad, puede añadir archivos adicionales a la lista de archivos a supervisar incluyendo los archivos adicionales en el archivo `/etc/security/rtc/rtcd_policy.conf`. Después de guardar el archivo, la nueva lista se utiliza inmediatamente como línea base y se supervisan por los cambios sin reiniciar el sistema.

Establecimiento de alertas para PowerSC Conformidad en tiempo real

Debe configurar la notificación de la característica PowerSC Conformidad en tiempo real indicando el tipo de alertas y los destinatarios de las alertas.

El daemon rtcd, que es el componente principal de la característica PowerSC Conformidad en tiempo real, obtiene su información sobre los tipos de alertas y destinatarios del archivo de configuración `/etc/security/rtc/rtcd.conf`. Puede editar este archivo para actualizar la información utilizando un editor de texto.

Información relacionada:

Formato de archivo /etc/security/rtc/rtcd.conf para la conformidad en tiempo real

Arranque fiable

La característica Arranque fiable utiliza el VTPM (Virtual Trusted Platform Module - Módulo de plataforma fiable virtual), que es una instancia virtual del TPM del Trusted Computing Group. El VTPM se utiliza para almacenar de forma segura las mediciones del arranque del sistema para la futura verificación.

Conceptos sobre Arranque fiable

Es importante conocer la integridad del proceso de arranque y saber clasificar el arranque como arranque fiable o arranque no fiable.

Puede configurar un máximo de 60 particiones lógicas (LPAR) habilitadas para VTPM para cada sistema físico utilizando la Consola de gestión de hardware (HMC). Cuando se configura, VTPM es exclusivo para cada LPAR. Cuando se utiliza con la tecnología de AIX Trusted Execution, VTPM proporciona seguridad y garantías a las particiones siguientes:

- La imagen de arranque en el disco
- El sistema operativo completo
- Las capas de aplicación

Un administrador puede ver sistemas fiables y no fiables desde una consola central que se instala con el verificador **openpts** que está disponible en el paquete de expansión de AIX. La consola **openpts** gestiona uno o más servidores Power Systems y supervisa o testifica el estado fiable de los sistemas AIX Profile Manager en todo el centro de datos. La testificación es el proceso donde el verificador determina (o testifica) si un recopilador ha realizado un arranque fiable.

Estado de arranque fiable

Se dice que una partición es fiable si el verificador testifica satisfactoriamente la integridad del recopilador. El verificador es la partición remota que determina si un recopilador ha realizado un arranque fiable. El recopilador es la partición AIX que tiene un VTPM (Virtual Trusted Platform Module) conectado y la TSS (Trusted Software Stack) instalada. Indica que las medidas que se registran en el VTPM coinciden con un conjunto de referencia mantenido por el verificador. Un estado de arranque fiable indica si la partición ha arrancado de forma fiable. Esta declaración trata sobre la integridad del proceso de arranque del sistema y no indica el nivel actual o en curso de la seguridad del sistema.

Estado de arranque no fiable

Una partición entra en un estado no fiable si el verificador no puede testificar satisfactoriamente la integridad del proceso de arranque. El estado no fiable indica que algún aspecto del proceso de arranque es incoherente con la información de referencia mantenida por el verificador. Las causas posibles para una testificación anómala incluyen arrancar desde un dispositivo de arranque diferente, arrancar una imagen de kernel diferente y cambiar la imagen de arranque existente.

Conceptos relacionados:

"Resolución de problemas del Arranque fiable" en la página 115
Existen algunos escenarios comunes y medidas correctivas que son necesarios para ayudar a identificar la razón del error de testificación cuando se utiliza el Arranque fiable.

Planificación del arranque fiable

Conozca las configuraciones de hardware y software que son necesarias para instalar el arranque fiable.

Requisitos previos de Arranque fiable

La instalación de Arranque fiable implica la configuración del recopilador y verificador.

Cuando se prepare para reinstalar el sistema operativo AIX en un sistema con Arranque fiable ya instalado, debe copiar el archivo `/var/tss/lib/tpm/system.data` y utilizarlo para sobrescribir el archivo en la misma ubicación después de que se haya completado una reinstalación. Si no copia este archivo, debe eliminar el módulo de plataforma fiable virtualizada de la consola de gestión y instalarlo en la partición.

Recopilador

Los requisitos de configuración para instalar un recopilador implica los siguientes requisitos previos:

- El hardware de POWER7 que se ejecuta en un release de firmware 740.
- Instale IBM AIX 6 con el nivel de tecnología 7 o instale IBM AIX 7 con el nivel de tecnología 1.
- Instale Hardware Management Console (HMC) versión 7.4 o posterior.
- Configure la partición con el VTPM y un mínimo de 1 GB de memoria.
- Instale Secure Shell (SSH), específicamente OpenSSH o equivalente.

Verificador

Se puede acceder al verificador **openpts** desde la interfaz de línea de mandatos y la interfaz gráfica de usuario que se ha designado para ejecutarse en un rango de plataformas. La versión de AIX del verificador de OpenPTS está disponible en el paquete de expansión de AIX. Las versiones del verificador de OpenPTS para Linux y otras plataformas están disponibles a través de una descarga web. Los requisitos de configuración incluyen los requisitos previos siguientes:

- Instale SSH, específicamente OpenSSH o equivalente.
- Establezca la conectividad de red (mediante SSH) al recopilador.
- Instale Java™ 1.6 o posterior para acceder a la consola de **openpts** desde la interfaz gráfica.

Preparación de la corrección

La información de Arranque fiable que se describe aquí sirve como guía para identificar situaciones que puedan necesitar corrección. No afecta al proceso de arranque.

Hay muchas circunstancias que pueden causar que una testificación falle y es difícil predecir la circunstancia que puede encontrar. Debe decidir sobre la acción adecuada dependiendo de la circunstancia. Sin embargo, es una buena práctica prepararse para algunos de los casos graves y tener una política o un flujo para ayudarle a manejar esas incidencias. La corrección es la acción correctiva que se debe realizar cuando la testificación indica que uno o varios recopiladores no son fiables.

Por ejemplo, si se ha producido una anomalía de testificación debido a que la imagen de arranque difiere de la referencia del verificador, considere la posibilidad de tener respuestas a las siguientes preguntas:

- ¿Cómo se puede verificar que la amenaza es creíble?
- ¿Hay algún mantenimiento planificado que se ha llevado a cabo, una actualización de AIX o nuevo hardware que se ha instalado recientemente?
- ¿Puede ponerse en contacto con el administrador que tiene acceso a esta información?
- ¿Cuándo se ha arrancado el sistema por última vez en un estado fiable?
- Si la amenaza de seguridad parece legítima, ¿qué acción debe realizar? (Las sugerencias incluye recopilar registros de auditoría, desconectar el sistema de la red, apagar el sistema y alertar a los usuarios).
- ¿Había otros sistemas comprometidos que se deban comprobar?

Conceptos relacionados:

"Resolución de problemas del Arranque fiable" en la página 115
Existen algunos escenarios comunes y medidas correctivas que son necesarios para ayudar a identificar la razón del error de testificación cuando se utiliza el Arranque fiable.

Consideraciones acerca de la migración

Tenga en cuenta estos requisitos previos antes de migrar una partición que está habilitada para el módulo de plataforma fiable virtual (VTPM).

Una ventaja de un VTPM durante un TPM físico es que permite que la partición se desplace entre sistemas mientras conserva el VTPM. Para migrar de forma segura la partición lógica, el firmware cifra los datos de VTPM antes de la transmisión. Para garantizar una migración segura, se deben implementar las siguientes medidas de seguridad antes de la migración:

- Habilite IPSEC entre el Virtual I/O Server (VIOS) que está realizando la migración.
- Establezca la clave de sistema fiable mediante la Consola de gestión de hardware (HMC) para controlar los sistemas gestionados que son capaces de descifrar los datos de VTPM después de la migración. El sistema de destino de migración debe tener la misma clave que el sistema de origen para migrar correctamente los datos.

Información relacionada:

Utilización de HMC

Migración de VIOS

Instalación del arranque fiable

Hay algunas configuraciones de hardware y software necesarias que se requieren para instalar el Arranque fiable.

Información relacionada:

"Instalación de PowerSC Standard Edition" en la página 7
Debe instalar un conjunto de archivos para cada función específica de PowerSC Standard Edition.

Instalación del recopilador

Debe instalar el recopilador utilizando el conjunto de archivos del CD base de AIX.

Para instalar el recopilador, instale los paquetes `powerscStd.vtpm` y `openpts.collector` que están en el CD base, utilizando el mandato **smit** o **installp**.

Instalación del verificador

El componente verificador OpenPTS se ejecuta en el sistema operativo AIX y en otras plataformas.

La versión AIX del verificador puede instalarse desde el conjunto de archivos utilizando el paquete de expansión de AIX. Para instalar el verificador en el sistema operativo AIX, instale el paquete `openpts.verifier` del paquete de expansión de AIX utilizando el mandato **smit** o **installp**. Esto instala la línea de mandatos y las versiones de interfaz gráfica del verificador.

El verificador OpenPTS para otros sistemas operativos pueden descargarse de `Descargar verificador de Linux OpenPTS para utilizarlo con el arranque fiable de AIX`.

Información relacionada:

Descargar el verificador de Linux OpenPTS para utilizarlo con el arranque fiable de AIX

Configuración del arranque fiable

Conozca el procedimiento para inscribir un sistema y para testificar un sistema para el arranque fiable.

Inscripción de un sistema

Conozca el procedimiento para inscribir un sistema en el verificador.

La inscripción de un sistema es el proceso de proporcionar un conjunto inicial de medidas al verificador, lo que forma la base para las solicitudes de testificación subsiguientes. Para inscribir un sistema desde la línea de mandatos, utilice el mandato siguiente desde el verificador:

```
openpts -i <nombre_host>
```

La información sobre la partición inscrita está ubicada en el directorio `$HOME/.openpts`. Cada nueva partición se asigna con un identificador exclusivo durante el proceso de inscripción y la información relacionada con las particiones inscritas se almacena en el directorio correspondiente al ID exclusivo.

Para inscribir un sistema desde la interfaz gráfica, realice los pasos siguientes:

1. Inicie la interfaz gráfica utilizando el mandato **/opt/ibm/openpts_gui/openpts_GUI.sh**.
2. Seleccione **Inscribir** en el menú de navegación.
3. Especifique el nombre de host y las credenciales SSH del sistema.
4. Pulse **Inscribir**.

Conceptos relacionados:

"Testificación de un sistema"
Conozca el procedimiento para testificar un sistema desde la línea de mandatos y utilizando la interfaz gráfica.

Testificación de un sistema

Conozca el procedimiento para testificar un sistema desde la línea de mandatos y utilizando la interfaz gráfica.

Para consultar la integridad de un arranque del sistema, utilice el mandato siguiente desde el verificador:

```
openpts <nombre_host>
```

Para testificar un sistema desde la interfaz gráfica, realice los pasos siguientes:

1. Seleccione una categoría en el menú de navegación.
2. Seleccione uno o varios sistemas que se deban testificar.
3. Pulse **Testificar**.

Inscripción y testificación de un sistema sin contraseña

La solicitud de testificación se envía a través de Secure Shell (SSH). Instale el certificado del verificador en el recopilador para permitir conexiones SSH sin ninguna contraseña.

Para configurar el certificado del verificador en el sistema del recopilador, siga los pasos siguientes:

- En el verificador, ejecute los mandatos siguientes:

  ```
  ssh-keygen    # Ninguna contraseña
  scp ~/.ssh/id_rsa.pub <recopilador>:/tmp
  ```

- En el recopilador, ejecute el mandato siguiente:

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

Gestión del arranque fiable

Conozca el procedimiento para gestionar los resultados de testificación del Arranque fiable.

Interpretación de los resultados de testificación

Conozca el procedimiento para ver e interpretar los resultados de testificación.

Una testificación puede producir uno de los estados siguientes:

1. La solicitud de testificación ha fallado: la solicitud de testificación no se ha completado satisfactoriamente. Consulte la sección Resolución de problemas para conocer las causas posibles de la anomalía.
2. Integridad de sistema válida: la testificación se ha completado satisfactoriamente y el arranque del sistema coincide con la información de referencia mantenida por el verificador. Esto indica un Arranque fiable satisfactorio.
3. Integridad de sistema válida: la solicitud de testificación ha finalizado pero se ha detectado una discrepancia entre la información que se recopila durante el arranque del sistema y la información de referencia mantenida por el verificador. Esto indica un arranque no fiable.

La testificación también indica si se ha aplicado una actualización al recopilador utilizando el siguiente mensaje:

Actualización de sistema disponible: este mensaje indica que se ha aplicado una actualización en el recopilador y hay disponible un conjunto de información de referencia actualizada que estará vigente en el próximo arranque. En el verificador se le solicita al usuario que acepte o rechace las actualizaciones. Por ejemplo, el usuario puede elegir aceptar estas actualizaciones si el usuario es consciente del mantenimiento que está teniendo lugar en el recopilador.

Para investigar una anomalía de testificación utilizando la interfaz gráfica, realice los pasos siguientes:

1. Seleccione una categoría en el menú de navegación.
2. Seleccione un sistema para investigarlo.
3. Efectúe una doble pulsación en la entrada correspondiente al sistema. Aparece una ventana de propiedades. Esta ventana contiene información de registro sobre la testificación que ha fallado.

Supresión de sistemas

Conozca el procedimiento para suprimir un sistema de la base de datos del verificador.

Para eliminar un sistema de la base de datos del verificador, ejecute el mandato siguiente:

```
openpts -r <nombre_host>
```

Resolución de problemas del Arranque fiable

Existen algunos escenarios comunes y medidas correctivas que son necesarios para ayudar a identificar la razón del error de testificación cuando se utiliza el Arranque fiable.

El mandato **openpts** declara un sistema como no válido si el estado de arranque actual del sistema no coincide con la información de referencia que se mantiene en el verificador. El mandato **openpts** determina la posible razón para que la integridad no sea válida. Existen varias variables en un arranque de AIX completo y una testificación anómala necesita un análisis para determinar la causa de la anomalía.

La tabla siguiente lista algunos de los escenarios comunes y las medidas correctivas para determinar la razón de la anomalía:

Tabla 12. Resolución de problemas de algunos de los casos de ejemplo comunes de anomalía

Razón de la anomalía	**Causas posibles de la anomalía**	**Corrección sugerida**

La testificación no se ha completado.	• Nombre de host incorrecto.
	• No hay ninguna ruta de red entre el origen y el destino.
	• Credenciales de seguridad incorrectas.
		Compruebe la conexión de Secure Shell (SSH) utilizando el mandato siguiente:
		`ssh ptsc@hostname`
		
		Si la conexión SSH es satisfactoria, compruebe las siguientes razones de anomalía de testificación:
		• El sistema que se está testificando no está ejecutando el daemon **tcsd**.
		• El sistema que se está testificando no se ha inicializado mediante el mandato **ptsc**. Este proceso debe producirse automáticamente durante el arranque de sistema pero compruebe la presencia de un directorio `/var/ptsc/` en el recopilador. Si el directorio `/var/ptsc/` no existe, ejecute el mandato siguiente en el recopilador:
		`ptsc -i`

El firmware CEC ha cambiado.	• Se ha aplicado una actualización de firmware. • La LPAR se ha migrado a un sistema que estaba ejecutando una versión diferente del firmware.	Compruebe el nivel de firmware del sistema que aloja la LPAR.
Han cambiado los recursos asignados a la LPAR.	Ha cambiado la CPU o la memoria asignada a la LPAR.	Compruebe el perfil de partición en la HMC.
El firmware ha cambiado para los adaptadores que están disponibles en la LPAR.	Se ha añadido o eliminado un dispositivo de hardware de la LPAR.	Compruebe el perfil de partición en la HMC.
La lista de dispositivos conectados a la LPAR ha cambiado.	Se ha añadido o eliminado un dispositivo de hardware de la LPAR.	Compruebe el perfil de partición en la HMC.
La imagen de arranque ha cambiado, lo que incluye el kernel de sistema operativo.	• Se ha aplicado una actualización de AIX y el verificador no conocía la actualización. • Se ha ejecutado el mandato **bosboot**.	• Confirme con el administrador del recopilador si se ha realizado algún mantenimiento antes de la última operación de rearranque. • Compruebe los registros en el recopilador para la actividad de mantenimiento.
La LPAR arranca desde un dispositivo diferente.	• La inscripción se ha realizado inmediatamente después de la instalación de red. • El sistema arranca desde un dispositivo de mantenimiento.	El dispositivo de arranque y los distintivos se pueden comprobar utilizando el mandato **bootinfo**. Si la inscripción se ha llevado a cabo inmediatamente después de la instalación de Network Installation Management (NIM) y antes de la operación de rearranque, los detalles inscritos pertenecen a la instalación de red y no al próximo arranque de disco. Esta inscripción se puede reparar eliminando la inscripción y volviendo a inscribir la partición lógica.
Se ha llamado al menú de arranque de SMS (Servicios de gestión del sistema) interactivo.		El proceso de arranque debe ejecutarse ininterrumpida sin interacción del usuario para que un sistema sea fiable. La entrada en el menú de arranque de SMS hace que el arranque no sea válido.
Se ha modificado la base de datos de Trusted Execution (TE).	• Se han añadido o eliminado archivos binarios de la base de datos de TE. • Se han actualizado archivos binarios en la base de datos.	Ejecute el mandato **trustchk** para verificar la base de datos.

Conceptos relacionados:

"Preparación de la corrección" en la página 112
La información de Arranque fiable que se describe aquí sirve como guía para identificar situaciones que puedan necesitar corrección. No afecta al proceso de arranque.

"Conceptos sobre Arranque fiable" en la página 111
Es importante conocer la integridad del proceso de arranque y saber clasificar el arranque como arranque fiable o arranque no fiable.

Información relacionada:

Utilización de HMC

Cortafuegos fiable

La característica Cortafuegos fiable proporciona seguridad de capa de virtualización que mejora el rendimiento y la eficiencia de recursos al comunicarse entre diferentes zonas de seguridad de LAN virtual (VLAN) en el mismo servidor de Power Systems. El cortafuegos fiable reduce la carga en la red externa moviendo la capacidad de filtrado de los paquetes de cortafuegos que cumplen las reglas especificadas a la capa de virtualización. Esta capacidad de filtrado la controlan reglas de filtro de red fácilmente definidas, que permiten el tráfico de red fiable para cruzar entre las zonas de seguridad de VLAN sin salir del entorno virtual. El cortafuegos fiable protege y direcciona el tráfico de red interno entre los sistemas operativos AIX, IBM i y Linux.

Conceptos sobre Cortafuegos fiable

Hay algunos conceptos básicos que se deben conocer al utilizar el Cortafuegos fiable.

El hardware de Power Systems puede configurarse con varias zonas de seguridad de red de área local virtual (VLAN). Una política configurada por el usuario, creada como una regla de filtro de cortafuegos fiable, permite que parte del tráfico de red fiable cruce zonas de seguridad de VLAN permanezca interno a la capa de virtualización. Esto es similar a colocar un cortafuegos físico conectado a red en el entorno virtualizado, lo que proporciona un método más eficiente para el rendimiento de implementar prestaciones de cortafuegos para centros de datos virtualizados.

Con el Cortafuegos fiable, puede configurar reglas para permitir que determinados tipos de tráfico se transfieran directamente de una VLAN de un Virtual I/O Server (VIOS) a otra VLAN del mismo VIOS, mientras se sigue manteniendo un alto nivel de seguridad limitando otros tipos de tráfico. Es un cortafuegos configurables dentro de la capa de virtualización de los servidores de Power Systems.

Utilizando el ejemplo de la Figura 1 en la página 120, el objetivo debe poder transferir información de forma segura y eficiente de LPAR1 en VLAN 200 y de LPAR2 en VLAN 100. Sin el cortafuegos fiable, la información destinada a LPAR2 desde LPAR1 se envía fuera de la red interna al direccionador, que direcciona la información de vuelta a LPAR2.

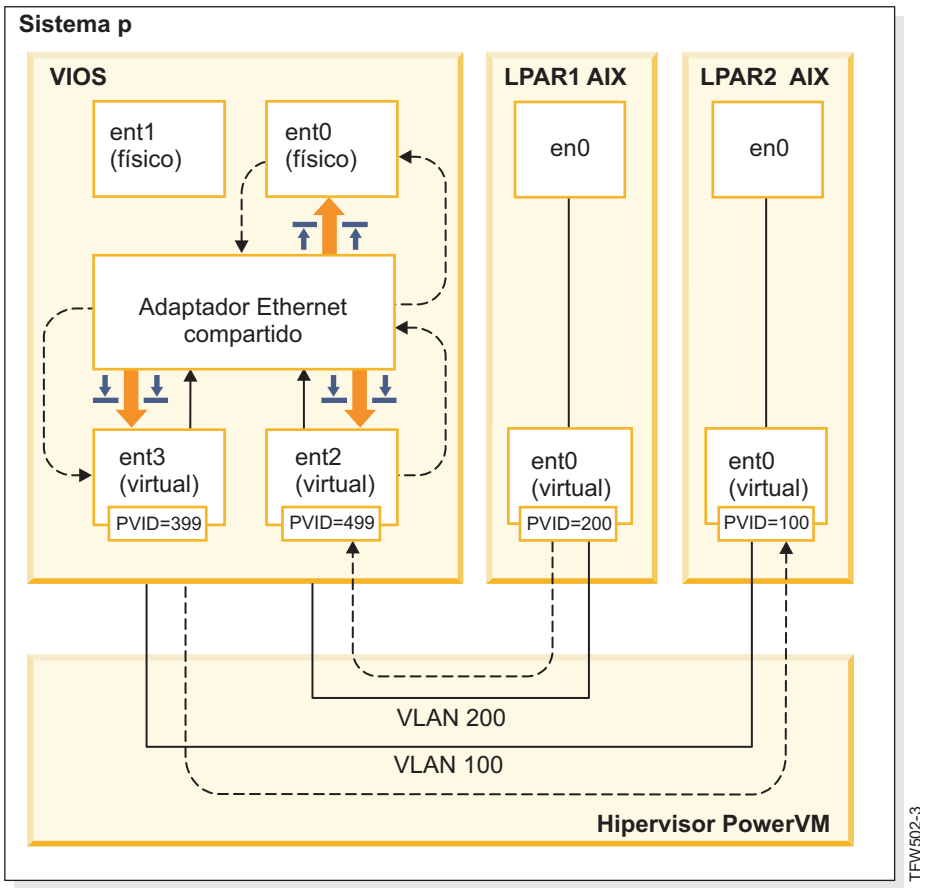

Figura 1. Ejemplo de transferencia de información entre VLAN sin cortafuegos fiable

Mediante el uso del cortafuegos fiable, puede configurar reglas para permitir que la información pase de LPAR1 a LPAR2 sin salir de la red interna. Esta vía de acceso se muestra en la Figura 2 en la página 121.

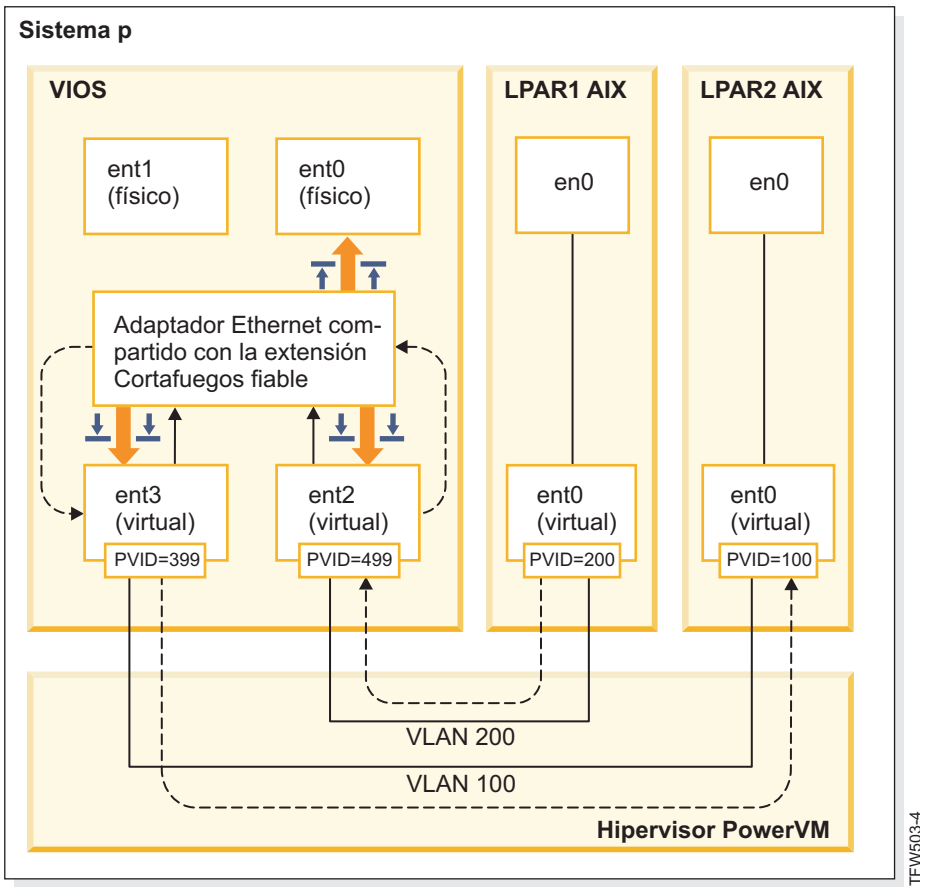

Figura 2. Ejemplo de transferencia de información entre VLAN con cortafuegos fiable

Las reglas de configuración que permiten que determinada información pase de forma segura a través de las VLAN acortan la vía de acceso al destino. El cortafuegos fiable utiliza el adaptador Ethernet compartido (SEA) y extensión de kernel de la máquina virtual de seguridad (SVM) para permitir la comunicación.

Adaptador Ethernet compartido
El SEA es el lugar donde empieza y finaliza el direccionamiento. Cuando se registra la SVM, el SEA recibe los paquetes y los reenvía a la SVM. Si la SVM determina que el paquete es para una LPAR en el mismo servidor de Power Systems, actualiza la cabecera de capa 2 del paquete. El paquete se devuelve al SEA para reenviarlo al destino final dentro del sistema o en la red externa.

Máquina virtual de seguridad
La SVM es el lugar donde se aplican las reglas de filtrado. Las reglas de filtrado son necesarias para mantener la seguridad en la red interna. Después de registrar la SVM en el SEA, los paquetes se reenvían a la SVM antes de enviarlos a la red externa. Según las reglas de filtrado activas, la SVM determina si un paquete permanece en la red interna o se mueve a la red externa.

Instalación del Cortafuegos fiable

La instalación del Cortafuegos fiable de PowerSC es similar a la instalación de otras características de PowerSC.

Requisitos previos:

- Las versiones de PowerSC anteriores a 1.1.1.0 no tienen el conjunto de archivos necesario para instalar el Cortafuegos fiable. Asegúrese de tener el CD de instalación de PowerSC para la versión 1.1.1.0 o posterior.

- Para aprovechar el Cortafuegos fiable, debe haber utilizado ya la Consola de gestión de hardware (HMC) o Virtual I/O Server (VIOS) para configurar las LAN virtuales (VLAN).

El Cortafuegos fiable se proporciona como un conjunto de archivos adicional en el CD de instalación de PowerSC Standard Edition. El nombre del archivo es `powerscStd.svm.rte`. Puede añadir el Cortafuegos fiable a una instancia existente de PowerSC Versión 1.1.0.0, o posterior, o instalarlo como parte de una nueva instalación de PowerSC Versión 1.1.1.0, o posterior.

Para añadir la función de Cortafuegos fiable a una instancia de PowerSC:

1. Asegúrese de que está ejecutando VIOS Versión 2.2.1.4 o posterior.
2. Inserte el CD de instalación de PowerSC para la versión 1.1.1.0 o descargue la imagen del CD de instalación.
3. Utilice el mandato **oem_setup_env** para el acceso como usuario root.
4. Utilice el mandato **installp** o la herramienta SMIT para instalar el conjunto de archivos `PowerscStd.svm.rte`.

Información relacionada:

"Instalación de PowerSC Standard Edition" en la página 7
Debe instalar un conjunto de archivos para cada función específica de PowerSC Standard Edition.

Configuración de cortafuegos fiable

Se necesitan valores de configuración adicionales para la característica de cortafuegos fiable después de instalarla.

Trusted Firewall Advisor

Trusted Firewall Advisor analiza el tráfico de sistema de diferentes particiones lógicas (LPAR) para proporcionar información para determinar si la ejecución de Cortafuegos fiable mejora el rendimiento del sistema.

Si la función Trusted Firewall Advisor registra una cantidad significativa de tráfico de diferentes LAN virtuales (VLAN) que están en el mismo complejo electrónico central, la habilitación de Cortafuegos fiable beneficiará al sistema.

Para habilitar Trusted Firewall Advisor, especifique el mandato siguiente:

```
vlantfw -m
```

Para visualizar los resultados de Advisor Trusted Firewall, escriba el mandato siguiente:

```
vlantfw -D
```

Para inhabilitar Trusted Firewall Advisor, especifique el mandato siguiente:

```
vlantfw -M
```

Registro de Cortafuegos fiable

El registro de Cortafuegos fiable compila una lista de vías de acceso de tráfico de red en el complejo electrónico central. La lista muestra los filtros que el Cortafuegos fiable utiliza para direccionar el tráfico.

Cuando Trusted Firewall Advisor determina que el direccionamiento interno del tráfico mejora la eficiencia, el registro de Cortafuegos fiable mantiene una lista de vías de acceso en el archivo `svm.log`. El tamaño del archivo `svm.log` está limitado a 16 MB. Si las entradas superan el límite de 16 MB, se eliminan las entradas más antiguas del archivo de registro.

Para iniciar el registro de Cortafuegos fiable, especifique el mandato siguiente:

```
vlantfw -l
```

Para detener el registro de Cortafuegos fiable, especifique el mandato siguiente:

```
vlantfw -L
```

Puede ver el archivo de registro en la siguiente ubicación: `/home/padmin/svm/svm.log`.

Nota: Puede ejecutar los mandatos para iniciar y detener el registro de Cortafuegos fiable sólo cuando esté autenticado como usuario root.

Varios adaptadores Ethernet compartidos

Puede configurar el Cortafuegos fiable en sistemas que utilizan varios adaptadores Ethernet compartidos.

Algunas configuraciones utilizan varios adaptadores Ethernet compartidos (SEA) en el mismo Virtual I/O Server (VIOS). Varios SEA pueden proporcionar beneficios de protección de migración tras error y nivelación de recursos. El Cortafuegos fiable soporta el direccionamiento mediante varios SEA, a condición de que estén en el mismo VIOS.

La Figura 3 muestra un entorno que utiliza varios SEA.

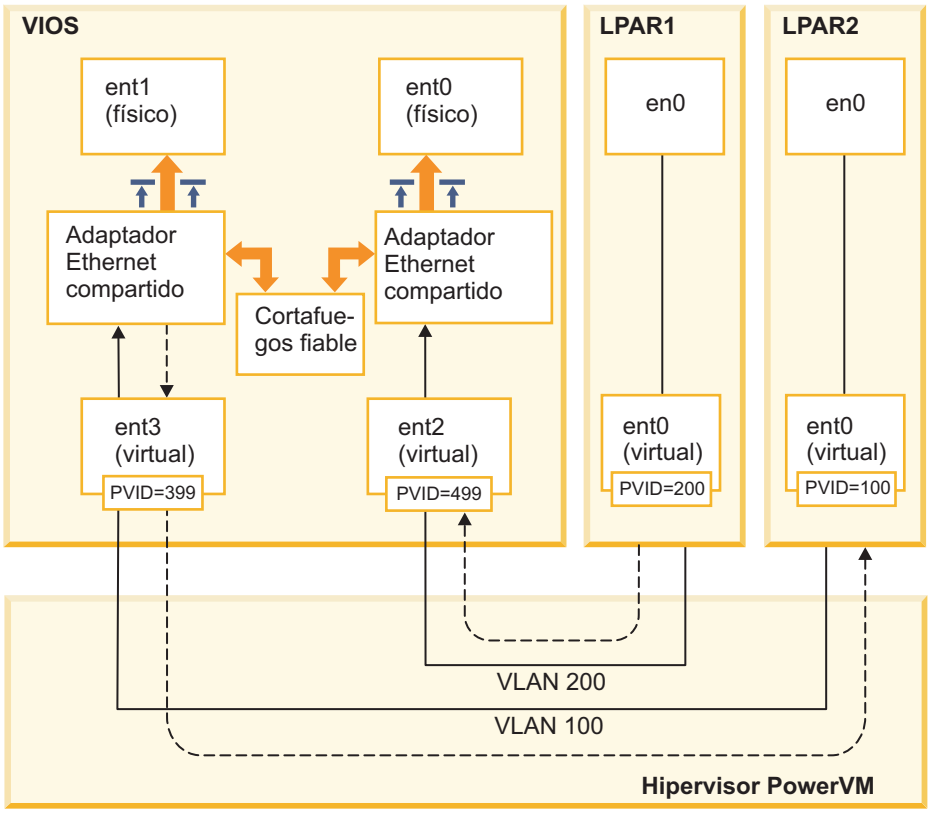

Figura 3. Configuración con varios adaptadores Ethernet compartidos en un único VIOS

Los siguientes son ejemplos de varias configuraciones de SEA soportadas por el Cortafuegos fiable:

- Los SEA están configurados con adaptadores troncales en el mismo conmutador virtual de hipervisor de Power. Esta configuración se soporta porque cada SEA recibe el tráfico de red con diferentes ID de VLAN.
- Los SEA están configurados con adaptadores troncales en diferentes conmutadores virtuales de hipervisor Power y cada adaptador troncal está en un ID de VLAN distinto. En esta configuración, cada SEA todavía recibe tráfico de red utilizando diferentes ID de VLAN.

- Los SEA están configurados con adaptadores troncales en diferentes conmutadores virtuales de hipervisor Power y los mismos ID de VLAN se reutilizan en los conmutadores virtuales. En este caso, el tráfico para ambos SEA tiene los mismos ID de VLAN.

  Un ejemplo de esta configuración tiene LPAR2 en VLAN200 con el conmutador virtual 10 y LPAR3 en VLAN200 con el conmutador virtual 20. Dado que ambas LPAR y sus correspondientes SEA utilizan el mismo ID de VLAN (VLAN200), ambos SEA tienen acceso a los paquetes con ese ID de VLAN.

No puede permitir extenderse en más de un VIOS. Por esta razón, el Cortafuegos fiable no soporta las diversas configuraciones de SEA siguientes:

- Varios VIOS y varios controladores de SEA.
- Compartimiento de carga de SEA redundante: los adaptadores troncales que están configurados para el direccionamiento entre VLAN no pueden dividirse entre los servidores de VIOS.

Eliminación de adaptadores Ethernet compartidos

Los pasos para eliminar dispositivos de adaptador Ethernet compartido del sistema deben realizarse en un orden específico.

Para eliminar un adaptador Ethernet compartido (SEA) del sistema, realice los pasos siguientes:

1. Elimine la Máquina virtual de seguridad que está asociada con el SEA especificando el mandato siguiente:

   ```
   rmdev -dev svm
   ```

2. Elimine el SEA especificando el mandato siguiente:

   ```
   rmdev -dev ID_adaptador_ethernet_compartido
   ```

Nota: Eliminar el SEA antes de eliminar SVM puede producir una anomalía del sistema.

Creación de reglas

Puede crear reglas para habilitar el direccionamiento de VLAN cruzadas de Cortafuegos fiable.

Para habilitar las características de direccionamiento de Trusted Firewall, debe crear reglas especificando qué comunicaciones están permitidas. Para mayor seguridad, no hay una sola regla que permita la comunicación entre todas las VLAN en el sistema. Cada conexión permitida requiere su propia regla, aunque cada regla que se activa permite la comunicación en ambas direcciones para sus puntos finales especificados.

Puesto que la creación de reglas se crea en la interfaz de Virtual I/O Server (VIOS), hay disponible información adicional sobre los mandatos en la colección de temas de VIOS en el Information Center de hardware de Power Systems.

Para crear una regla, realice los pasos siguientes:

1. Abra la interfaz de línea de mandatos de VIOS.
2. Inicialice el controlador de SVM especificando el mandato siguiente:

   ```
   mksvm
   ```

3. Inicie el Cortafuegos fiable escribiendo el mandato de inicio:

   ```
   vlantfw -s
   ```

4. Para visualizar todas las direcciones LPAR IP y MAC, especifique el mandato siguiente:

   ```
   vlantfw -d
   ```

   Necesitará las direcciones IP y MAC de las particiones lógicas (LPAR) para las que está creando reglas.

5. Cree la regla de filtro para permitir la comunicación entre las dos LPAR (LPAR1 y LPAR2) especificando uno de los siguientes mandatos (los mandatos deben escribirse en una sola línea):

```
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: De forma predeterminada una regla de filtro permite la comunicación en ambas direcciones, dependiendo de las entradas de puerto y protocolo. Por ejemplo, puede habilitar Telnet para LPAR1 a LPAR2 ejecutando el mandato siguiente:

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

6. Active todas las reglas de filtro en el kernel especificando el mandato siguiente:

```
mkvfilt -u
```

Nota: Este procedimiento activa esta regla y otras reglas de filtrado que existen en el sistema.

Ejemplos adicionales

Los ejemplos siguientes muestran otras reglas de filtro que puede crear utilizando el Cortafuegos fiable.

- Para permitir la comunicación Secure Shell desde la LPAR en la VLAN 100 a la LPAR en la VLAN 200, especifique el mandato siguiente:

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

- Para permitir el tráfico entre todos los puertos 0 - 499, escriba el mandato siguiente:

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

- Para permitir todo el tráfico TCP entre las LPAR, especifique el mandato siguiente:

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

  Si no especifica ningún puerto u operaciones de puerto, el tráfico puede utilizar todos los puertos.

- Para permitir la mensajería de Protocolo de mensajes de control de Internet entre las LPAR, especifique el mandato siguiente:

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

Conceptos relacionados:

"Desactivación de reglas"
Puede desactivar las reglas que permiten el direccionamiento de VLAN cruzadas en la característica Cortafuegos fiable.

Referencia relacionada:

"Mandato genvfilt" en la página 168

"Mandato mkvfilt" en la página 170

"Mandato vlantfw" en la página 190

Información relacionada:

Virtual I/O Server (VIOS)

Desactivación de reglas

Puede desactivar las reglas que permiten el direccionamiento de VLAN cruzadas en la característica Cortafuegos fiable.

Dado que las reglas se desactivan en la interfaz de Virtual I/O Server (VIOS), hay información adicional sobre los mandatos y procesos disponible en la colección de temas de VIOS en el Information Center de Hardware de Power Systems.

Para desactivar una regla, realice los pasos siguientes:

1. Abra la interfaz de línea de mandatos de VIOS.

2. Para visualizar todas las reglas de filtro activas, especifique el mandato siguiente:
   ```
   lsvfilt -a
   ```

   Puede omitir el distintivo **-a** para visualizar todas las reglas de filtro almacenadas en el Gestor de datos de objetos.
3. Anote el número de identificación de la regla de filtro que está desactivando. Para este ejemplo, el número de identificación de la regla de filtro es 23.
4. Desactive la regla de filtro 23 cuando esté activa en el kernel especificando el mandato siguiente:
   ```
   rmvfilt -n 23
   ```

   Para desactivar todas las reglas de filtro en el kernel, escriba el mandato siguiente:
   ```
   rmvfilt -n all
   ```

Conceptos relacionados:

"Creación de reglas" en la página 124
Puede crear reglas para habilitar el direccionamiento de VLAN cruzadas de Cortafuegos fiable.

Referencia relacionada:

"Mandato lsvfilt" en la página 170

"Mandato rmvfilt" en la página 190

Registro fiable

El registro fiable de PowerVM permite a las particiones lógicas (LPAR) de AIX grabar en archivos de registro que están almacenados en un Virtual I/O Server (VIOS) adjunto. Los datos se transmiten al VIOS directamente a través del hipervisor y la conectividad de red no es necesaria entre la LPAR de cliente y VIOS.

Registros virtuales

El administrador de Virtual I/O Server (VIOS) crea y gestiona los archivos de registro y éstos se presentan al sistema operativo AIX como dispositivos de registro virtuales en el directorio `/dev`, similares a los discos virtuales o soportes ópticos virtuales.

El almacenamiento de archivos de registro como registros virtuales aumenta el nivel de confianza en los registros porque no los puede cambiar ningún usuario con privilegios de root en el cliente LPAR donde se han generado. Se puede adjuntar varios dispositivos de registro virtuales al mismo cliente LPAR y cada registro es un archivo diferente en el directorio `/dev`.

El registro fiable permite que los datos de registro de varias LPAR de cliente se consoliden en un sistema de archivos único, que es accesible desde el VIOS. Por lo tanto, el VIOS proporciona una sola ubicación en el sistema para el análisis de registro y archivado. El administrador de LPAR del cliente puede configurar aplicaciones y el sistema operativo AIX para grabar datos en los dispositivos de registro virtuales, lo que es similar a grabar datos en los archivos locales. El subsistema de auditoría de AIX puede configurarse para que dirija los registros de auditoría a registros virtuales y otros servicios de AIX, como syslog, funcionan con su configuración existente para dirigir los datos a registros virtuales.

Para configurar el registro virtual, el administrador de VIOS debe especificar un nombre para el registro virtual, que tiene los siguientes componentes independientes:

- Nombre de cliente
- Nombre de registro

El administrador de VIOS puede establecer los nombres de los dos componentes en cualquier valor, pero normalmente el nombre de cliente es el mismo para todos los registros virtuales que están conectados a una LPAR determinada (por ejemplo, el nombre de host de LPAR). El nombre de registro se utiliza para identificar la finalidad del registro (por ejemplo, audit o syslog).

En una AIX LPAR, cada dispositivo de registro virtual está presente como dos archivos funcionalmente equivalentes en el sistema de archivos `/dev`. El primer archivo tiene el nombre del dispositivo, por ejemplo, `/dev/vlog0`, y el segundo archivo se denomina concatenando un prefijo `vl` con el nombre de registro y el número de dispositivo. Por ejemplo, si el dispositivo de registro virtual `vlog0` tiene `audit` como nombre de registro, está presente en el sistema de archivos `/dev` como `vlog0` y `vlaudit0`.

Información relacionada:

Creación de registros virtuales

Detección de dispositivos de registro virtual

Una vez que un administrador de VIOS ha creado dispositivos de registro virtuales y los ha conectado a un cliente LPAR, la configuración de dispositivo de LPAR de cliente debe renovarse para que los dispositivos estén visibles.

El administrador de LPAR de cliente renueva los valores utilizando uno de los métodos siguientes:

- Rearrancar la LPAR de cliente
- Ejecutar el mandato **cfgmgr**

Ejecute el mandato **lsdev** para visualizar los dispositivos de registro virtuales. Los dispositivos tienen el prefijo `vlog` de forma predeterminada. A continuación, se muestra un ejemplo de la salida de mandato **lsdev** en una LPAR de AIX en la que hay dos dispositivos de registros virtuales:

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

Revise las propiedades de un dispositivo de registro virtual individual utilizando el mandato `lsattr –El <nombre_dispositivo>`, que produce salida que es similar a la siguiente:

```
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
```

Esta salida muestra el nombre de cliente, el nombre de dispositivo y la cantidad de datos de registro que VIOS puede almacenar.

El registro virtual almacena dos tipos de datos de registro, que son:

- Datos de registro: Los datos de registro en bruto generados por aplicaciones en la LPAR de AIX.
- Datos de estado: Información sobre cuándo los dispositivos se han configurado, abierto, cerrado y otras operaciones que se utilizan para analizar la actividad de registro.

El administrador de VIOS especifica la cantidad de **datos de registro** y **datos de estado** que pueden almacenarse para cada registro virtual y la cantidad se indica mediante los atributos `max_log_size` y `max_state_size`. Cuando la cantidad de datos almacenados supera el límite especificado, los primeros datos de registro se sobrescriben. El administrador de VIOS debe asegurarse de que los datos de registro se recopilan y archivan con frecuencia para conservar los registros.

Instalación del Registro fiable

Puede instalar la característica Registro fiable de PowerSC utilizando la interfaz de línea de mandatos o la herramienta SMIT.

Los requisitos previos para instalar el Registro fiable son VIOS 2.2.1.0 o posterior y IBM AIX 6 con el nivel de tecnología 7 o IBM AIX 7 con el nivel de tecnología 1.

El nombre de archivo para instalar la característica de Registro fiable es `powerscStd.vlog`, que se incluye en el CD de instalación de PowerSC Standard Edition.

Para instalar la función de Registro fiable:

1. Asegúrese de que está ejecutando VIOS Versión 2.2.1.0 o posterior.
2. Inserte el CD de instalación de PowerSC o descargue la imagen del CD de instalación.
3. Utilice el mandato **installp** o la herramienta SMIT para instalar el conjunto de archivos `powerscStd.vlog`.

Información relacionada:

"Instalación de PowerSC Standard Edition" en la página 7
Debe instalar un conjunto de archivos para cada función específica de PowerSC Standard Edition.

Configuración del registro fiable

Conozca el procedimiento para configurar el registro fiable en el subsistema de auditoría de AIX y syslog.

Configuración del subsistema de auditoría de AIX

El subsistema de auditoría de AIX puede configurarse para grabar datos binarios en un dispositivo de registro virtual, además de grabar registros en el sistema de archivos local.

Nota: Antes de configurar el subsistema de auditoría de AIX, debe completar el procedimiento descrito en "Detección de dispositivos de registro virtual" en la página 127.

Para configurar el subsistema de auditoría de AIX, realice los pasos siguientes:

1. Configure el subsistema de auditoría de AIX para registrar datos en modalidad binaria (`auditbin`).
2. Active el Registro fiable para la auditoría de AIX editando el archivo de configuración `/etc/security/audit/config`.
3. Añada un parámetro `virtual_log = /dev/vlog0` a la stanza `bin:`.

   Nota: La instrucción es válida si el administrador de LPAR desea que se graben datos de `auditbin` en `/dev/vlog0`.
4. Reinicie el subsistema de auditoría de AIX en la secuencia siguiente:

   ```
   audit shutdown
   audit start
   ```

Los registros de auditoría se graban en Virtual I/O Server (VIOS) mediante el dispositivo de registro virtual especificado, además de grabar registros en el sistema de archivos local. Los registros se almacenan bajo el control de los parámetros `bin1` y `bin2` existentes en la stanza `bin:` del archivo de configuración `/etc/security/audit/config`.

Información relacionada:

Subsistema de auditoría

Configuración de syslog

Syslog puede configurarse para grabar mensajes en registros virtuales añadiendo reglas al archivo `/etc/syslog.conf`.

Nota: Antes de configurar el archivo `/etc/syslog.conf`, debe completar el procedimiento en "Detección de dispositivos de registro virtual" en la página 127.

Puede editar el archivo `/etc/syslog.conf` para que coincida con los mensajes de registro, que se basan en los siguientes criterios:

- Recurso
- Nivel de prioridad

Para utilizar los registros virtuales para los mensajes de syslog, se debe configurar el archivo `/etc/syslog.conf` con reglas para grabar los mensajes deseados en el registro virtual adecuado en el directorio `/dev`.

Por ejemplo, para enviar mensajes a nivel de depuración generados por cualquier recurso al registro virtual `vlog0`, añada la línea siguiente al archivo `/etc/syslog.conf`:

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

Nota: No utilice los recursos de rotación de registro que están disponibles en el daemon `syslogd` para cualquier mandato que graba datos en registros virtuales. Los archivos del sistema de archivos `/dev` no son archivos normales y no se pueden renombrar ni mover. El administrador de VIOS debe configurar la rotación de registro virtual dentro del VIOS.

El daemon `syslogd` se debe reiniciar después de la configuración utilizando el mandato siguiente:

```
refresh -s syslogd
```

Información relacionada:

Daemon syslogd

Grabación de datos en dispositivos de registro virtuales

Se graban datos arbitrarios en un dispositivo de registro virtual abriendo el archivo apropiado en el directorio `/dev` y grabando datos en el archivo. Un registro virtual puede abrirlo un proceso a la vez.

Por ejemplo:

Para grabar mensajes en los dispositivos de registro virtuales utilizando el mandato **echo**, especifique el mandato siguiente:

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

Para almacenar archivos en los dispositivos de registro virtuales utilizando el mandato **cat**, especifique el mandato siguiente:

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

El tamaño de grabación individual máximo está limitado a 32 KB y los programas que intentan grabar más datos en una única operación de grabación reciben un error de E/S (EIO). Los programas de utilidad de interfaz de línea de mandatos (CLI), por ejemplo el mandato **cat**, dividen automáticamente las transferencias en operaciones de grabación de 32 KB.

Trusted Network Connect (TNC)

Trusted Network Connect (TNC) forma parte del grupo de cálculo fiable (Trusted computing group - TCG) que proporciona especificaciones para verificar la integridad de punto final. TNC ha definido la arquitectura de solución abierta que ayuda a los administradores a aplicar políticas para controlar de forma efectiva el acceso a la infraestructura de red.

Trusted Network Connect (TNC) tiene cuatro componentes:

- Servidor de TNC
- TNC Patch Management
- Servidor de TNC
- Referenciador IP de TNC

Conceptos sobre Trusted Network Connect

Conozca los componentes, la configuración de la comunicación segura y el sistema de gestión de parches de Trusted Network Connect (TNC).

Componentes de Trusted Network Connect

Conozca los componentes de la infraestructura de Trusted Network Connect (TNC).

El modelo de TNC consta de los siguientes componentes:

Servidor de Trusted Network Connect (TNC)

El servidor de Trusted Network Connect (TNC) identifica los clientes que se añaden a la red e inicia una verificación sobre ellos.

El cliente de TNC proporciona la información de nivel de conjunto de archivos necesaria para el servidor para la verificación. El servidor determina si el cliente está en el nivel configurado por el administrador. Si el cliente no es compatible, el servidor de TNC notifica al administrador sobre las correcciones que son necesarias.

El servidor de TNC inicia las verificaciones en los clientes que intentan acceder a la red. El servidor de TNC carga un conjunto de verificadores de medición de integridad (IMV) que pueden solicitar las mediciones de integridad de los clientes y verificarlas. AIX tiene un IMV predeterminado, que verifica el conjunto de archivos y el nivel de parche de seguridad de los sistemas. El servidor de TNC es una infraestructura que carga y gestiona varios módulos IMV. Para verificar un cliente, se basa en los IMV para solicitar información de los clientes y verifica los clientes.

TNC Patch Management

El servidor de Trusted Network (TNC) se integra con SUMA (Service Update Management Assistant) y cURL para proporcionar una solución de gestión de parches.

El gestor de parche descarga los Service Pack y los arreglos de seguridad más recientes que están disponibles en los sitios web del IBM ECC y Fix Central. El daemon de TNC Patch Management envía la última información actualizada al servidor de TNC, que sirve de conjunto de archivos de línea base para verificar los clientes.

El daemon **tncpmd** se debe configurar para gestionar las descargas SUMA y enviar la información de conjunto de archivos al servidor de TNC. Este daemon debe alojarse en un sistema que esté conectado a

Internet para descargar automáticamente las actualizaciones. Para utilizar el servidor de TNC Patch Management sin conectarlo a Internet, puede registrar un repositorio de arreglos definidos por el usuario en el servidor de TNC Patch Management.

Nota: El servidor TNC y el daemon **tncpmd** pueden estar alojados en el mismo sistema.

Patch Management se proporciona mediante uno de los métodos siguientes:

- Utilizando la interfaz de línea de mandatos (pmconf)
- Utilizando el daemon (tncpmd2)

Utilización de la interfaz de línea de mandatos (pmconf) para proporcionar gestión de parches:

SUMA y cURL se invocan cuando se descarga un nivel de Service Pack (nivel de SP) utilizando el mandato **pmconf add**.

Cuando un nivel de Service Pack (nivel de SP) se descarga utilizando el mandato **pmconf add**, se invoca SUMA para descargar y registrar el nivel de SP con TNC. Además, cURL se invoca para descargar los arreglos de seguridad nuevos o que faltan.

Los siguientes argumentos de mandato **pmconf get** proporcionan control adicional sobre la gestión de arreglos de seguridad:

- **display-only** permite al usuario examinar descripciones de vulnerabilidades tratadas por los arreglos de seguridad que son aplicables para el nivel de SP. Los arreglos de seguridad no se descargan utilizando este mandato.
- **download-only** permite al usuario descargar, pero no aplicar, arreglos de seguridad en un directorio de descarga proporcionado por el usuario. No se aplicar arreglos.

Utilización del daemon (tncpmd2) para proporcionar gestión de parches:

El componente planificador del daemon puede configurarse para comprobar automáticamente las actualizaciones que afectan a la seguridad de los clientes de TNC.

Un intervalo de descarga controla la frecuencia con la que el planificador comprueba los niveles de Service Pack nuevos. Si se detecta un nuevo nivel de Service Pack para un nivel de tecnología (TL) que actualmente está registrado en TNC, se descargan y se añaden al repositorio el nuevo nivel de Service Pack y los arreglos de seguridad nuevos o que faltan. El intervalo de descarga se establece utilizando el mandato **pmconf init**. El valor recomendado es como mínimo una vez al mes (43.200 minutos).

Un “ifix_download_interval” controla la frecuencia con la que el planificador comprueba cualquier arreglo temporal de seguridad nuevo que pueda publicarse. Los arreglos de seguridad nuevos se descargan y se añaden al repositorio. El intervalo de descarga de arreglo temporal recomendado es una vez al día (1440 minutos).

Cliente de Trusted Network Connect

El cliente de Trusted Network Connect (TNC) proporciona la información que es necesaria para el servidor de TNC para la verificación.

El servidor determina si el cliente está en el nivel configurado por el administrador. Si el cliente no es compatible, el servidor de TNC notifica al administrador sobre las actualizaciones que son necesarias.

El cliente de TNC carga los IMC en el arranque y utiliza los IMC para recopilar la información necesaria.

Referenciador IP de Trusted Network Connect

El servidor de Trusted Network Connect (TNC) puede iniciar automáticamente la verificación en los clientes que forman parte de la red. El referenciador IP que se ejecuta en la partición de Virtual I/O

Server (VIOS) detecta los nuevos clientes a los que VIOS da servicio y envía las direcciones IP al servidor de TNC. El servidor de TNC verifica el cliente en lo que respecta a la política que está definida.

Comunicación segura de Trusted Network Connect

Los daemons de Trusted Network Connect (TNC) se comunican a través de los canales cifrados habilitados por TLS (Seguridad de la capa de transporte) o SSL (Capa de sockets seguros).

La comunicación segura es garantizar que los datos y mandatos que fluyen en la red estén autenticados y sean seguros. Cada sistema debe tener su propia clave y certificado, que se generan cuando se ejecuta el mandato de inicialización para los componentes. Este proceso es completamente transparente para el administrador y requiere menos intervención del administrador.

Para verificar un nuevo cliente, el certificado del cliente debe importarse a la base de datos del servidor. El certificado se ha marcado como no fiable inicialmente y, a continuación, el administrador utiliza el mandato **psconf** para ver y marcar los certificados como fiables especificando el mandato siguiente:

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

Para utilizar una clave y un certificado diferentes, el mandato **psconf** proporciona la opción para importar el certificado.

Para importar el certificado del servidor, especifique el mandato siguiente:

```
psconf import  -S -k<nombre_archivo_claves> -f<nombre_archivo_claves>
```

Para importar el certificado del cliente, especifique el mandato siguiente:

```
psconf import -C -k<nombre_archivo_claves> -f<nombre_archivo_claves>
```

Protocolo Trusted Network Connect

El protocolo Trusted Network Connect (TNC) se utiliza con la infraestructura de TNC para mantener la integridad de red.

TNC proporciona especificaciones para verificar la integridad de punto final. Los puntos finales que solicitan acceso se evalúan basándose en las medidas de integridad de componentes críticos que pueden afectar al entorno operativo. La infraestructura de TNC permite a los administradores supervisar la integridad de los sistemas en la red. TNC se integra con la infraestructura de distribución de parches de AIX para crear una solución de gestión de parches completa.

Las especificaciones de TNC deben satisfacer los requisitos de la arquitectura de sistema AIX y de la familia POWER. Los componentes de TNC están diseñados para proporcionar una solución de gestión de parches completa en el sistema operativo AIX. Esta configuración permite a los administradores gestionar eficazmente la configuración de software en los despliegues de AIX. Proporciona herramientas para verificar los niveles de parche de los sistemas y generar un informe sobre los clientes que no son compatibles. Además, la gestión de parches simplifica el proceso de descarga de los parches y de instalación de los mismos.

Módulos de IMC e IMV

El servidor o cliente de Trusted Network Connect (TNC) utilizan internamente los módulos de recopilador de medidas de integridad (IMC) y de verificador de medidas de integridad (IMV) para la verificación del servidor.

Esta infraestructura permite la carga de varios módulos IMC e IMV en el servicio y los clientes. El módulo que realiza la verificación a nivel de sistema operativo (OS) y conjunto de archivos se envía con el sistema operativo AIX de forma predeterminada. Para acceder a los módulos que se envían con el sistema operativo AIX, utilice una de los siguientes vías de acceso:

- `/usr/lib/security/tnc/libfileset_imc.a`: Recopila el nivel de sistema operativo e información sobre el conjunto de archivos que se ha instalado del sistema cliente y la envía a IMV (servidor de TNC) para su verificación.
- `/usr/lib/security/tnc/libfileset_imv.a`: Solicita la información de nivel de sistema operativo y de conjunto de archivos al cliente y la compara con la información de línea base. También actualiza el estado del cliente en la base de datos del servidor de TNC. Para ver el estado, escriba el mandato siguiente:

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

Referencia relacionada:

"Mandato psconf" en la página 175

Requisitos de TNC

Para utilizar plenamente todas las características de cada componente de TNC, debe verificar que los requisitos mínimos están disponibles en el entorno.

TNC Patch Management

AIX	SUMA	OpenSSL	Notas
7.2 TL1	7.2.1.0	1.0.2	Proporcionado con el sistema operativo
7.2 TL0	7.2.1.0	1.0.2	SUMA/Java puede necesitar instalarse por separado.
7.1 TL4	7.2.1.0	1.0.2	SUMA/Java puede necesitar instalarse por separado.
7.1 TL1, TL2, TL3			No hay soporte para descargar niveles de Service Pack de AIX 7.2
7.1 TL0			Nivel de release mínimo soportado para TNCPM

Configuración de los componentes de TNC

Cada uno de los componentes de Trusted Network Connect (TNC) necesita configuración para ejecutarse en el entorno específico.

Cada uno de los pasos del procedimiento siguiente es necesario para configurar los componentes de TCN. Se describen pasos opcionales adicionales en

1. Identifique las direcciones IP de los sistemas donde se configurarán el servidor de TNC, el servidor de TNC Patch Management (TNCPM) y el referenciador IP de TNC para el Virtual I/O Server (VIOS).
2. Configure el servidor de NIM (Gestión de instalación de red). El sistema que se ha configurado como servidor de TNCPM es el maestro NIM. El conjunto de archivos `sets:bos.sysmgt.nim.master` debe estar instalado en este sistema.
3. Debe habilitar Autonomic Health Advisor (AHA) para la notificación automática de nuevos Service Packs y arreglos de seguridad al servidor de TNC. Si no se habilita AHA, el planificador de TNC actualizará el servidor de TNC a intervalos planificados. Para habilitar AHA para la notificación automática:

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

4. Para inicializar los repositorios de arreglos para TNC Patch Management, escriba el mandato siguiente (entre el mandato en una sola línea):

   ```
   pmconf init -i <intervalo_descarga> -l <lista_TL> [-A] [-P <vía_acceso_descarga>]
   [-x <intervalo_ifix>] [-K <clave_ifix>]
   ```

A continuación se muestra un ejemplo del mandato **pmconf**:

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

El mandato **init** descarga el último Service Pack para cada nivel de tecnología y lo deja disponible para el servidor de TNC. Los Service Pack actualizados permiten al servidor de TNC ejecutar una verificación de cliente de TNC de línea base y que el servidor de TNC Patch Management instale actualizaciones de cliente de TNC. Especifique el distintivo **-A** para aceptar todos los acuerdos de licencia cuando se ejecutan las actualizaciones de cliente. De forma predeterminada, los repositorios de arreglos descargados por el servidor de TNC Patch Management están en el archivo `/var/tnc/tncpm/fix_repository`. Utilice el distintivo **-P** para especificar un directorio diferente.

5. Configure el servidor de TNCPM. El servidor de TNCPM puede configurarse en el sistema NIM. El servidor de TNCPM utiliza SUMA para descargar los parches de los sitios web de IBM Fix Central y ECC. El servidor de TNCPM utiliza cURL para descargar arreglos temporales del sitio de seguridad de IBM. Para descargar las actualizaciones, el sistema debe estar conectado a Internet. Especifique el mandato siguiente para configurar el servidor de TNCPM:

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

   Por ejemplo:

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

6. Configure las políticas sobre el servidor de TNC. Para crear las políticas para verificar los clientes, consulte “Creación de políticas para el cliente de Trusted Network Connect” en la página 139
7. Configure los clientes utilizando el mandato siguiente:

   ```
   psconf mkclient tncport=<puerto> tncserver=<ip_servidor>:<puerto>
   ```

   Por ejemplo:

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

8. Complete la configuración de los componentes de TNC realizando los pasos opcionales para cada componente.

Referencia relacionada:

“Mandato psconf” en la página 175

Información relacionada:

“Instalación de PowerSC Standard Edition” en la página 7
Debe instalar un conjunto de archivos para cada función específica de PowerSC Standard Edition.

Instalación con NIM

IBM Fix Central

Passport Advantage Online Help Center

Configuración de opciones para los componentes de TNC

Puede configurar una o más opciones para cada uno de los componentes de TNC.

Configuración de opciones para el servidor de Trusted Network Connect (TNC)

Conozca los pasos para configurar el servidor de TNC.

Para configurar el servidor de TNC, el archivo `/etc/tnccs.conf` debe tener un valor similar al siguiente:

```
component = SERVER
```

Para configurar un sistema como servidor, especifique el mandato siguiente:

```
psconf mkserver tncport=<puerto> pmserver=<ip|nombrehost[,ip2|nombrehost2..]:puerto>
[recheck_interval=<tiempo en mins>]
```

Por ejemplo:

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

Nota: El puerto `tncport` y el puerto `pmserver` se deben establecer en valores diferentes y, si no se proporciona el valor del parámetro `recheck_interval`, se utiliza un valor predeterminado de 1440 minutos.

Se utiliza el valor de puerto predeterminado de 42830 para el puerto `tncport` y se utiliza el valor predeterminado de 38240 para el puerto `pmserver`.

Referencia relacionada:

"Mandato psconf" en la página 175

Configuración de opciones adicionales para el cliente de Trusted Network Connect

Conozca los pasos para configurar el cliente de TNC (Trusted Network Connect) y los valores de configuración que son necesarios para la configuración.

Para configurar el cliente de TNC, el archivo `/etc/tnccs.conf` debe tener un valor similar al siguiente:

```
component = CLIENT
```

Para configurar un sistema como cliente, especifique el mandato siguiente:

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

Por ejemplo:

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

Nota: El valor del puerto de servidor y del `tncport`, que es un puerto de cliente, debe ser el mismo.

Referencia relacionada:

"Mandato psconf" en la página 175

Configuración de opciones para el servidor de TNC Patch Management

El servidor de Trusted Network Connect Patch Manager (TNCPM) se integra con SUMA y cURL para proporcionar una solución completa de gestión de parches.

El servidor de TNCPM debe configurarse en el servidor de Gestión de instalación de red (NIM) para que los clientes TNC puedan actualizarse.

Para habilitar las descargas automáticas de IBM Security Advisory y de arreglos temporales, puede especificar un intervalo de arreglo temporal. Esta característica proporciona la notificación automática de arreglos temporales de seguridad recién publicados e identificadores de CVE (Common Vulnerabilities and Exposures). Todas las advertencias de seguridad y los arreglos temporales se verifican antes del registro en TNC. La clave pública de vulnerabilidad de IBM AIX, que es necesaria para descargar automáticamente arreglos temporales, está disponible en el sitio web de seguridad de IBM AIX. Las descargas automáticas de paquetes de servicio y de arreglos temporales se inhabilitan estableciendo el intervalo de descarga y el intervalo de arreglo temporal en 0.

También puede actualizar el registro de Service Pack y de arreglo temporal manualmente. Para registrar manualmente un IBM Security Advisory junto con los correspondientes arreglos temporales, especifique el mandato siguiente:

```
pmconf add -y <archivo de advertencia> -v <archivo de firmas>  -e <archivo tar de ifix>
```

Para registrar manualmente un arreglo temporal autónomo, especifique el mandato siguiente:

```
pmconf add -p <SP> -e <archivo de ifix>
```

Para registrar un nuevo nivel de tecnología y descargar su último Service Pack, especifique el mandato siguiente:

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

Para descargar un Service Pack que no es de la versión más actual, o para descargar un nivel de tecnología que se utilizará para las actualizaciones de verificación y cliente, especifique el mandato siguiente:

```
pmconf add -l <lista TL> -d
pmconf add -s <lista SP>
```

Para registrar un repositorio de arreglos de nivel de tecnología y de service pack que existe en el sistema, especifique el mandato siguiente:

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

Para configurar un sistema para que sirva como servidor de Patch Management, especifique el mandato siguiente:

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

A continuación se muestra un ejemplo de este mandato:

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

El servidor de TNC Patch Management siempre soporta la gestión de APAR (Informes autorizados de análisis de programa) de seguridad. Especifique el mandato siguiente para configurar TNC Patch Management para gestionar otros tipos de APAR:

```
pmconf add -t <lista_tipos_APAR>
```

En el ejemplo anterior, <lista_tipos_APAR> es una lista separada por comas que contiene los siguientes tipos de APAR:

- HIPER
- PE
- Mejora

Para gestionar los Repositorios de Open Package de TNCPM, especifique uno o varios de los mandatos siguientes:

```
pmconf add -o <nombre_paquete> -V <versión> -T [installp|rqm] -D <vía_acceso_definida_por usuario>
pmconf delete -o <nombre_paquete> -V <versión>
pmconf list -o <nombre_paquete> -V <versión>
pmconf list -O [-c] [-q]
```

Se añaden Open Packages a este directorio predeterminado:

`/var/tnc/tncpm/fix_repository/packages`.

Vía de acceso definida por el usuario = Ubicación de paquete en el sistema

Para visualizar la información descriptiva tratada por los arreglos de seguridad para un nivel de Service Pack específico, sin aplicar los arreglos al repositorio, especifique el mandato siguiente:

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

Por ejemplo:

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

Para descargar arreglos de seguridad para un nivel de Service Pack específico, sin aplicar los arreglos al repositorio, especifique el mandato siguiente:

```
pmconf get -p <SP> -D <directorio_descarga>
```

Nota: El *directorio_descarga* debe existir antes de ejecutar este mandato.

Por ejemplo:

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

El servidor de TNC Patch Management soporta el mandato **syslog** para descargar actualizaciones de service pack, de nivel de tecnología y de cliente. El recurso es `user` y la prioridad es `info`. Un ejemplo de esto es `user.info`.

El servidor de TNC Patch Management también mantiene un registro con todas las actualizaciones de cliente en el directorio `/var/tnc/tncpm/log/update/<ip>/<indicación_fecha_hora>`.

Referencia relacionada:

"Mandato psconf" en la página 175

Información relacionada:

Seguridad de IBM AIX

Configuración de notificación de correo electrónico de servidor de Trusted Network Connect

Conozca el procedimiento para configurar la notificación de correo electrónico para el servidor de Trusted Network Connect (TNC).

El servidor de TNC ve el nivel de parche del cliente y si el servidor de TNC considera que el cliente no es conforme, envía un correo electrónico al administrador con el resultado y la corrección necesaria.

Para configurar la dirección de correo electrónico del administrador, especifique el mandato siguiente:

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

Por ejemplo:

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

En el ejemplo anterior, el correo electrónico para el grupo de IP *vayugrp1* y *vayugrp2* se envía a la dirección de correo electrónico abc@ibm.com.

Para enviar un correo electrónico a una dirección de correo electrónico global para el grupo de IP que no tiene asignada una dirección de correo electrónico, especifique el mandato siguiente:

```
psconf add –e <dirección_correo>
```

Por ejemplo:

```
psconf add –e abc@ibm.com
```

En el ejemplo anterior, si un grupo de IP no tiene asignada una dirección de correo electrónico, el correo se envía a la dirección de correo electrónico abc@ibm.com. Actúa como una dirección de correo electrónico global.

Referencia relacionada:

"Mandato psconf" en la página 175

Configuración del referenciador IP en VIOS

Aprenda a configurar el referenciador IP en Virtual I/O Server (VIOS) para iniciar la verificación automáticamente.

Nota: Debe configurar la extensión de kernel SVM en Virtual I/O Server (VIOS) antes de configurar el referenciador IP.

Para configurar el referenciador IP de TNC, el archivo de configuración `/etc/tnccs.conf` debe tener un valor similar al siguiente `component = IPREF`.

Puede configurar un sistema como cliente especificando el mandato siguiente:

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

Por ejemplo:

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

El valor del puerto `tncserver` y de `tncport`, que es el puerto de cliente, deben ser iguales.

Configure el referenciador IP de TNC en VIOS. Esta configuración en VIOS desencadena la verificación en los clientes que están conectándose a la red. Especifique el mandato siguiente para configurar el referenciador:

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

Por ejemplo:

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

Nota: El valor del puerto de servidor y del puerto de TNC, que es un puerto de cliente, debe ser el mismo.

Referencia relacionada:

"Mandato psconf" en la página 175

Gestión de componentes de Trusted Network Connect (TNC)

Aprenda a gestionar Trusted Network Connect (TNC) para implementar tareas como, por ejemplo, añadir los clientes, políticas, registros, resultados de verificación. actualizar clientes y certificados relacionados con TNC.

Visualización de los registros de servidor de Trusted Network Connect

Aprenda a visualizar los registros del servidor de Trusted Network Connect (TNC).

El servidor de TNC registra los resultados de verificación de todos los clientes. Para ver el registro, ejecute el mandato **psconf**:

```
psconf list –H –i <ip |ALL>
```

Referencia relacionada:

"Mandato psconf" en la página 175

Creación de políticas para el cliente de Trusted Network Connect

Aprenda a configurar políticas relacionadas con el cliente de Trusted Network Connect (TNC).

La consola de `psconf` proporciona la interfaz que es necesaria para gestionar las políticas de TNC. Cada cliente o un grupo de clientes se puede asociar con una política.

Se pueden crear las políticas siguientes:

- Un grupo de Internet Protocol (IP) contiene varias direcciones IP de cliente.
- Cada IP de cliente puede pertenecer sólo a un grupo.
- El grupo de IP está asociado con un grupo de políticas.
- Un grupo de políticas contiene diferentes clases de políticas. Por ejemplo, la política de conjunto de archivos que especifica cuál debe ser el nivel de sistema operativo del cliente (es decir, release, nivel de tecnología y Service Pack). Puede haber varias políticas de conjunto de archivos en un grupo de políticas y el cliente que hace referencia a esta política debe estar en el nivel especificado por una de las políticas de conjunto de archivos.

Los mandatos siguientes muestran cómo crear un grupo de IP, grupo de políticas y políticas de conjunto de archivos.

Para crear un grupo de IP, escriba el mandato siguiente:

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

Por ejemplo:

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

Nota: Para un grupo, se debe proporcionar como mínimo una dirección IP. Varias IP deben separarse con una coma.

Para crear una política de conjunto de archivos, especifique el mandato siguiente:

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

Por ejemplo:

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

Nota: La información de compilación debe estar en el formato `<rel00-TL-sp>`.

Para crear una política y para asignar un grupo de IP, escriba el mandato siguiente:

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

Por ejemplo:

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

Para asignar la política de conjunto de archivos a una política, escriba el mandato siguiente:

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

Por ejemplo:

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

Para añadir la política OpenPackage, especifique el mandato siguiente:

```
pconf add -O <grupo_openpkg> <nombre_openpkg:versión>
```

A continuación se muestra un ejemplo de adición de una política de OpenPackage:

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

Para asignar la política OpenPackage a Fspolicy, especifique el mandato siguiente:

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

Nota: Si se proporcionan varias políticas de conjunto de archivos, el sistema aplica la política que mejor coincide en el cliente. Por ejemplo, si el cliente está en `6100-02-01` y se menciona la política de conjunto de archivos como `7100-03-04` y `6100-02-03`, se aplica `6100-02-03` en el cliente.

Referencia relacionada:

"Mandato psconf" en la página 175

Inicio de la verificación para el cliente de Trusted Network Connect

Aprenda a verificar el cliente de Trusted Network Connect (TNC).

Utilice uno de los métodos siguientes para la verificación de cliente:

- El daemon de referenciador de IP en el Virtual I/O Server (VIOS) reenvía la IP de cliente al servidor de TNC: la LPAR de cliente adquiere la IP e intenta acceder a la red. El daemon de referenciador de IP en VIOS detecta la nueva dirección IP y la reenvía al servidor de TNC: el servidor de TNC inicia la verificación al recibir la nueva dirección IP.
- El servidor de TNC verifica el cliente periódicamente: el administrador puede añadir las IP de cliente que se deben verificar en la base de datos de políticas de TNC. El servidor de TNC verifique los clientes que están en la base de datos. La reverificación se produce automáticamente a intervalos regulares con referencia al valor del atributo `recheck_interval` que se especifica en el archivo de configuración `/etc/tnccs.conf`.
- El administrador inicia la verificación de cliente manualmente: el administrador puede iniciar la verificación manualmente para verificar si un cliente se ha añadido a la red ejecutando el mandato siguiente:

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

Nota: Para recursos que no están conectados a un VIOS, los clientes se pueden verificar y actualizar cuando se añaden manualmente al servidor de TNC.

Referencia relacionada:

"Mandato psconf" en la página 175

Visualización de los resultados de verificación de Trusted Network Connect

Conozca el procedimiento para ver los resultados de verificación del cliente de Trusted Network Connect (TNC).

Para ver los resultados de verificación de los clientes en la red, especifique el mandato siguiente:

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

Este mandato muestra todos los clientes que tienen un estado de **IGNORED**, **COMPLIANT** o **FAILED**.

- **IGNORED**: La IP de cliente se ignora en la lista de IP (es decir, el cliente puede estar exento de verificación).
- **COMPLIANT**: El cliente ha pasado la verificación (es decir, el cliente es compatible con la política).
- **FAILED**: El cliente ha fallado en la verificación (es decir, el cliente no es compatible con la política y se necesita una acción de administración).

Para determinar el motivo de la anomalía, ejecute el mandato **psconf** con la IP de cliente que ha fallado:

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

Referencia relacionada:

"Mandato psconf" en la página 175

Actualización del cliente de Trusted Network Connect

El servidor de Trusted Network Connect (TNC) verifica un cliente y actualiza la base de datos con el estado del cliente y el resultado de la verificación. El administrador puede ver los resultados y tomar medidas para actualizar el cliente.

Para actualizar un cliente que está en un nivel anterior, especifique el mandato siguiente:

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

Por ejemplo:

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

El mandato **psconf** actualiza el cliente con la compilación y las instalaciones APAR si no están instaladas.

Para actualizar el cliente con paquetes abiertos:

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

Referencia relacionada:

"Mandato psconf" en la página 175

Gestión de políticas de gestión de parches

El mandato **pmconf** se utiliza para configurar las políticas de gestión de parches.

Las políticas de gestión de parches proporcionan información, como por ejemplo la dirección IP del servidor de TNC y el intervalo de tiempo para iniciar una actualización SUMA.

Para gestionar la política de gestión de parches, especifique el mandato siguiente:

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

Por ejemplo:

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

Nota: Los puertos `pmport` y `tncserver` deben ser diferentes.

Referencia relacionada:

"Mandato pmconf" en la página 171

Importación de certificados de Trusted Network Connect

Conozca el procedimiento para importar un certificado y transmitir de forma segura los datos en la red.

Los daemons de Trusted Network Connect (TNC) se comunican a través de los canales cifrados habilitados utilizando el protocolo de TLS (Seguridad de la capa de transporte) o SSL (Capa de sockets seguros). Este daemon asegura que los datos y mandatos que se transportan en la red se autentican y sean seguros. Cada sistema tiene su propia clave y certificado, que se generan cuando se ejecuta el mandato de inicialización para los componentes. Este proceso es transparente para el administrador y requiere menos intervención del administrador. Cuando se está verificando un cliente por primera vez, su certificado se importa a la base de datos del servidor. El certificado se marca como no fiable inicialmente y el administrador utiliza el mandato **psconf** para ver y marcar el certificado como fiables especificando el mandato siguiente:

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

Si el administrador desea utilizar una clave y un certificado diferentes, el mandato **psconf** proporciona la característica para importar la clave y el certificado.

Para importar el certificado desde un servidor, especifique el mandato siguiente:

```
psconf import  -S -k <nombre_archivo_clave> -f <nombre_archivo>
```

Para importar el certificado de un cliente, especifique el mandato siguiente:

```
psconf import -C -k <nombre_archivo_clave> -f <nombre_archivo>
```

Referencia relacionada:

| “Mandato psconf” en la página 175

Informes de servidor TNC

El servidor de Trusted Network Connect (TNC) soporta el formato de valores separados por comas (CSV) y el formato de salida de texto para sus vulnerabilidades y exposiciones comunes (CVE), IBM Security Advisory, políticas de servidor de TNC, arreglo de seguridad de cliente de TNC e informes de Service Pack y arreglo temporal registrados.

El informe CVE muestra todas las exposiciones y vulnerabilidades comunes para los Service Pack registrados. Para visualizar los resultados de este informe, escriba el mandato siguiente:

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

El informe de IBM Security Advisory muestra las vulnerabilidades de seguridad conocidas en el software de IBM instalado. Para visualizar los resultados de este informe, escriba el mandato siguiente:

```
psconf report -A <nombre_advertencia>
```

El informe de políticas de servidor de TNC muestra las políticas de seguridad que se aplican en el servidor TNC. Para visualizar los resultados de este informe, escriba el mandato siguiente:

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

El informe de arreglo de cliente de TNC muestra los arreglos temporales instalado y omitidos para el cliente de TNC. Para visualizar los resultados de este informe, escriba el mandato siguiente:

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

También puede ejecutar un informe que genera una lista de Service Pack registrados y los informes de análisis de programa autorizado (APAR) y arreglos temporales relacionados. Para visualizar los resultados de este informe, escriba el mandato siguiente:

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

Para visualizar una lista de paquetes de código abierto registrado, especifique el mandato de informe siguiente:

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

Referencia relacionada:

“Mandato psconf” en la página 175

Resolución de problemas de Trusted Network Connect y Patch Management

Conozca las causas posibles de la anomalía y los pasos para resolver problemas de y del sistema de gestión de parches.

Para resolver problemas de TNC y del sistema de gestión de parches, verifique los valores de configuración que se listan en la tabla siguiente.

Tabla 13. Resolución de problemas de los valores de configuración para los sistemas TNC y Patch Management

Problema	Solución
El servidor de TNC no se inicia o no responde	Complete el siguiente procedimiento: 1. Determine si el daemon de servidor de TNC se está ejecutando especificando el mandato: `ps –eaf | grep tnccsd` 2. Si no se está ejecutando, suprima el archivo `/var/tnc/.tncsock`. 3. Reinicie el servidor. Si esto no resuelve el problema, consulte en el archivo de configuración `/etc/tnccs.conf` la entrada `component = SERVER` en el servidor de TNC.
El servidor de TNC Patch Management no se inicia o no responde	• Determine si el daemon de servidor de TNC Patch Management se está ejecutando especificando el mandato siguiente: `ps –eaf | grep tncpmd` • Consulte en el archivo de configuración `/etc/tnccs.conf` la entrada `component = TNCPM` en el servidor de TNC Patch Management.
El cliente de TNC no inicia o no responde	• Determine si el daemon de cliente de TNC se está ejecutando especificando el mandato siguiente: `ps –eaf | grep tnccsd` • Consulte en el archivo de configuración `/etc/tnccs.conf` la entrada `component = CLIENT` en el cliente de TNC.
El referenciador IP de TNC no se ejecuta en Virtual I/O Server (VIOS)	• Determine si el daemon de referenciador IP de TNC se está ejecutando especificando el mandato siguiente: `ps –eaf | grep tnccsd` • Consulte en el archivo de configuración `/etc/tnccs.conf` la entrada `component = IPREF` en VIOS.
No se puede configurar un sistema como servidor y cliente de TNC	El servidor y el cliente de TNC no se pueden ejecutar simultáneamente en el mismo sistema.
Los daemons se están ejecutando pero no se produce la verificación	Habilite los mensajes de registro para la daemons. Establezca el registro `level=info` en el archivo `/etc/tnccs.conf`. Puede analizar los mensajes de registro.

Interfaz gráfica de usuario (GUI) de PowerSC

Esta sección describe la Interfaz gráfica de usuario (GUI) de PowerSC de IBM que incluye información sobre cómo instalar, mantener y utilizar la interfaz.

La GUI de PowerSC de IBM mejora la usabilidad del producto PowerSC Standard Edition proporcionando una alternativa a la interacción de línea de mandatos y archivo de registro. La GUI de PowerSC proporciona una consola de gestión centralizada para la visualización de puntos y su estado, aplicar, deshacer o comprobar los niveles de conformidad, agrupar sistemas para la aplicación de acciones de nivel de conformidad y ver y personalizar los perfiles de configuración de conformidad.

La GUI de PowerSC también incluye FIM (File Integrity Monitoring - Supervisión de integridad de archivos). FIM incluye RTC (Real Time Compliance - Conformidad en tiempo real) y TE (Trusted Execution). Mediante el uso de la GUI de PowerSC, puede configurar RTC y TE y ver sucesos de tiempo real. La GUI de PowerSC también proporciona amplias posibilidades de informe y edición de perfiles.

Conceptos sobre la GUI de PowerSC

Antes de utilizar la GUI de PowerSC, debe conocer los conceptos generales relacionados con la seguridad y el descubrimiento de punto final.

Seguridad de la GUI de PowerSC

La GUI de PowerSC proporciona seguridad utilizando la comunicación HTTPS bidireccional entre el servidor de GUI de PowerSC y los agentes de GUI de PowerSC en cada uno de los puntos finales de AIX.

El proceso de conformidad de conexión de TLS utiliza certificados que están disponibles en el servidor de GUI de PowerSC y los agentes de GUI de PowerSC. El proceso de conformidad de conexión de TLS soporta la autenticación única en ambas direcciones porque el agente de GUI de PowerSC o el servidor de GUI de PowerSC puede iniciar la comunicación. El agente crea un nonce, que es un número aleatorio, que se envía al servidor de GUI de PowerSC durante la primera conexión. Entonces el servidor de GUI de PowerSC incluye este nonce con cada mandato que se envía a ese agente. Este nonce proporciona otra capa de confirmación al agente de punto final que está ejecutando un mandato que se ha originado en el servidor de GUI de PowerSC auténtico. El punto final debe asegurarse de que el origen de la llamada de servicio web es fiable. El conocimiento inicial y el nonce garantizan la confianza.

Toda la comunicación entre los agentes de la GUI de PowerSC y el servidor de la GUI de PowerSC se cifra utilizando protocolos y suites de cifrado que sean coherentes con los requisitos de seguridad de los sistemas protegidos. Actualmente, el nivel de protocolo es TLS 1.2. El servidor de GUI de PowerSC interactúa con todos los agentes de GUI de PowerSC y con todos los usuarios de GUI de PowerSC. Por lo tanto, el servidor de GUI de PowerSC debe tener un certificado que sea fiable para todas las conexiones de los navegadores web del usuario. Por ejemplo, los certificados de una autoridad conocida públicamente como Verisign o de una autoridad de certificados de confianza interna.

Durante la instalación, el servidor de GUI de PowerSC crea un certificado autofirmado para su propio uso. Este certificado puede utilizarse indefinidamente, pero está destinado a utilizarse temporalmente y puede reemplazarse por un certificado reconocido ampliamente proporcionado por el usuario. La instalación de servidor de GUI de PowerSC también crea un certificado para firmas que se utiliza para firmar todos los certificados de punto final.

El proceso de instalación crea automáticamente un archivo de almacén de confianza para cada punto final. El archivo de almacén de confianza es el mismo para cada punto final y debe copiarse del servidor

de GUI de PowerSC en cada punto final. Esta combinación de certificados en el servidor de GUI de PowerSC y los puntos finales proporciona un alto nivel de seguridad de comunicación.

Se proporciona más control de seguridad utilizando grupos de UNIX. Cualquier usuario, como un usuario LDAP o un usuario local definido por el sistema operativo debe ser un miembro de un grupo UNIX especificado para iniciar la sesión en la GUI de PowerSC. El administrador puede establecer o cambiar la pertenencia a grupo utilizando el mandato **pscuiserverctl**.

Después de haber iniciado la sesión, puede que todavía esté restringido a la modalidad de sólo vista. Puede utilizar la función de autoridad de usuario para realizar acciones en puntos finales controlados por la pertenencia a grupos de UNIX. Para realizar cualquier acción, debe ser un miembro de un grupo UNIX que tenga permiso para gestionar el punto final. Para obtener más información, consulte el tema Especificación de los grupos que tienen acceso.

De forma predeterminada, cualquier usuario que sea miembro del grupo de seguridad puede gestionar cada punto final que sea visible en la GUI de PowerSC. El administrador de PowerSC puede restringir el acceso de usuario al nivel de punto final individual utilizando el mandato **setGroups.sh**.

Hay diversos mandatos de configuración que sólo puede ejecutar un usuario administrativo. Los ejemplos incluyen la posibilidad de cambiar los valores de correo electrónico globales o de crear un nuevo perfil. La autoridad de usuario administrativo se establece utilizando grupos de UNIX y puede configurarse utilizando el mandato **pscuiserverctl**.

Cómo llenar el contenido de punto final en la página de conformidad

El servidor de la GUI de PowerSC y el agente de la GUI de PowerSC se comunican con el punto final para descubrir el nivel de conformidad.

Tras el arranque, y de forma intermitente hasta que se realice satisfactoriamente, el agente intenta iniciar el contacto con el servidor de GUI de PowerSC. Cuando se establece contacto, se realiza un conocimiento de seguridad de servidor-agente de una sola vez. Después de que el conocimiento de seguridad de agente a servidor se haya negociado correctamente la primera vez, el servidor crea un elemento de dominio con un identificador exclusivo (UID) para la representación interna del punto final y pasa el UID de nuevo al punto final. Entonces el UID se incluye con la comunicación del agente al servidor. Esta acción finaliza el proceso de descubrimiento. El servidor de la GUI de PowerSC y el punto final pueden comunicarse de forma segura en cualquiera de las direcciones.

Después de completar el reconocimiento de descubrimiento inicial o después de que el agente de la GUI de PowerSC se haya reiniciado, el agente de la GUI de PowerSC intenta determinar la información de estado de conformidad actual para el punto final y actualiza el servidor de la GUI de PowerSC. La existencia del punto final y de la información de conformidad actual se utiliza para llenar la página de estado de conformidad de la GUI de PowerSC. Si no se puede determinar información de estado de conformidad, la entrada no está disponible en la página de estado de conformidad.

El servidor de la GUI de PowerSC contiene una representación de todos los puntos finales conocidos, que se crean automáticamente como resultado de conexión y comunicación iniciales de agente y servidor. A medida que los agentes de punto final realizan el seguimiento de los cambios en el estado de conformidad del punto final, los cambios se pasan al servidor y se retienen. Toda la interacción del usuario desde la GUI de PowerSC con un punto final se realiza a través del servidor de la GUI de PowerSC. La interfaz de usuario no interactúa directamente con ningún punto final o agente de punto final.

Instalación de la GUI de PowerSC

Los agentes de la GUI de PowerSC y los componentes de servidor de la GUI de PowerSC se instalan durante la instalación de PowerSC Standard Edition. Cada uno se instala desde los conjuntos de archivos `installp`.

Agente de la GUI de PowerSC

El agente de la GUI de PowerSC se instala en cada punto final AIX. El agente de la GUI de PowerSC rastrea la actividad en el punto final y proporciona esa información al servidor de la GUI de PowerSC.

El agente de la GUI de PowerSC también ejecuta los mandatos que se desencadenan desde la GUI de PowerSC. Todas las comunicaciones entre los agentes de la GUI de PowerSC y el servidor de la GUI de PowerSC servidor están cifradas.

El mandato `installp` instala el producto PowerSC Standard Edition básico y el agente de GUI de PowerSC. Se utiliza el conjunto de archivos `powerscStd.uiAgent.rte` para la instalación de agente de GUI de PowerSC. El ejemplo siguiente muestra el mandato `installp` que se ejecuta en cada punto final:

Nota: En el ejemplo siguiente, las imágenes de instalador se expanden en el directorio `/tmp/inst.images/`.

```
#installp -agXYd /tmp/inst.images powerscStd.ice powerscStd.license powerscStd.uiAgent.rte
```

Servidor de la GUI de PowerSC

El servidor de la GUI de PowerSC puede ejecutarse en cualquier sistema AIX, se recomienda que cree una LPAR de AIX dedicada en la que instalar y ejecutar le servidor de la GUI de PowerSC.

El mandato **installp** instala el producto PowerSC Standard Edition básico y el servidor de GUI de PowerSC. El conjunto de archivos `powerscStd.uiServer.rte` de **installp** se utiliza para la instalación de servidor de la GUI de PowerSC. El ejemplo siguiente visualiza el mandato **installp** que se ejecuta en un punto final:

Nota: En el ejemplo siguiente, las imágenes de instalador se expanden en el directorio `/tmp/inst.images/`.

```
#installp -agXYd /tmp/inst.images powerscStd.ice powerscStd.license powerscStd.uiServer.rte
```

Requisitos de la GUI de PowerSC

Conozca los requisitos de hardware y software para la GUI de PowerSC.

Hardware

- Los componentes de servidor de la GUI de PowerSC debe instalarse en una LPAR independiente o una máquina virtual que ejecute o AIX 7.1 o posterior.
- Los componentes de agente de la GUI de PowerSC deben instalarse en cada punto final AIX.

Software

- El servidor de GUI de PowerSC necesita AIX 7.1 o posterior.
- El servidor de GUI de PowerSC necesita que el daemon sendmail esté en ejecución.
- El conjunto de archivos `bos.loc.utf.<LANG>` debe estar instalado para que la GUI de PowerSC visualice correctamente las descripciones de regla de perfil en idiomas que no sean el inglés.

Distribución del certificado de seguridad de almacén de confianza en los puntos finales

Los administradores de sistema deben desplegar el certificado de seguridad de almacén de confianza en todos los puntos finales.

Durante la instalación, se crea un archivo de almacén de confianza que todos los puntos finales pueden utilizar. El nombre del archivo es `endpointTruststore.jks`. El archivo se coloca en el directorio `/etc/security/powersc/uiServer/`.

Después de la instalación, debe colocar el archivo `endpointtruststore.jks` en cada punto final para el agente de la GUI de PowerSC en ese punto final para establecer contacto con el servidor de la GUI de PowerSC e iniciar el proceso que da lugar a la creación del almacén de claves en el punto final.

Puede distribuir el archivo de almacén de confianza de una de las siguientes maneras:

- Copie manualmente el archivo `endpointTruststore.jks` en cada punto final.
- Si se utiliza PowerVC (u otro gestor de virtualización) en el entorno, el archivo `endpointTruststore.jks` puede ponerse en la imagen de PowerVC. Cuando la imagen de PowerVC se despliega en un punto final, se incluyen el agente de la GUI de PowerSC y el archivo de almacén de confianza.

Una vez que `endpointTruststore.jks` se haya desplegado utilizando uno de los métodos y cuando un punto final empieza a ejecutarse, el agente de la GUI de PowerSC utiliza el archivo de almacén de confianza para determinar la ubicación donde se está ejecutando el servidor de la GUI de PowerSC. El agente de la GUI de PowerSC envía entonces un mensaje al servidor de GUI de PowerSC con una solicitud para unirse a la lista de puntos finales disponibles y supervisados.

Copia manual del archivo de almacén de confianza en puntos finales

Los administradores de sistema deben copiar manualmente el archivo de almacén de confianza en cada punto final existente en el entorno.

El archivo de almacén de confianza también debe copiarse en cada punto final nuevo que se añade.

Nota: Si tiene un gestor de virtualización de datos como PowerVC, puede copiar el archivo de almacén de confianza en un nuevo punto final creando una imagen que contiene el agente de GUI de PowerSC y el archivo de almacén de confianza. Consulte “Copia del archivo de almacén de confianza en puntos finales utilizando un gestor de virtualización” en la página 149.

1. Para copiar el almacén de confianza de punto final `/etc/security/powersc/uiServer/endpointTruststore.jks` en el archivo `/etc/security/powersc/uiAgent/endpointTruststore.jks` en cada punto final, ejecute el siguiente mandato **scp**:

   ```
   # scp endpointTruststore.jks user@endpoint-host-name:
                          /etc/security/powersc/uiAgent
   ```

2. Para reiniciar los agentes de punto final después de instalar el certificado de seguridad, ejecute los mandatos siguientes en el punto final:

   ```
   stopsrc -s pscuiagent
   startsrc -s pscuiagent
   ```

3. Repita los pasos 1 y 2 para cada punto final existente y para cada punto final nuevo (si no tiene un gestor de virtualización de datos).

Copia del archivo de almacén de confianza en puntos finales utilizando un gestor de virtualización

Los administradores del sistema pueden utilizar un gestor de virtualización como PowerVC para copiar el archivo de almacén de confianza en cada nuevo punto final utilizando una imagen que contiene el agente PowerSC y el archivo de almacén de confianza.

1. Copie el archivo `/etc/security/powersc/uiServer/endpointTruststore.jks` de almacén de confianza de punto final en la imagen de PowerVC.
2. Despliegue la imagen de PowerVC en cada nuevo punto final que se añada al sistema.

Configuración de cuentas de usuario

De forma predeterminada, cualquier usuario, tanto si es un usuario LDAP o un usuario local definido por el sistema operativo, debe ser miembro del grupo de seguridad para iniciar la sesión en la GUI de PowerSC.

El administrador puede cambiar esta pertenencia a grupo necesaria utilizando el mandato **pscuiserverctl**. Después de iniciar la sesión en la GUI de PowerSC, un usuario sólo puede ver el estado de los puntos finales si la cuenta de usuario es miembro de un grupo de UNIX al que se permite gestionar el punto final. El administrador puede cambiar los valores de cuenta de usuario para el nivel de punto final individual utilizando el mandato **setGroups.sh**.

Tenga en cuenta los siguientes puntos:

- Existe una relación de muchos a muchos entre los puntos finales y los grupos AIX:
  - Un grupo de AIX puede asociarse con muchos puntos finales.
  - Un punto final puede asociarse con muchos grupos de AIX.
- Después de que un usuario haya iniciado la sesión en la GUI de PowerSC, se utilizan asociaciones de grupo para determinar si se permite que un usuario ejecute mandatos en puntos finales específicos o si se permite que el usuario sólo se vea el estado de punto final.
  - Para ejecutar mandatos en un punto final específico utilizando la GUI de PowerSC, el usuario debe estar asociado con uno de los grupos que está asociado con el punto final.
  - La pertenencia a grupo del usuario se compara con el conjunto de grupos que están asociados con cada punto final. Si la pertenencia a grupo del usuario coincide con grupos que están asociados con cada punto final, se permite al usuario ejecutar mandatos como **Aplicar perfiles**, **Deshacer** y **Comprobar** en ese punto final. Si la pertenencia a grupo del usuario no coincide con ningún grupo que esté asociado con cada punto final, el usuario puede ver sólo el estado de ese punto final.

Los siguientes scripts de shell están disponibles en el servidor de GUI de PowerSC en el directorio `/opt/powersc/uiServer/bin/`.

Tabla 14. Scripts de shell de grupo

Script de shell	Descripción
`pscuiserverctl`	Especifica un grupo (UNIX) de inicio de sesión de AIX del que debe ser miembro un usuario para iniciar la sesión en la GUI de PowerSC. El usuario sólo necesita ser miembro de uno de los grupos.
`setGroups.sh`	Especifica uno o varios grupos AIX de los que un usuario debe ser miembro para ejecutar mandatos en puntos finales específicos.

Ejecución de mandatos y scripts de configuración de grupo

Los administradores de sistema deben ejecutar el mandato **pscuiserverctl** y el script **setGroups** para especificar a qué grupos de sistema operativo se les permite iniciar la sesión en la GUI de PowerSC, realizar funciones de administrador y ejecutar mandatos en puntos finales específicos.

1. En el servidor de GUI de PowerSC, cambie el directorio a `/opt/powersc/uiServer/bin/`.
2. Ejecute el mandato siguiente para especificar el grupo de AIX del que un usuario debe ser miembro para iniciar la sesión en la GUI de PowerSC. El grupo que especifique se graba en el archivo `/etc/security/powersc/uiServer/uiServer.conf`.

   ```
   pscuiserverctl set logonGroupList abp,security
   ```

   Consejo: Antes de ejecutar el mandato, puede utilizar el mandato **groups** *nombre_usuario* para ver los grupos de los que el usuario es miembro.
3. Ejecute el mandato siguiente para especificar los grupos de UNIX a los que se les permite realizar funciones de administrador utilizando la GUI de PowerSC.

   ```
   pscuiserverctl set administratorGroupList unixgrpadmin1,unixgrpadmin2
   ```
4. Ejecute el script siguiente para especificar los grupos de AIX de los que un usuario debe ser miembro para ejecutar mandatos en puntos finales específicos. Debe proporcionar los nombres de host completos de los puntos finales. Los grupos que especifique se graban en el archivo `/etc/security/powersc/uiServer/groups.txt`.

   ```
   ./setGroups.sh nombre_grupo "lista_separada_por_comas_de_nombres_de_host_de_punto_final"
   ```

   Nota: Se soportan caracteres comodín limitados al buscar puntos finales. Por ejemplo, las especificaciones siguientes son válidas para especificar todos los puntos finales que tienen un nombre que empieza por "Boston_" o finaliza por ".rs.com":
   - ./setGroups.sh groupname "Boston_*"
   - ./setGroups.sh groupname "*.rs.com"

   Consejo: Un asterisco (*) es el único carácter comodín soportado para este mandato. Sólo puede utilizarse al principio o al final de una serie.

Utilización de la GUI de PowerSC

Puede utilizar la GUI de PowerSC para ver los puntos finales que se descubren en el sistema, crear grupos personalizados, crear perfiles personalizados, copiar perfiles personalizados para puntos finales y aplicar perfiles. También puede verificar la comunicación entre los puntos finales y el servidor de GUI de PowerSC y detener la comunicación entre un punto final y el servidor de la GUI de PowerSC.

La página principal de la GUI de PowerSC contiene las siguientes secciones:

- Bandeja **Grupos**: lista los grupos que están definidos para el entorno. Los grupos son colecciones de puntos finales que se agrupan basándose los elementos en común. El grupo **Todos los sistemas** se crea automáticamente cuando se descubren los puntos finales del entorno. Puede crear grupos personalizados. Por ejemplo, puede crear un grupo de puntos finales cuyo elemento en común sea HIPPA.
- La página **Conformidad** incluye tres secciones:
  - El panel superior muestra información estadística sobre el grupo seleccionado en la bandeja **Grupos**. La información estadística muestra los resultados de los últimos niveles de conformidad que se han aplicado a los puntos finales del grupo seleccionado. Para el grupo seleccionado, puede ver el porcentaje de aprobaciones y anomalías de sistema, el número total de reglas que se han comprobado y las reglas específicas que han fallado.
  - El panel central es una barra de tareas que se puede utilizar para realizar acciones en uno o varios puntos finales. Puede aplicar, deshacer o comprobar un nivel de conformidad.
  - El panel inferior muestra una tabla que incluye todos los puntos finales o un grupo de puntos finales que están disponibles en el entorno. La tabla incluye la siguiente información para cada punto final:
    - Nombre de sistema
    - Tipo de regla de conformidad

- Hora y fecha en que se ha aplicado el nivel de conformidad al punto final
- Hora y fecha en que se ha comprobado el nivel de conformidad en el punto final
- Estado de nivel de conformidad
- Número de reglas en el punto final que han fallado
- Número de reglas en el punto final que han pasado satisfactoriamente durante la comprobación de nivel de conformidad

• La página **Seguridad** incluye dos secciones:
  – El panel superior muestra información de seguridad en tiempo real en el grupo de puntos finales que ha seleccionado en la bandeja **Grupos**. Para el grupo seleccionado, puede ver el número total de sucesos de Conformidad en tiempo real (RTC), el número total de sucesos de Trusted Execution (TE), el porcentaje de puntos finales que están actualizados con los parches de TNC, el porcentaje de puntos finales que tienen instalado el Arranque fiable, el número de puntos finales que tienen instalado el Cortafuegos fiable y el porcentaje de puntos finales que tienen instalado el Registro fiable.
  – El panel inferior muestra una tabla que incluye los puntos finales de sistema en el grupo. La tabla incluye la siguiente información para cada punto final:
    - Nombre del punto final de sistema
    - Indicadores de suceso de integridad de archivo
    - Estado de activación de RTC
    - Estado de activación de TE
    - Estado de parche de TNC actualizado
• La página **Informes** incluye informes de integridad de archivo y conformidad. Se incluyen informes de visión general y de detalle.
• La página **Editor de perfiles** incluye tres secciones:
  – El panel superior tiene un menú desplegable que lista los perfiles incorporados y personalizados disponibles
  – El panel central es una barra de tareas que puede utilizarse para suprimir perfiles, crear perfiles nuevos y copiar perfiles en puntos finales que forman parte de un grupo.
  – El panel inferior muestra una tabla que incluye todas las reglas que se incluyen en el perfil seleccionado. Para cada regla se visualiza la siguiente información:
    - Nombre de regla de conformidad
    - Tipo de regla de conformidad
    - Descripción de la regla

Especificación del idioma de la GUI de PowerSC

La GUI de PowerSC puede representarse en distintos idiomas.

Para seleccionar el idioma para la GUI de PowerSC, pulse el icono **Idiomas y valores** en la barra de menús de la página principal. El idioma actual utilizado para representar la interfaz se muestra en el menú. Para cambiar el idioma, pulse el icono asociado. Seleccione el idioma para la sesión en la lista de idiomas disponibles.

Navegación en la GUI de PowerSC

En la GUI de PowerSC puede configurar y administrar la comunicación de punto final y servidor, organizar y agrupar puntos finales, supervisar y aplicar niveles y perfiles de conformidad incorporados y personalizados, supervisar y configurar la seguridad de punto final y generar y distribuir informes sobre una base planificada.

1. Abra la GUI de PowerSC. La GUI de PowerSC muestra la página de inicio.

2. Para administrar la comunicación de punto final y servidor, pulse el icono **Idiomas y valores** en la barra de menús de la página principal. Pulse el icono **Administración de puntos finales** para verificar o detener la comunicación entre los puntos finales y el servidor de GUI de PowerSC. Para obtener más información, consulte "Administración de la comunicación de punto final y servidor".
3. Pulse la elipse de línea horizontal en el panel de navegación de las páginas de conformidad o seguridad para abrir el Editor de grupos. Mediante el Editor de grupos puede crear grupos personalizados de puntos finales. Para obtener más información, consulte "Creación de grupos personalizados" en la página 154.
4. Para crear perfiles de conformidad personalizados y copiar perfiles en puntos finales, pulse la pestaña **Editor de perfiles**. Para obtener más información, consulte "Trabajo con perfiles de conformidad" en la página 155.
5. Para supervisar y aplicar niveles y perfiles de conformidad incorporados y personalizados, pulse la pestaña **Conformidad**. Para obtener más información, consulte Aplicación de niveles y perfiles de conformidad.
6. Para supervisar y configurar la seguridad de punto final, pulse la pestaña **Seguridad**. Para obtener más información, consulte Supervisión de seguridad de punto final.
7. Para generar y distribuir informes a petición o de forma planificada, pulse la pestaña **Informes**. Para obtener más información, consulte Trabajar con informes.

Administración de la comunicación de punto final y servidor

Desde la página **Administración de puntos finales**, puede verificar o detener la comunicación entre los puntos finales y el servidor de GUI de PowerSC. También puede verificar y generar solicitudes de almacén de claves.

Verificación de la comunicación de punto final y servidor

Puede verificar la comunicación entre los puntos finales descubiertos y el servidor de GUI de PowerSC.

1. Pulse el icono **Idiomas y valores** en la barra de menús de la página principal. Pulse **Administración de punto final**. Se abre la página de administración de punto final.
2. En la bandeja **Grupos**, seleccione el grupo que incluye los puntos finales que desea verificar. Los puntos finales para ese grupo se listan en la tabla de puntos finales.
3. Todos los puntos finales del sistema para un grupo seleccionado se visualizan en la tabla de conformidad. Puede filtrar los puntos finales que se visualizan utilizando el campo **Filtrado por texto**. Escriba el texto por el que desea filtrar en el campo y pulse Intro. La lista de puntos finales del grupo seleccionado se filtra dinámicamente para mostrar sólo las filas que contienen el texto.
4. Para renovar la información de estado visualizada, pulse **Renovar tabla**.
5. Seleccione el recuadro de selección asociado para cada punto final que desea verificar.
6. Pulse el icono **Verificar**.
7. Un mensaje de confirmación sobre la conexión válida se muestra en las columnas **Verificado** y **Diagnóstico de conectividad**.

Eliminación de puntos finales de la supervisión de la GUI de PowerSC

Cuando un punto final se descubre, se supervisa continuamente. Si se elimina el punto final del entorno, también debe eliminarlo del servidor de la GUI de PowerSC.

Para eliminar puntos finales de la supervisión en la GUI de PowerSC, realice los pasos siguientes:

1. Pulse el icono **Idiomas y valores** en la barra de menús de la página principal. Pulse **Administración de punto final**. Se abre la página de administración de punto final.
2. En la bandeja **Grupos**, seleccione el grupo que incluye los puntos finales que desea eliminar. Los puntos finales para ese grupo se listan en la tabla de puntos finales.

3. Todos los puntos finales del sistema para un grupo seleccionado se visualizan en la tabla de conformidad. Puede filtrar los puntos finales que se visualizan utilizando el campo **Filtrado por texto**. Escriba el texto por el que desea filtrar en el campo y pulse Intro. La lista de puntos finales del grupo seleccionado se filtra dinámicamente para mostrar sólo las filas que contienen el texto.
4. Para renovar la información de estado visualizada, pulse **Renovar tabla**.
5. Seleccione el recuadro de selección asociado para cada punto final que desea dejar de supervisar.
6. Pulse el icono **Suprimir**.
7. Se visualiza un mensaje de confirmación sobre la supresión del punto final en las columnas **Indicación de fecha y hora verificada** y **Diagnóstico de conectividad**.

Verificación y generación de solicitudes de almacén de claves

Para cada punto final debe verificar que una solicitud de almacén de claves es válida y, si es válida, puede generar un almacén de claves para el punto final.

La primera vez que un punto final empieza a ejecutarse, el agente de la GUI de PowerSC utiliza el archivo de almacén de claves para determinar dónde se ejecuta el servidor de GUI de PowerSC. Entonces el agente de GUI de PowerSC envía un mensaje al servidor de GUI de PowerSC con una solicitud para unirse a la lista de puntos finales supervisados disponibles.

Mediante el uso de la página **Solicitudes de almacén de claves** del **Administrador de punto final** puede verificar que una solicitud de almacén de claves es válida y, si es válida, puede generar un almacén de claves para el punto final.

1. Pulse el icono **Idiomas y valores** en la barra de menús de la página principal. Pulse **Administración de punto final**. Se abre la página de administración **Punto final - Todos los sistemas**.
2. Cada punto final conocido se lista en la columna **Nombre de sistema**. Pulse **Solicitudes de almacén de claves** para verificar si hay solicitudes de almacén de claves pendientes. Se abre la página **Solicitudes de almacén de claves** de **Administración de punto final**.
3. Las solicitudes de almacén de claves para todos los servidores nuevos o añadidos se listan en la columna **Nombre de host**. Tras confirmar que desea ampliar un almacén de claves al punto final, seleccione el recuadro de selección para el punto final y pulse **Verificar**.
4. PowerVC realiza la verificación. Especifique el ID de usuario y la contraseña en la ventana **Credenciales de PowerVC necesarias**. Pulse **Aceptar**. Si no tiene PowerVC, omita este paso y el siguiente.

   Nota: La verificación es el proceso mediante el cual se utilizan las API de Openstack para comprobar si PowerVC es consciente del punto final recién declarado. Si PowerVC no está presente en el entorno de usuario o si powervcKeystoneUrl no se ha configurado correctamente (utilizando pscuiserverctl), PowerSC no podrá verificar el punto final.
5. Tras la verificación, se visualiza un mensaje como texto contextual en la columna **Nombre de host**. El mensaje confirma si PowerVC reconoce el nuevo punto final. Según la información del mensaje, puede elegir generar el almacén de claves.
6. Para generar el almacén de claves, pulse **Generar almacén de claves**. La fila de punto final de la tabla parpadea mientras se genera el almacén de claves. Tras la finalización, el valor de la columna **Almacén de claves generado** cambia de **no** a **yes**.

   Nota: Si no ha verificado el punto final utilizando PowerVC, se visualiza un mensaje preguntando si desea continuar con la verificación. Pulse **Continuar** si reconoce el punto final y si desea generar el almacén de claves.

   El agente PowerSC puede tardar unos minutos en descubrir que se ha generado el almacén de claves. Después de que el agente haya instalado el almacén de claves, el nuevo punto final se lista como un punto final totalmente gestionado en las páginas **Administración de punto final - todos los sistemas**, **Conformidad**, **Seguridad** e **Informes** de la GUI de PowerSC.

7. Si no desea generar un almacén de claves para el punto final, puede eliminar la solicitud. Seleccione el recuadro de selección para el punto final que desea eliminar y pulse el icono **Suprimir**.
8. Se visualizan todos los puntos finales que esperan la verificación de almacén de claves en la tabla de punto final. Puede filtrar los puntos finales que se visualizan utilizando el campo **Filtrado por texto**. Escriba el texto por el que desea filtrar en el campo y pulse **Intro**. La lista de puntos finales se filtra dinámicamente para mostrar sólo las filas que contienen el texto.
9. Para renovar la información de tabla de punto final, pulse **Renovar tabla**.

Organización y agrupación de puntos finales

Los administradores de sistema pueden organizar y agrupar puntos finales basándose en alguna propiedad común. Se pueden definir grupos personalizados que pueden contener un conjunto seleccionado explícitamente de puntos finales que se gestionan utilizando la GUI de PowerSC.

Por ejemplo, si tiene 3 - 4 entornos, es aconsejable crear grupos que contengan puntos finales de producción, puntos finales de prueba y puntos finales de control de calidad.

Durante la instalación se crea un grupo predeterminado que se denomina **Todos los sistemas**. Este grupo contiene todos los puntos finales que se han descubierto en el entorno.

Creación de grupos personalizados

Puede crear un grupo personalizado con una lista de puntos finales enumerada seleccionada explícitamente.

1. En la bandeja **Grupos** seleccione **Crear nuevo grupo**. Se abre la bandeja **Se está creando un grupo nuevo**. Si la bandeja **Grupos** no se expande, pulse la elipse de línea horizontal en el panel izquierdo de la página principal de la interfaz.
2. Especifique un nombre exclusivo para el nuevo grupo y pulse Intro. El nuevo grupo se añade a la bandeja **Grupos**.
3. Añada los sistemas que desea incluir en este grupo. En la lista **Todos los sistemas** de sistemas de punto final disponibles, seleccione los sistemas que desea incluir en el grupo. Pulse la flecha derecha para mover todos los sistemas seleccionados al nuevo grupo. Para eliminar sistemas de punto final del grupo, resalte el punto final en la nueva lista de grupos y pulse la flecha izquierda.
4. Después de añadir o eliminar miembros de grupo, guarde los cambios pulsando el icono **Guardar** en la barra de menús del panel de contenido.
5. Pulse la elipse de línea horizontal para volver a la bandeja **Grupos**. Se lista el nuevo grupo.

Adición o eliminación de sistemas asignados a un grupo existente

Puede añadir o eliminar puntos finales que están asignados a un grupo existente.

1. En la bandeja **Grupos** pulse el elipse a la derecha del grupo en el que desea añadir o del que desea eliminar un sistema de punto final. Si la bandeja **Grupos** no se expande, pulse la elipse de línea horizontal en el panel izquierdo de la página principal de la interfaz.
2. Pulse **Editar grupo**.
3. Para añadir un sistema de punto final al grupo, seleccione el sistema en la lista **Todos los sistemas** y pulse la flecha derecha. El sistema se añade a la lista *NombreGrupo*.
4. Para eliminar un punto final del grupo, seleccione el sistema en la lista **Sistema de grupo** y pulse la flecha izquierda. El sistema se elimina de la lista *nombre_grupo*.
5. Pulse el icono **Guardar cambios de grupo** para guardar los cambios.
6. Para suprimir un sistema del grupo, seleccione el sistema y pulse la flecha izquierda.
7. Para cancelar los cambios en el grupo, pulse **Cancelar cambios de grupo**
8. Pulse la elipse **Grupos** para volver a la bandeja **Grupos**.

Supresión de un grupo

Puede suprimir grupos que ya no son aplicables.

1. En la bandeja **Grupos**, pulse el elipse a la derecha del grupo que desea suprimir. Si la bandeja **Grupos** no se expande, pulse la elipse de línea horizontal en el panel de navegación de la página principal de la interfaz.
2. Pulse **Suprimir grupo**. El grupo se suprime y se elimina de la lista de grupos de la bandeja **Grupos**.

Cómo renombrar un grupo

Puede renombrar un grupo de puntos finales.

1. En la bandeja **Grupos**, pulse la elipse a la derecha del grupo que desea eliminar. Si la bandeja **Grupos** no se expande, pulse la elipse de línea horizontal en el panel de navegación de la página principal de la interfaz.
2. Pulse **Renombrar grupo**. Especifique el nuevo nombre para el grupo en el campo **Nombre de grupo**.

Clonación de un grupo

Puede clonar un grupo para crear un duplicado con los mismos puntos finales y un nuevo nombre.

1. En la bandeja **Grupos**, pulse el elipse a la derecha del grupo que desea suprimir. Si la bandeja **Grupos** no se expande, pulse la elipse de línea horizontal en el panel de navegación de la página principal de la interfaz.
2. Pulse **Clonar grupo**. El grupo se copia y se le asigna un nuevo nombre.

Trabajo con perfiles de conformidad

Mediante el editor de perfiles de la GUI de PowerSC, puede ver los perfiles de conformidad incorporados, crear perfiles personalizados y copiar perfiles en puntos finales de sistema.

El producto PowerSC Standard Edition se entrega con un conjunto de perfiles incorporados que se pueden utilizar para configurar los puntos finales de sistema para que cada punto final cumpla con los estándares de seguridad siguientes:

- Conformidad con Payment Card Industry - Data Security Standard (PCI)
- Conformidad con la ley Sarbanes-Oxley y COBIT (SOX-COBIT)
- Conformidad con US Department of Defense STIG (DoD)
- Health Insurance Portability and Accountability Act (HIPAA)
- Conformidad con North American Electric Reliability Corporation (NERC)

Para obtener más información sobre los perfiles incorporados, consulte el tema “Conceptos sobre la Automatización de la seguridad y conformidad” en la página 9.

Cada uno de los perfiles incorporados incluye reglas que deben aplicarse a un punto final para satisfacer los requisitos de seguridad. Cuando es necesario aplicar sólo un subconjunto o una combinación diferente de estas reglas o personalizar niveles de conformidad, puede crear un perfil personalizado.

En la mayoría de entornos, los administradores con frecuencia editan archivos de conformidad para eliminar las reglas de problemas. Una vez completadas las comprobaciones de compatibilidad, los archivos de reglas de conformidad se considera estables y se despliegan en servidores de producción.

Se puede utilizar la GUI de PowerSC para perfiles personalizados combinando reglas de perfiles incorporados (u otros personalizados).

Visualización de perfiles de conformidad

Puede ver las reglas que se incluyen en cada uno de los perfiles incorporados y personalizados.

1. En la página principal, seleccione la pestaña **Editor de perfiles**. Se abre la página **Editor de perfiles**.
2. Pulse la flecha hacia abajo para abrir la lista de perfiles. El menú desplegable lista los **Perfiles incorporados** y **Perfiles personalizados** que están disponibles.
3. Seleccione el perfil que desea ver. Cada regla incluida en el perfil se visualiza con su nombre, tipo y una descripción. Para obtener más información sobre las reglas, consulte el tema "Conceptos sobre la Automatización de la seguridad y conformidad" en la página 9.
4. Todas las reglas para el perfil seleccionado se visualizan en la tabla de perfiles. Puede filtrar los perfiles que se visualizan utilizando el recuadro **Filtrado por texto**. Escriba el texto por el que desea filtrar en el recuadro de texto. Se renueva la lista de reglas en el perfil seleccionado.

Creación de un perfil personalizado

Puede crear un nuevo perfil que se base en un perfil existente y, a continuación, personalizar el nuevo perfil para incluir sólo un conjunto de reglas específico.

1. En la página principal, seleccione la pestaña **Editor de perfiles**. Se abre la página **Editor de perfiles**.
2. Pulse la flecha hacia abajo para abrir la lista de perfiles. El menú desplegable lista los **Perfiles incorporados** y **Perfiles personalizados** que están disponibles.
3. Seleccione el perfil en el que desea basar el nuevo perfil.
4. Pulse el icono **Crear nuevo perfil**. Se abre la ventana Nombre y tipo de perfil nuevo.
5. Especifique el nombre para el nuevo perfil en el campo **Nombre de perfil**.
6. Especifique el tipo en el campo **Tipo de perfil**. Normalmente el tipo que se especifica identifica el tipo de política incorporada en la que se basa el nuevo perfil más un identificador exclusivo. Por ejemplo PCIxx, SOX-COBITxy, DoDxyz, HIPAAwxyz o NERCabc.
7. Pulse **Confirmar**.
8. Para añadir una regla al perfil personalizado, seleccione la regla en el perfil original en el que está basando el perfil personalizado y pulse la flecha derecha. La regla se añade al nuevo perfil personalizado. Repítalo para cada regla que desea incluir.
9. Para eliminar una regla del perfil personalizado, seleccione la regla en el perfil personalizado y pulse la flecha izquierda. La regla se elimina del nuevo perfil personalizado. Repítalo para cada regla que desea eliminar.
10. Pulse **Guardar** cuando haya terminado de añadir las reglas.

Copia de perfiles en miembros de grupo

Puede copiar perfiles personalizados en un grupo de puntos finales. Después de que el perfil personalizado se haya copiado en el punto final, está disponible para la aplicación en el punto final. También está disponible para la comprobación para verificar si puede aplicarse al punto final sin errores.

1. En la página principal, seleccione la pestaña **Editor de perfiles**. Se abre la página **Editor de perfiles**.
2. Pulse la flecha hacia abajo para abrir la lista de perfiles. El menú desplegable lista los **Perfiles incorporados** y **Perfiles personalizados** que están disponibles.
3. Seleccione el perfil que desea copiar en los miembros de un grupo.
4. Pulse el icono **Copiar perfil en los miembros del grupo**. Se abre la ventana **Copiar** *nombre_perfil* **en**.
5. Cada grupo que ha creado para la organización se lista con un recuadro de selección asociado. Seleccione el recuadro de selección para cada grupo donde desea copiar el perfil seleccionado.
6. Pulse **Copiar**.
7. Para aplicar o comprobar el perfil, vuelva a la página **Conformidad** seleccionando la pestaña **Conformidad**.

Supresión de un perfil personalizado

Puede suprimir perfiles personalizados.

1. En la página principal, seleccione la pestaña **Editor de perfiles**. Se abre la página **Editor de perfiles**.
2. Pulse la flecha hacia abajo para abrir la lista de perfiles. El menú desplegable lista los **Perfiles incorporados** y **Perfiles personalizados** que están disponibles.
3. Expanda la lista **Perfiles personalizados**.
4. Seleccione el perfil que desea suprimir.
5. Pulse el icono **Suprimir perfil**. El perfil personalizado que ha seleccionado se suprime.

Administración de niveles y perfiles de conformidad

Los administradores de sistema pueden aplicar, comprobar o deshacer niveles y perfiles de conformidad incorporados y personalizados en varios puntos finales.

La tabla siguiente lista los perfiles predefinidos y niveles de conformidad soportados por PowerSC Standard Edition.

Tabla 15. Perfiles predefinidos y niveles de conformidad soportados por PowerSC Standard Edition

Perfiles	**de administración**
Database	bajo
DoD	medio
DoD_to_AIXDefault	alto
DoDv2	predeterminado
DoDv2_to_AIXDefault	
HIPAA	
NERC	
NERC_to_AIXDefault	
NERCv5	
NERCv5_to_AIXDefault	
PCI	
PCI_to_AIXDefault	
PCIv3	
PCIv3_to_AIXDefault	
SOX-COBIT	

En la página **Conformidad** de la GUI de PowerSC, puede realizar las tareas siguientes:

- Seleccione y aplique un perfil o nivel definido a uno o varios puntos finales.
- Desencadene una operación de deshacer en uno o varios puntos finales.
- Compruebe en un perfil o nivel definido el estado actual de uno o varios puntos finales. La operación de comprobación no produce ningún cambio en el punto final, pero establece el valor **Indicación de fecha y hora comprobada** para indicar cuándo se ha realizado la última comprobación.

Aplicación de niveles y perfiles de conformidad

Puede aplicar un nivel o perfil de conformidad a uno o varios puntos finales de un grupo seleccionado.

1. En la página principal, seleccione la pestaña **Conformidad**. Se abre la página **Conformidad**.
2. En la bandeja **Grupos**, seleccione el grupo que incluya los puntos finales a los que desea aplicar los niveles y perfiles de conformidad.
3. Todos los puntos finales del sistema para un grupo seleccionado se visualizan en la tabla de conformidad. Puede filtrar los puntos finales que se visualizan utilizando el recuadro de texto

Filtrado por texto. Escriba el texto por el que desea filtrar en el recuadro de texto y pulse Intro. La lista de puntos finales del grupo seleccionado se filtra dinámicamente para mostrar sólo las filas que contienen el texto.

4. Para renovar la información de estado visualizada, pulse **Renovar tabla**. Para establecer la frecuencia con la que se renueva automáticamente la pantalla, pulse **Intervalo de renovación**.
5. En la columna **Tipo de regla de conformidad**, puede ver los niveles y perfiles que se han copiado en el punto final asociado. Seleccione el nivel o perfil que desea aplicar al punto final. Compruebe el recuadro de selección asociado.
6. Repita el paso 5 para cada punto final del grupo al que desea aplicar los niveles y perfiles de conformidad.
7. Pulse el icono **Aplicar perfiles**.
8. Los niveles y perfiles de conformidad seleccionados se aplican a cada uno de los puntos finales seleccionados. Si no se pueden aplicar una o más reglas, se considera que han fallado. Si fallan una o más reglas, el punto final se marca con una barra roja y se visualiza el texto **Fallidos** en la columna **Nº reglas fallidas**.
9. En la columna **Nº reglas fallidas** para cada punto final marcado puede ver por qué ha fallado la regla. Puede ajustar las reglas que se aplican creando un perfil personalizado o editando un perfil personalizado.

Cómo deshacer los niveles de conformidad

Puede deshacer el último perfil o nivel de conformidad que se ha aplicado a uno o varios puntos finales de un grupo seleccionado.

Para deshacer los niveles de conformidad, realice los pasos siguientes:

1. En la página principal, seleccione la pestaña **Conformidad**. Se abre la página **Conformidad**.
2. En la bandeja **Grupos**, seleccione el grupo que incluya los puntos finales para los que desea deshacer los perfiles y niveles de conformidad.
3. Se visualizan todos los puntos finales para un grupo seleccionado en la tabla de conformidad. Puede filtrar los puntos finales que se visualizan utilizando el recuadro de texto **Filtrado por texto**. Escriba el texto por el que desea filtrar en el recuadro de texto y pulse Intro. La lista de puntos finales del grupo seleccionado se filtra dinámicamente para mostrar sólo las filas que contienen el texto.
4. Para renovar la información de estado visualizada, pulse **Renovar tabla**. Para establecer la frecuencia con la que se renueva automáticamente la pantalla, pulse **Intervalo de renovación**.
5. Para deshacer un nivel o un perfil que se ha aplicado a un punto final:
   a. Marque el recuadro de selección asociado del punto final.
   b. Pulse el icono **Deshacer**.

Comprobación del último nivel y perfil de conformidad aplicados

Puede comprobar el último nivel o perfil de conformidad que se ha aplicado a uno o varios puntos finales en un grupo seleccionado.

1. En la página principal, seleccione la pestaña **Conformidad**. Se abre la página **Conformidad**.
2. En la bandeja **Grupos**, seleccione el grupo que incluye los puntos finales para los que desea comprobar los niveles y perfiles de conformidad.
3. Se visualizan todos los puntos finales para un grupo seleccionado en la tabla de conformidad. Puede filtrar los puntos finales que se visualizan utilizando el recuadro de texto **Filtrado por texto**. Escriba el texto por el que desea filtrar en el recuadro de texto y pulse Intro. La lista de puntos finales del grupo seleccionado se filtra dinámicamente para mostrar sólo las filas que contienen el texto.
4. Para renovar la información de estado visualizada, pulse **Renovar tabla**. Para establecer la frecuencia con la que se renueva automáticamente la pantalla, pulse **Intervalo de renovación**.

5. Seleccione el recuadro de selección asociado para el nombre de sistema de punto final para el que desea comprobar para el último nivel o perfil que se ha aplicado.
6. Repita el paso 5 en la página 158 para cada punto final en el grupo para el que desea comprobar los niveles y perfiles de conformidad.
7. Pulse el icono **Comprobar**.
8. El punto final se comprueba para ver si se pueden aplicar las reglas que están en el nivel o perfil de conformidad. Los puntos finales no se actualizan. Si no se pueden aplicar reglas, se considera que fallan cuando se aplican. Si fallan una o más reglas, el punto final se marca con una barra roja y se visualiza el texto **Fallidos** en la columna **Nº reglas fallidas**.
9. En la lista **Nº reglas fallidas** para cada punto final marcado, puede ver el mensaje que indica por qué ha fallado la regla. Puede ajustar las reglas que se aplican creando un perfil personalizado.

Comprobación de un nivel o perfil de conformidad que no se ha aplicado

Puede comprobar un nivel o perfil de conformidad que no se ha aplicado a uno o varios puntos finales de un grupo seleccionado.

1. En la página principal, seleccione la pestaña **Conformidad**. Se abre la página **Conformidad**.
2. En la bandeja **Grupos**, seleccione el grupo que incluye los puntos finales para los que desea comprobar el efecto de un nivel o perfil de conformidad.
3. Se visualizan todos los puntos finales para un grupo seleccionado en la tabla de conformidad. Puede filtrar los puntos finales que se visualizan utilizando el recuadro de texto **Filtrado por texto**. Escriba el texto por el que desea filtrar en el recuadro de texto y pulse Intro. La lista de puntos finales del grupo seleccionado se filtra dinámicamente para mostrar sólo las filas que contienen el texto.
4. Para renovar la información de estado visualizada, pulse **Renovar tabla**. Para establecer la frecuencia con la que se renueva automáticamente la pantalla, pulse **Intervalo de renovación**.
5. Seleccione el recuadro de selección asociado para el nombre de sistema de punto final para el que desea comprobar para el último nivel o perfil que se ha aplicado. Puede seleccionar más de un punto final.
6. Abra la lista desplegable **Último tipo comprobado**. Seleccione una de las opciones siguientes:
   - **Todos los niveles disponibles** Muestra una lista de todos los niveles disponibles que puede comprobar en un punto final.
   - **Todos los perfiles disponibles** Muestra una lista de todos los perfiles disponibles que puede comprobar en un punto final.
7. Seleccione el nivel o perfil que desea comprobar en un punto final.
8. Pulse el icono **Comprobar**. Los resultados de la comprobación se devuelven y se listan bajo el punto final.

Envío de notificación de correo electrónico cuando se produce un suceso de conformidad

Desde la página Conformidad, puede enviar una notificación de correo electrónico a uno o varios destinatarios cuando se produce un suceso de conformidad.

1. En la página principal, seleccione la pestaña **Conformidad**. Se abre la página **Conformidad**.
2. Pulse el icono **Valores de correo electrónico** en la parte superior derecha de la barra de menús. Se abre la ventana **Valores de correo electrónico**.
3. Seleccione el recuadro de selección **Enviarme correos electrónicos**.
4. Especifique las direcciones de correo electrónico de cada destinatario separadas por coma en el campo **Direcciones (separadas por coma)**.

Supervisión de la seguridad de punto final

En la página **Seguridad**, puede supervisar la seguridad de punto final en tiempo real.

La página Seguridad visualiza el estado de puntos finales supervisados por Conformidad en tiempo real (RTC) y Trusted Execution (TE).

Tanto RTC, un subcomponente de PowerSC, como TE, un componente de AIX, representan FIM (File Integrity Monitoring - Supervisión de integridad de archivos). FIM supervisa los cambios en los archivos importantes para asegurarse de que los sucesos que afectan a los archivos están autorizados. Los sucesos que pueden repercutir en la seguridad incluyen el cambio inesperado del permiso en un archivo, la actualización del contenido de un archivo o la instalación de una aplicación no planificada. Debe reconocer estos sucesos para asegurar los archivos y aplicaciones importantes.

La página **Seguridad** es la página de supervisión en tiempo real de la GUI de PowerSC. Muestra los sucesos que se generan cuando cambian los archivos supervisados por RTC o TE. Los sucesos incluyen los detalles sobre cuándo ha cambiado el contenido del archivo, cuándo se ha accedido al punto final o cuándo ha cambiado la configuración.

Puede utilizar la página **Seguridad** para realizar las tareas siguientes:

- Ver información de supervisión en tiempo real de RTC y TE
- Configurar RTC y TE para todos los puntos finales
- Ver el estado de otros productos PowerSC en puntos finales
- Activar y desactivar TE

Configuración de Conformidad en tiempo real (RTC)

Desde la página **Seguridad** puede configura el producto Conformidad en tiempo real (RTC) para un punto final específico o un grupo de puntos finales.

1. Pulse la elipse a la derecha del punto final para el que desee editar la configuración de RTC.
2. Pulse **Configurar RTC**. Se abre la ventana Configuración de políticas de RTC.
3. Todas las opciones de configuración de RTC disponibles se listan con una explicación. Para cambiar una o varias de las opciones de configuración de RTC, seleccione o borre el recuadro de selección a la izquierda de la opción. En algunos casos, los cambios en las opciones no se implementan hasta que se reinicia el servidor.
4. Pulse **Guardar**.

Restauración de opciones de configuración de Conformidad en tiempo real (RTC) a una fecha y hora anteriores

Puede restaurar la configuración de RTC a una fecha y hora anteriores.

1. Pulse la elipse a la derecha del punto final para el que desea retrotraer las opciones de configuración de RTC a una versión anterior.
2. Pulse **Retrotraer RTC**. Se listan las indicaciones de fecha y hora para cada versión de configuración de RTC.
3. Pulse la indicación de fecha y hora para la versión de configuración a la que desea revertir. Se restauran las opciones de configuración de RTC que estaban en vigor en esa fecha y hora.

Copia de opciones de configuración de RTC (Real Time Compliance - Conformidad en tiempo real) en otros grupos

Puede copiar las opciones de configuración RTC en otro grupo de puntos finales o en un conjunto específico de puntos finales.

1. Pulse la elipse a la derecha del punto final cuyas opciones de configuración desea copiar en otro grupo de puntos finales o un conjunto específico de puntos finales.
2. Pulse **Copiar configuración de RTC**. Se lista cada grupo de puntos finales que incluye el grupo **Todos los sistemas**.
3. Seleccione el grupo o puntos finales específicos de una de las siguientes formas:
   - Seleccione el recuadro de selección para el grupo de puntos finales en la lista de grupos disponibles. Las opciones de configuración se copian en cada punto final que está en el grupo.
   - Utilice la flecha derecha para expandir un grupo para ver una lista de todos los puntos finales del grupo. Seleccione el recuadro de selección para cada punto final del grupo en el que desea copiar las opciones de configuración.
   - Expanda la lista de puntos finales en el grupo **Todos los sistemas**. Seleccione el recuadro de selección para cada punto final del grupo en el que desea copiar los puntos finales.
4. Pulse **Aceptar**. Las opciones de configuración se copian en el grupo seleccionado o el (los) punto(s) final(es) seleccionado(s).

Edición de la lista de archivos de Conformidad en tiempo real (RTC)

Puede ver y editar las opciones de supervisión de RTC para cada archivo en un punto final.

1. Pulse la elipse a la derecha del punto final que aloja los archivos cuyas opciones de supervisión de RTC desea ver o editar.
2. Pulse **Editar lista de archivos de RTC**. La página **Configuración de la lista de archivos de RTC** se abre listando todos los directorios y archivos que se encuentran en el punto final. Una marca de selección en el icono de carpeta de directorio indica que se están supervisando uno o más archivos en este directorio.
3. Si el archivo cuyas opciones desea editar está en un directorio, efectúe una doble pulsación en el directorio para listar los archivos. Se lista cada uno de los archivos del directorio.
4. Las opciones de supervisión para cada archivo del punto final se listan en las columnas **Contenido** y **Atributos**. Si se supervisan los cambios de contenido en el archivo, el recuadro de selección está seleccionado en la columna **Contenido**. Si se supervisan los cambios de atributo en el archivo, el recuadro de selección está seleccionado en la columna **Atributos**. Para editar las opciones de supervisión, seleccione o borre los recuadros de selección de uno o más archivos en el punto final.
5. Pulse **Guardar**.

Restauración de opciones de supervisión de archivos de Conformidad en tiempo real (RTC) a una configuración anterior

Puede retrotraer a una versión anterior de los archivos que RTC está supervisando.

1. Pulse la elipse a la derecha del punto final para el que desea retrotraer las opciones de supervisión de archivos de RTC a una versión anterior.
2. Pulse **Retrotraer lista de archivos de RTC**. Se listan las indicaciones de fecha y hora para cada versión de configuración de los archivos supervisados.
3. Pulse la indicación de fecha y hora para la versión de configuración de opciones de supervisión a la que desea revertir. Se restauran las opciones de configuración que estaban en vigor para esa fecha y hora.

Copia de opciones de supervisión de lista de archivos de Conformidad en tiempo real (RTC) en otros grupos

Puede copiar las opciones de supervisión de archivo de RTC en otro grupo de puntos finales o en un conjunto específico de puntos finales.

1. Pulse la elipse a la derecha del punto final cuyas opciones de supervisión de archivo que desea copiar en otro grupo de puntos finales o un conjunto específico de puntos finales.

2. Pulse **Copiar lista de archivos de RTC**. Se lista cada grupo de puntos finales que incluye el grupo **Todos los sistemas**.
3. Seleccione el grupo o puntos finales específicos de una de las siguientes formas:
   - Seleccione el recuadro de selección para el grupo de puntos finales en la lista de grupos disponibles. Las opciones de supervisión de lista de archivos se copian en cada punto final que hay en el grupo.
   - Utilice la flecha derecha para expandir un grupo para ver una lista de todos los puntos finales del grupo. Seleccione el recuadro de selección para cada punto final del grupo en el que desea copiar las opciones de supervisión de archivos.
   - Expanda la lista de puntos finales en el grupo **Todos los sistemas**. Seleccione el recuadro de selección para cada punto final del grupo en el que desea copiar los puntos finales.
4. Pulse **Aceptar**. Las opciones de supervisión de archivos se copian en el grupo seleccionado o el (los) punto(s) final(es) seleccionado(s).

Ejecución de una comprobación de Conformidad en tiempo real (RTC)

En la página Seguridad, puede ejecutar una comprobación de la conformidad en tiempo real para verificar si un punto final todavía está en conformidad.

1. Pulse la elipse a la derecha del punto final para el que desea ejecutar una comprobación de Conformidad en tiempo real (RTC).
2. Pulse **Ejecutar comprobación de conformidad**. La página **Conformidad** se abre con la fila de punto final que parpadea para indicar que la selección está en ejecución.
3. Si las reglas no se han podido aplicar, se visualiza un mensaje indicando la anomalía en la columna **Nº reglas fallidas**. Utilice la flecha abajo a la izquierda del punto final para ver la regla que ha fallado.

Configuración de Trusted Execution (TE)

En la página **Seguridad** puede configurar el producto Trusted Execution (TE) para un punto final o grupo de puntos finales específico.

1. Pulse la elipse a la derecha del punto final para el que desee editar las opciones de configuración de TE.
2. Pulse **Configurar TE**. Se abre la ventana Configuración de políticas de TE.
3. Todas las opciones de configuración de TE se listan con una explicación. Para cambiar una o varias de las opciones de configuración de TE, seleccione o borre el recuadro de selección asociado. En algunos casos, los cambios en las opciones no se implementan hasta que se reinicia el servidor.
4. Pulse **Guardar**.

Copia de opciones de Trusted Execution (TE) en otros grupos

Puede copiar las opciones de configuración de TE en otro grupo de puntos finales o en un conjunto específico de puntos finales.

1. Pulse la elipse a la derecha del punto final cuyas opciones de configuración desea copiar en otro grupo de puntos finales o un conjunto específico de puntos finales.
2. Pulse **Copiar configuración de TE**. Se lista cada grupo de puntos finales que incluye el grupo **Todos los sistemas**.
3. Seleccione el grupo o puntos finales específicos de una de las siguientes formas:
   - Seleccione el recuadro de selección para el grupo de puntos finales en la lista de grupos disponibles. Las opciones de configuración se copian en cada punto final que está en el grupo.
   - Expanda un grupo para ver una lista de todos los puntos finales del grupo. Seleccione el recuadro de selección para cada punto final del grupo en el que desea copiar las opciones de configuración.
   - Expanda la lista de puntos finales en el grupo **Todos los sistemas**. Seleccione el recuadro de selección para cada punto final del grupo en el que desea copiar los puntos finales.

4. Pulse **Aceptar**. Las opciones de configuración se copian en el grupo seleccionado o el (los) punto(s) final(es) seleccionado(s).

Edición de la lista el archivos de Trusted Execution (TE)

Puede ver y editar las opciones de supervisión de TE para cada archivo en un punto final.

1. Pulse la elipse a la derecha del punto final que aloja los archivos cuyas opciones de supervisión de TE desea ver o editar.
2. Pulse **Editar lista de archivos de TE**. Se abre la página **Configuración de la lista de archivos de TE** se abre listando todos los directorios y archivos que están en el punto final. Una marca de selección en el icono de carpeta de directorio indica que se están supervisando uno o más archivos en este directorio.
3. Si el archivo cuyas opciones desea ver o editar está en un directorio, efectúe una doble pulsación en el directorio para listar los archivos. Se lista cada uno de los archivos del directorio.
4. Las opciones de supervisión para cada archivo del punto final se listan en las columnas **TE** y **Volátil**. El recuadro de selección está seleccionado en la columna **TE** si se supervisan los cambios de contenido en el archivo. El recuadro de selección está seleccionado en la columna **Volátil** si sólo se supervisan los cambios de permiso en el archivo. Para cambiar las opciones de supervisión, seleccione o borre los recuadros de selección de uno o más archivos en el punto final.
5. Pulse **Guardar**.

Copia de opciones de supervisión de lista de archivos de Trusted Execution (TE) en otros grupos

Puede copiar las opciones de supervisión de archivo de TE en otro grupo de puntos finales o en un conjunto específico de puntos finales.

1. Pulse la elipse a la derecha del punto final cuyas opciones de supervisión de archivo que desea copiar en otro grupo de puntos finales o un conjunto específico de puntos finales.
2. Pulse **Copiar lista de archivos de TE**. Se lista cada grupo de puntos finales que incluye el grupo **Todos los sistemas**.
3. Seleccione el grupo o puntos finales específicos de una de las siguientes formas:
   - Seleccione el recuadro de selección para el grupo de puntos finales en la lista de grupos disponibles. Las opciones de supervisión de lista de archivos se copian en cada punto final que hay en el grupo.
   - Expanda un grupo para ver una lista de todos los puntos finales del grupo. Seleccione el recuadro de selección para cada punto final del grupo en el que desea copiar las opciones de supervisión de archivos.
   - Expanda la lista de puntos finales en el grupo **Todos los sistemas**. Seleccione el recuadro de selección para cada punto final del grupo en el que desea copiar los puntos finales.
4. Pulse **Aceptar**. Las opciones de supervisión de archivos se copian en el grupo seleccionado o el (los) punto(s) final(es) seleccionado(s).

Visualización del estado de otras características PowerSC

En la página Seguridad puede ver el estado de las características de PowerSC Arranque fiable, Cortafuegos fiable y Registro fiable. También puede ver el estado de las actualizaciones de Trusted Network Connect (TNC) en un punto final.

1. En la página principal, seleccione la pestaña **Seguridad**. Se abre la página **Seguridad**.
2. El componente TNC de PowerSC se utiliza para comprobar y actualizar los parches de seguridad en cada punto final. La columna **Actualizar mediante TNC** de la tabla de puntos finales indica si el punto final está actualizado o no desde la perspectiva del servidor de TNC. La sección **Actualizar mediante TNC** en el banner de panel de instrumentos muestra el porcentaje de puntos finales del grupo que están actualizados. Para eliminar la visualización de la información de actualización de TNC de la página **Seguridad**, realice los pasos siguientes:

a. Pulse el icono **Idiomas y valores** en la barra de menús de la página principal.
b. Pulse **Uso de subproducto**.
c. Establezca **Actualizar mediante TNC** en desactivado.
d. Para restablecer la pantalla, deslice **Actualizar mediante TNC** a la posición de activado.

3. La columna **TB** de la tabla final indica si el Arranque fiable de PowerSC está disponible en el punto final. La sección **Arranque fiable** en el banner de panel de instrumentos muestra el porcentaje de puntos finales del grupo seleccionado actualmente que tienen el Arranque fiable de PowerSC activado. Para eliminar la visualización de la información de Arranque fiable de PowerSC de la página **Seguridad**, realice los pasos siguientes:
   a. Pulse el icono **Idiomas y valores** en la barra de menús de la página principal.
   b. Pulse **Uso de subproducto**.
   c. Deslice el conmutador asociado con **Arranque fiable** a la posición de desactivado.
   d. Para restablecer la pantalla, deslice el conmutador a la posición de activado.
4. La columna **TF** de la tabla de punto final indica si el Cortafuegos fiable de PowerSC está disponible en el punto final. La sección **Cortafuegos fiable** en el banner de panel de instrumentos muestra el porcentaje de puntos finales del grupo seleccionado actualmente que tienen el Cortafuegos fiable de PowerSC activo. Para eliminar la visualización de la información de Cortafuegos fiable en la página **Seguridad** , complete los pasos siguientes:
   a. Pulse el icono **Idiomas y valores** en la barra de menús de la página principal.
   b. Pulse **Uso de subproducto**.
   c. Deslice el conmutador asociado con **Cortafuegos fiable** a la posición de desactivado.
   d. Para restablecer la pantalla, deslice el conmutador a la posición de activado.
5. La columna **TL** en la tabla de punto final indica si el Registro fiable de PowerSC está disponible en el punto final. La sección **Registro fiable** en el banner de panel de instrumentos muestra el porcentaje de puntos finales del grupo seleccionado actualmente que tienen el Registro fiable de PowerSC activo. Para eliminar la visualización de la información de Registro fiable de la página **Seguridad**, complete los pasos siguientes:
   a. Pulse el icono **Idiomas y valores** en la barra de menús de la página principal.
   b. Pulse **Uso de subproducto**.
   c. Deslice el conmutador asociado con **Registro fiable** a la posición de desactivado.
   d. Para restablecer la pantalla, deslice el conmutador a la posición de activado.

Conmutación de la supervisión de Trusted Execution

Puede activar y desactivar a supervisión de Trusted Execution (TE). También puede desactivar la supervisión de TE y planificarla para que se active basándose en un intervalo de tiempo especificado.

1. Pulse el icono **Conmutación de ejecución de confianza**.
2. En la bandeja desplegable seleccione una de las opciones siguientes:
   - **Activar para todos los puntos finales** para activar la supervisión de TE para cada punto final.
   - **Desactivar para todos los puntos finales** para desactivar la supervisión de TE para cada punto final.
3. Si se desactiva la supervisión de TE, quedan disponibles las opciones para establecer un momento en que se reinicie la supervisión de TE. Puede seleccionar uno de los siguientes tiempos de reinicio:
   - **1 hora**
   - **5 horas**
   - **1 día**
   - **1 semana**
   - **Nunca**
4. Pulse **Guardar**.

Envío de una notificación de correo electrónico cuando se produce un suceso de seguridad

En la página Seguridad, puede enviar una notificación de correo electrónico a uno o varios destinatarios cuando se produce un suceso de seguridad.

1. En la página principal, seleccione la pestaña **Seguridad**. Se abre la página **Seguridad**.
2. Pulse el icono **Valores de correo electrónico** en la esquina derecha de la barra de menús. Se abre la ventana **Valores de correo electrónico**.
3. Marque el recuadro de selección **Enviarme correos electrónicos**.
4. Entre las direcciones de correo electrónico de cada destinatario separadas por comas en el campo **Direcciones (separadas por coma)**.

Trabajar con informes

Puede acceder a varios informes desde la página Informes de la GUI de PowerSC.

Están disponibles los siguientes informes:

- El informe **Visión general de conformidad** es una instantánea de la información de alto nivel que se visualiza en la página **Conformidad** de la interfaz.
- El informe **Detalle de conformidad** es una instantánea de la información detallada y de alto nivel que se visualiza en la página **Conformidad**.
- El informe **Visión general de la integridad de archivos** es una instantánea de la información de alto nivel que se visualiza en la página **Seguridad** de la interfaz.
- El informe **Detalles de la integridad de archivos** es una instantánea de la información detallada y de alto nivel que se visualiza en la página **Seguridad**.
- **Conformidad combinada y FIM**

De forma predeterminada, la página **Informes** visualiza los informes **Visión general de conformidad** y **Visión general de la integridad de archivos** para el grupo **Todos los sistemas**. No hay grupos predeterminados especificados para los informes **Detalle de conformidad**, **Detalles de la integridad de archivos** o **Conformidad combinada y FIM**.

Puede producir cada tipo de informe para el grupo **Todos los sistemas** y cada grupo que ha definido. Puede generar el informe para todos los puntos finales de un grupo o un subconjunto de los puntos finales del grupo. Después de generar un informe, puede planificar distribuir el informe en el correo electrónico en formato HTML y como un archivo CSV a uno o varios destinatarios de correo electrónico a petición o cada día.

La lista de informes que se visualizan en la página **Informes** varía en función del ID de inicio de sesión de usuario. Sólo puede generar informes para aquellos puntos finales que gestione basándose en el ID de inicio de sesión. Cada informe que genere en una sesión determinada aparecerá listado cuando abra la próxima sesión.

Selección del grupo de informes

Puede ejecutar cada uno de los informes para el grupo **Todos los sistemas** y cada grupo que ha definido. Puede elegir ejecutar un informe para todos los puntos finales que se han incluido en un grupo o para un subconjunto de puntos finales del grupo.

1. En la página principal, pulse la pestaña **Informes**. Se abre la página **Informes**.
2. Pulse la elipse a la derecha del tipo de informe que desea ejecutar.
3. Pulse **Cambiar grupo**.

4. Se abre un recuadro de selección que lista todos los grupos disponibles. Seleccione el botón de selección junto al grupo para el que desea ejecutar el informe. Pulse **Confirmar**. El informe se ejecuta y el contenido del panel principal se renueva con la información para el grupo seleccionado.
5. Para ejecutar un informe para un subconjunto de puntos finales, expanda el grupo **Todos los sistemas**. Se visualiza una lista de todos los puntos finales disponibles. Seleccione el recuadro de selección junto a cada punto final que desea incluir en el informe. Pulse **Confirmar** para ejecutar el informe.

   Nota: Si desea ejecutar un informe sobre un grupo específico de puntos finales, puede crear un grupo que contengan esos puntos finales. Crear el grupo ahorra tiempo y todos los usuarios lo pueden utilizar porque los grupos son globales (todos los usuarios de la interfaz los pueden ver).
6. Puede buscar un punto final específico especificando el nombre del punto final en el recuadro de texto de búsqueda. Pulse **Confirmar** para ejecutar el informe para ese punto final.

Distribución de un informe mediante el correo electrónico

Después de establecer el grupo para un informe puede planificarlo para su distribución en forma de correo electrónico con formato HTML y un archivo CSV. Puede planificar que el correo electrónico se envíe a uno o varios destinatarios de correo electrónico inmediatamente o cada día.

La inclusión de la versión de CSV del informe permite a los destinatarios cargar los datos de informe en una hoja de cálculo o importarlos a alguna otra aplicación de software que consuma archivos CSV. Los archivos CSV no tienen los conceptos de gráficos o panel de instrumentos. Un archivo CSV generado a partir de un informe de visión general contiene cada una de las cabeceras de columna separadas por comas como primera fila. Las filas subsiguientes listan el punto final y los valores para cada una de las columnas.

Se generan varios archivos CSV a partir de los informes de detalle. El primer archivo CSV está formateado de manera similar al informe de visión general. Se genera un archivo CSV independiente para cada nivel de detalle del informe. Por ejemplo, en el informe de detalles de integridad de archivo, los siguientes niveles de detalle generarán un archivo CSV independiente:

- **Configuración de TE**
- **Configuración de RTC**
- **Estado de subproducto**

1. En la página principal, pulse la pestaña **Informes**. Se abre la página **Informes**.
2. En la lista de informes disponibles, seleccione el informe que desea distribuir. El informe se ejecuta y se renueva el contenido de la página principal.
3. Pulse la elipse a la derecha del informe que desea distribuir.
4. Pulse **Opciones de correo electrónico**. Se abre la ventana Enviar informe por correo electrónico.
5. Especifique la dirección de correo electrónico para cada destinatario en el campo **Direcciones**. Separe varias direcciones de destinatario con un punto y coma (;).
6. Especifique una descripción del correo electrónico en el campo **Asunto**.
7. Elija una de las opciones siguientes:
   - Seleccione el recuadro de selección **Realizar el envío cada día a las** para enviar el informe a los destinatarios cada día. Especifique la hora local para enviar el informe seleccionando el tiempo en horas y minutos. Pulse **Guardar y cerrar**. El informe se envía cada día a la hora especificada.
   - Pulse **Enviar inmediatamente** para enviar el informe. El informe se envía y la ventana se cierra.

Mandatos de PowerSC Standard Edition

PowerSC Standard Edition proporciona mandatos que permiten la comunicación con el componente Trusted Network y el componente Trusted Network Connect utilizando la línea de mandatos.

Mandato chvfilt

Finalidad

Cambia los valores de la regla de filtro de cruce de LAN virtual existente.

Sintaxis

chvfilt [**-v** <**4**|**6**>] **-n fid** [**-a** <**D**|**P**>] [**-z** <**vlan_origen**>] [**-Z** <**vlan_destino**>] [**-s** <**dirección_origen**>] [**-d** <**dirección_destino**>] [**-o** <**op_puerto_origen**>] [**-p** <**puerto_origen**>] [**-O** <**op_puerto_destino**>] [**-P** <**puerto_destino**>] [**-c** <**protocolo**>]

Descripción

El mandato **chvfilt** se utiliza para cambiar la definición de una regla de filtro de cruce de LAN virtual de la tabla de reglas de filtro.

Distintivos

-a Especifica la acción. Los valores válidos son los siguientes:
- D (Denegar): Bloquea el tráfico
- P (Permitir): Permite el tráfico

-c Especifica los diferentes protocolos a los que es aplicable la regla de filtro. Los valores válidos son los siguientes:
- udp
- icmp
- icmpv6
- tcp
- any

-d Especifica la dirección de destino en formato IPv4 o IPv6.

-m Especifica la máscara de dirección de origen.

-M Especifica la máscara de dirección de destino.

-n Especifica el ID de filtro de la regla de filtro que debe modificarse.

-o Especifica el puerto de origen o la operación de tipo ICMP (protocolo de mensajes de control de Internet). Los valores válidos son los siguientes:
- lt
- gt
- eq
- any

-O Especifica el puerto de destino o la operación de código ICMP. Los valores válidos son los siguientes:
- lt

- gt
- eq
- any

-p Especifica el puerto de origen o el tipo de ICMP.

-P Especifica el puerto de destino o el código de ICMP.

-s Especifica la dirección de origen en formato v4 o v6.

-v Especifica la versión de IP de la tabla de reglas de filtro. Los valores válidos son 4 y 6.

-z Especifica el ID de LAN virtual de la partición lógica de origen.

-Z Especifica el ID de LAN virtual de la partición lógica de destino.

Estado de salida

Este mandato devuelve los siguientes valores de salida:

0 Finalización satisfactoria.

>0 Se ha producido un error.

Ejemplos

1. Para cambiar una regla de filtro válida que exista en el kernel, escriba el mandato como se indica a continuación:

   ```
   chvfilt -n 1 -v4 -a P -z 100 -Z 300 -o eq -p 23 -O lt -P 345 -c tcp
   ```

2. Cuando no existe una regla de filtro (n=2) en el kernel, la salida es la siguiente:

   ```
   chvfilt -n 2 -v4 -a P -z 100 -Z 300 -o eq -p 23 -O lt -P 345 -c tcp
   ```

   El sistema muestra la salida siguiente:

   ```
   ioctl(QUERY_FILTER) ha fallado, ninguna regla de filtro err=2
   No se puede cambiar la regla de filtro.
   ```

Mandato genvfilt

Finalidad

Añade una regla de filtro para el cruce de LAN virtual (VLAN) entre particiones lógicas del mismo servidor IBM Power Systems.

Sintaxis

genvfilt -v <**4**|**6**> **-a** <**D**|**P**> **-z** <**svlan**> **-Z** <**dvlan**> [**-s** <**dirección_origen**>] [**-d** <**dirección_d**>] [**-o** <**op_puerto_origen**>] [**-p** <**puerto_origen**>] [**-O** <**op_puerto_dst**>] [**-P** <**puerto_dst**>] [**-c** <**protocolo**>]

Descripción

El mandato **genvfilt** añade una regla de filtro para el cruce de LAN virtual (VLAN) entre particiones lógicas (LPAR) del mismo servidor IBM Power Systems.

Distintivos

-a Especifica la acción. Los valores válidos son los siguientes:

- D (Denegar): Bloquea el tráfico
- P (Permitir): Permite el tráfico

-c Especifica los diferentes protocolos a los que es aplicable la regla de filtro. Los valores válidos son los siguientes:
- udp
- icmp
- icmpv6
- tcp
- any

-d Especifica la dirección de destino en formato v4 o v6.

-m Especifica la máscara de dirección de origen

-M Especifica la máscara de dirección de destino.

-o Especifica el puerto de origen o la operación de tipo ICMP (protocolo de mensajes de control de Internet). Los valores válidos son los siguientes:
- lt
- gt
- eq
- any

-O Especifica el puerto de destino o la operación de código ICMP. Los valores válidos son los siguientes:
- lt
- gt
- eq
- any

-p Especifica el puerto de origen o el tipo de ICMP.

-P Especifica el puerto de destino o el código de ICMP.

-s Especifica la dirección de origen en formato IPv4 o IPv6.

-v Especifica la versión de IP de la tabla de reglas de filtro. Los valores válidos son 4 y 6.

-z Especifica el ID de LAN virtual de la LPAR de origen. El ID de LAN virtual debe estar en el rango de 1 a 4096.

-Z Especifica el ID de LAN virtual de la LPAR de destino. El ID de LAN virtual debe estar en el rango de 1 a 4096.

Estado de salida

Este mandato devuelve los siguientes valores de salida:

0 Finalización satisfactoria.

>0 Se ha producido un error.

Ejemplos

1. Para añadir una regla de filtro para permitir datos TCP desde un ID de VLAN de origen de 100 a un ID de VLAN de destino de 200 en determinados puertos, escriba el mandato del siguiente modo:
   ```
   genvfilt -v4 -a P -z 100 -Z 200  -o lt -p 345 -O lt -P 345 -c tcp
   ```

Referencia relacionada:

"Mandato mkvfilt" en la página 170

"Mandato vlantfw" en la página 190

Mandato lsvfilt

Finalidad

Lista las reglas de filtro de cruce de LAN virtual de la tabla de filtros.

Sintaxis

lsvfilt [**-a**]

Descripción

El mandato **lsvfilt** se utiliza para listar las reglas de filtro de cruce de LAN virtual y su estado.

Distintivos

-a Lista solamente las reglas de filtro activas.

Estado de salida

Este mandato devuelve los siguientes valores de salida:

0 Finalización satisfactoria.

>0 Se ha producido un error.

Ejemplos

1. Para listar todas las reglas de filtro activas en el kernel, escriba el mandato como sigue:

   ```
   lsvfilt -a
   ```

Conceptos relacionados:

"Desactivación de reglas" en la página 125
Puede desactivar las reglas que permiten el direccionamiento de VLAN cruzadas en la característica Cortafuegos fiable.

Mandato mkvfilt

Finalidad

Activa las reglas de filtro de cruce de LAN virtual mediante el mandato **genvfilt**.

Sintaxis

mkvfilt -u

Descripción

El mandato **mkvfilt** activa las reglas de filtro de cruce de LAN virtual definidas por el mandato **genvfilt**.

Distintivos

-u Activa las reglas de filtro en la tabla de reglas de filtro.

Estado de salida

Este mandato devuelve los siguientes valores de salida:

0 Finalización satisfactoria.

>0 Se ha producido un error.

Ejemplos

1. Para activar las reglas de filtro en el kernel, escriba el mandato como se indica a continuación:

   ```
   mkvfilt -u
   ```

Referencia relacionada:

"Mandato genvfilt" en la página 168

Mandato pmconf

Finalidad

Notifica y gestiona el servidor de TNCPM (Trusted Network Connect Patch Management) registrando los niveles de tecnología y servidores TNC para los arreglos más recientes y generando informes sobre el estado de TNCPM.

| **Nota:** El servidor de TNCPM sólo se debe ejecutar en AIX Versión 7.2 con el nivel de tecnología 7100-02
| para permitir la descarga de los metadatos del service pack.

Sintaxis

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

pmconf rmtncpm

pmconf start

pmconf stop

pmconf init -i <*intervalo_descarga*> **-l** <*Lista_TL*> **-A** [**-P** <*vía_acceso_descarga*>] [**-x** <*intervalo_ifix*>] [**-K** <*clave_ifix*>]

pmconf add -l *lista_TL*

pmconf add -o <*nombre_paquete*> -V <*versión*> -T [installp|rqm] -D <*vía_acceso_definida_usuario*>

pmconf add -p <*Lista_SP*> [**-U** <*vía_acceso_SP_definida_usuario*>]

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

pmconf add -y <*archivo_advertencia*> **-v** <*archivo_firmas*> **-e**

pmconf chtncpm attribute = *valor*

pmconf delete -l <*lista_TL*>

pmconf delete -o <*nombre_paquete*> -V <*versión*>

pmconf delete -p <*Lista_SP*>

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

pmconf export -f *nombre_archivo*

| **pmconf get** -o <paquete> -V <versión> -T <installp | rpm> -D <directorio_descarga>

| **pmconf get** -L -o <paquete> -V <versión | all> -T <installp | rpm>

| **pmconf get** -L -p <SP>

| **pmconf get** -p <SP> -D <directorio_descarga>

pmconf hist -d

pmconf hist -u

pmconf import -f *nombre_archivo_cert* **-k** *nombre_archivo_claves*

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

pmconf list -a *SP*

pmconf list -C

pmconf list -l *SP*

pmconf list -o <*nombre_paquete*> -V <*versión*>

pmconf list -o [-c] [-q]

pmconf log loglevel = info | error | none

pmconf modify -i <*intervalo_descarga*>

´**pmconf modify -P** <*vía_acceso_descarga*>

pmconf modify -g <*yes o no para aceptar todas las licencias*>

pmconf modify -t <*lista_tipo_APAR*>

pmconf modify -x <*intervalo_ifix*>

pmconf modify -K <*clave_ifix*>

| **pmconf proxy** display

| **pmconf proxy** [enable=yes | no] [host=<nombre_host>] [port=<núm_puerto>]

pmconf restart

pmconf status

Descripción

Las funciones del mandato **pmconf** son las siguientes:

Gestión de repositorio de arreglos
Registra o elimina el registro de los niveles de tecnología; elimina el registro de los servidores de TNC. TNCPM crea un repositorio de arreglos para cada nivel de tecnología que contenga los arreglos más recientes, la información de **lslpp** (por ejemplo, información sobre los conjuntos de archivos instalados o las actualizaciones de conjuntos de archivos) y la información de arreglos de seguridad para dicho nivel de tecnología.

Informes

Genera informes sobre el estado de TNCPM.

Las siguientes operaciones se pueden realizar utilizando el mandato **pmconf**:

Elemento	Descripción
add	Registra un nivel de tecnología nuevo utilizando TNCPM.
chtncpm	Cambia los atributos en el archivo tnccs.conf. Se necesita un mandato **start** explícito para que los cambios entren en vigor en el servidor de TNCPM.
delete	Elimina el registro de un nivel de tecnología utilizando TNCPM.
get	Visualiza o descarga información sobre los arreglos de seguridad y los paquetes de código abierto disponibles.
history	Visualiza el historial de actualizaciones y descargas.
list	Visualiza la información sobre TNCPM.
log	Establece el nivel de registro para los componentes de TNC.
mktncpm	Crea el servidor de TNCPM.
modify	Modifica los atributos de tncpm.conf.
proxy	Gestiona la configuración de parámetros de servidor proxy.
rmtncpm	Elimina el servidor de TNCPM.
start	Inicia el servidor de TNCPM.
stop	Detiene el servidor de TNCPM.

Distintivos

Elemento	Descripción
-A	Acepta todos los acuerdos de licencia al realizar actualizaciones de cliente.
-a <archivo_advertencia>	Especifica el archivo de advertencia que corresponde con el parámetro **ifix**. Si no se proporciona el archivo de advertencia, el parámetro **ifix** no se considera como dirección de vulnerabilidades y exposiciones comunes (CVE) del arreglo temporal.
-a *SP*	Genera un informe de información de APAR (informe autorizado de análisis de programa) de seguridad para el Service Pack. *SP* está en el formato REL00-TL-SP (por ejemplo, `6100-01-04` representa el Service Pack 04 para el nivel de tecnología 01 y la versión 6.1).
-e <archivo_ifix>	Especifica los arreglos temporales que se añaden a TNCPM.
-i *intervalo_descarga*	Especifica el intervalo durante el que TNCPM comprueba para un nuevo paquete de servicio los niveles de tecnología registrados. El intervalo es un valor entero que representa minutos o representa el formato siguiente: **d** (núm. de días): **h** (horas): **m** (minutos). El rango soportado para el *intervalo_descarga* es de 30 a 525600 minutos.
-K <clave_ifix>	Especifica la clave pública de IBM AIX Product Security Incident Response Tool (PSIRT) que se utiliza para autenticar los avisos descargados y los arreglos temporales. Esta clave pública se puede descargar de un servidor de claves públicas PGP utilizando el ID **0x28BFAA12**.
-L	Especifica la modalidad de lista o búsqueda sólo.
o *nombre_paquete*	Nombre del paquete de código abierto en el que se debe realizar la búsqueda o la descarga.
-P *vía_acceso_repositorio_arreglos*	Especifica el directorio de descarga para los repositorios de arreglos que TNCPM descargará. El directorio predeterminado es **/var/tnc/tncpm/fix_repository**.
-p *lista_SP*	Especifica una lista de Service Pack que se deben descargar. La lista es una lista separada por comas en el formato, REL00-TL-SP (por ejemplo, `6100-01-04` representa el Service Pack 04 para el nivel de tecnología 01 y la versión 6.1). Cuando utilice el distintivo -U, especifique sólo un SP.
-t *lista_tipos_APAR*	Especifica los tipos de APAR a los que TNCPM soporta para la actualización de cliente y la lista de servidores TNC. Los APAR de seguridad siempre se soportan. Lista_tipos_APAR es una lista separada por comas de los tipos siguientes: HIPER, FileNet Process Engine, Mejora.
T *tipo_paquete*	Especifica el tipo de paquete de código abierto en el que se debe realizar la búsqueda o la descarga
-U *repositorio_arreglo_definido_usuario*	Especifica la vía de acceso al repositorio de arreglos definido por el usuario. Especifique el release, el nivel de tecnología y el Service Pack asociados con el repositorio de arreglos que se utiliza para la verificación y las actualizaciones de los clientes.
-s	Genera un informe de Service Packs registrados.
-l *SP*	Genera un informe de información de **lslpp** para el Service Pack. *SP* está en el formato REL00-TL-SP (por ejemplo, `6100-01-04` representa el Service Pack 04 para el nivel de tecnología 01 y la versión 6.1).
-u	Genera un informe del historial de actualización de cliente.
V *versión*	La versión del paquete de código abierto en el que se debe realizar la búsqueda o la descarga. En modalidad de búsqueda (-L) se puede especificar un valor "all" para buscar todas las versiones disponibles del paquete especificado.
-d	Genera un informe del historial de descarga de Service Pack.
-C	Genera un informe para el certificado de servidor.

Elemento	Descripción
-f *nombre_archivo*	Especifica el nombre de archivo de certificado.
-k	Especifica el archivo del que se debe leer la clave de certificado en caso de una operación de importación.

-c	Visualiza los atributos de usuario en registros separados por dos puntos, como se indica a continuación:
	`# name: atributo1: atributo2: ...`
	`policy: valor1: valor2: ...`

-v <*archivo_firmas*>	Especifica el archivo de firmas para la advertencia de vulnerabilidad de IBM AIX.
-y <*archivo de advertencia*>	Especifica un archivo de advertencia de vulnerabilidad de IBM AIX.
-q	Suprime la información de cabecera.
-x <*intervalo_ifix*>	Especifica el intervalo en minutos para comprobar y descargar nuevos arreglos temporales. Si este valor se establece en 0, se inhabilitará la descarga y notificación automáticas de arreglos temporales. El intervalo predeterminado es de 24 horas. El rango soportado para <*intervalo_ifix*> es de 30 a 525600 minutos.

Estado de salida

Este mandato devuelve los siguientes valores de salida:

Elemento	Descripción
0	El mandato se ha ejecutado correctamente y se han realizado todos los cambios solicitados.
>0	Se ha producido un error. El mensaje de error impreso incluye más detalles sobre el tipo de anomalía.

Ejemplos

1. Para inicializar TNCPM, especifique el siguiente mandato:
   ```
   pmconf init -f 10080 -l 5300-11,6100-00
   ```
2. Para crear el daemon TNCPM, escriba el mandato siguiente:
   ```
   mktncpm pmport=55777 tncserver=11.11.11.11:77555
   ```
3. Para iniciar el servidor, escriba el mandato siguiente:
   ```
   pmconf start
   ```
4. Para detener el servidor, especifique el mandato siguiente:
   ```
   pmconf stop
   ```
5. Para registrar un nuevo nivel de tecnología utilizando TNCPM, especifique el mandato siguiente:
   ```
   pmconf add -l 6100-01
   ```
6. Para eliminar el registro de un nivel de tecnología de TNCPM, especifique el mandato siguiente:
   ```
   pmconf delete -l 6100-01
   ```
7. Para eliminar el registro de un servidor TNC que tiene una dirección IP de 11.11.11.11 de TNCPM, especifique el mandato siguiente:
   ```
   pmconf delete -t 11.11.11.11
   ```
8. Para registrar una versión más reciente de un Service Pack anterior en TNCPM, especifique el mandato siguiente:
   ```
   pmconf add -s 6100-01-04
   ```
9. Para eliminar el registro de un Service Pack anterior de TNCPM, especifique el mandato siguiente:
   ```
   pmconf delete -s 6100-01-04
   ```
10. Para generar un informe de repositorios de arreglos para cada nivel de tecnología registrado, especifique el mandato siguiente:
    ```
    pmconf list -s
    ```
11. Para generar un informe de la información de un nivel de tecnología registrado **lslpp**, especifique el mandato siguiente:
    ```
    pmconf list -l 6100-01-02
    ```
12. Para generar un informe desde el historial de actualizaciones, especifique el siguiente mandato:
    ```
    pmconf hist -u
    ```
13. Para generar un informe desde el historial de descargas, especifique el mandato siguiente:

```
pmconf hist -d
```

14. Para generar un informe del certificado de servidor, especifique el mandato siguiente:

```
pmconf list -C
```

15. Para generar un informe de la información de un APAR de seguridad de Service Pack, especifique el mandato siguiente:

```
pmconf list -a 6100-01-02
```

16. Para importar un certificado de servidor, especifique el mandato siguiente:

```
pmconf import -f /tmp/server.txt -k /tmp/server-cert-key.txt
```

17. Para exportar el certificado del servidor, especifique el mandato siguiente:

```
pmconf export -f /tmp/server.txt
```

18. Para visualizar todas las versiones en formato rpm del paquete de código abierto 'emacs', especifique el mandato siguiente:

```
pmconf get -L -o emacs -V all -T rpm
```

19. Para descargar la Versión 4.5.1 del paquete de código abierto 'lsof', en formato rpm, en el directorio /tmp/new_lsof, especifique los mandatos siguientes:

```
mkdir /tmp/new_lsof
pmconf get -o lsof -V 4.5.1 -T rpm -D /tmp/new_lsof
```

20. Para visualizar todas las versiones disponibles de OpenSSH en formato de installp, especifique el mandato siguiente:

```
pmconf get -o openssh -T installp -L -V all
```

21. Para visualizar los valores de configuración de proxy actuales que cURL utilizará cuando descargue paquetes de código abierto o arreglos de seguridad, especifique el mandato siguiente:

```
pmconf proxy display
```

22. Para establecer que se inhabilite la configuración de proxy, especifique el mandato siguiente:

```
pmconf proxy enable=no
```

23. Para habilitar el proxy y establecer el host en 'myProxyServer' en el puerto 9876, escriba el mandato siguiente:

```
pmconf proxy enable=yes host=myProxyServer port=9876
```

24. Para cambiar el puerto de servidor proxy a utilizar, especifique el mandato siguiente:

```
pmconf proxy port=1234
```

25. Para visualizar las vulnerabilidades conocidas tratadas por los arreglos de seguridad para el nivel de Service Pack 7100-03-02, especifique el mandato siguiente:

```
 pmconf get -L -p 7100-03-02
```

26. Para descargar, pero no aplicar, arreglos de seguridad para el nivel de Service Pack 7200-00-01, en el directorio /tmp/ifixes_for_7.2.0.1, especifique los mandatos siguientes:

```
mkdir /tmp/ifixes_for_7.2.0.1
pmconf get -p 7200-00-01 -D /tmp/ifixes_for_7.2.0.1
```

Mandato psconf

Finalidad

Notifica y gestiona el servidor de Trusted Network Connect (TNC), el cliente de TNC, el TNC IP Referrer (IPRef) y Service Update Management Assistant (SUMA). Gestiona el conjunto de archivos y las políticas de gestión de parches con relación a la integridad de punto final (servidor y cliente) durante o después de la conexión de red para proteger la red de amenazas y ataques.

Sintaxis

Operaciones de servidor de TNC:

psconf mkserver [**tncport=**<*puerto*>] **pmserver=**<*host:puerto*> [tsserver=<host>] [**recheck_interval=**<*tiempo_en_minutos*> | **d** (días) : **h** (horas) : **m** (minutos)] [**dbpath** = <*directorio_definido_por_usuario*>] [**default_policy=**<*yes* | *no* >] [**clientData_interval=**<*tiempo_en_minutos*> | **d** (días) : **h** (horas) : **m** (minutos)] [**clientDataPath=**<*vía_acceso_completa* >]

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

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

psconf chserver attribute = *valor*

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

psconf add -F <*nombre_política_FS*> -r <*info_compilación*> [**apargrp= [±]**<*grupo_apar1, grupo_apar2.. >*] [*grupo_ifix*=[+|-]<*grupo_ifix1,grupo_ifix2...>*]

psconf add { **-G** <*nombre_grupo_ip*> **ip=[±]**<*host1, host2...>* | {**-A**<*grupo_apar*> [**lista_apar**=[**±**]*apar1, apar2...* | {**-V** <*grupo_ifix*> [*lista_ifix*=[+|-]*ifix1,ifix2...*]}

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

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

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

psconf delete { **-F** <*nombre_política_FS*> | **-G** <*nombre_grupo_ip*> | **-P** <*nombre_política*> | **-A** <*grupo_apar*> | **-V** <*grupo_ifix*>}

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

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

psconf certdel -i <*host*>

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

psconf update [-p] {-i<*host*>| **-G** <*grupo_ip*>[**-r** <*info_compilación*> | **-a** <*apar1, apar2...*> | **[-u] -v** <*ifix1, ifix2,...*> | **-O** <*grupo_paquete_abierto1, grupo_paquete_abierto2,...*>}

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

psconf import -C -i <*host*> **-f** <*nombre_archivo*> | **–d** <*nombre_archivo_base_datos_import*>

psconf { **import -k** <*nombre_archivo_claves*> | **export**} **-S -f** <*nombre_archivo*>

psconf list { **-S** | **-G** < *nombre_grupo_ip* | **ALL** > | **-F** < *nombre_política_FS* | **ALL** > | **-P** < *nombre_política* | **ALL** > | **-r** < *info_compilación* | **ALL** > | **-I -i** < *ip* | **ALL** > | **-A** < *grupo_apar* | **ALL** > | **-V** <*grupo_ifix*> | -O <*grupo_paquete_abierto*|*ALL*>} **[-c] [-q]**

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

psconf export -d <vía_acceso_a_directorio_exportación>

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

psconf report -A <nombre_advertencia>

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

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

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

psconf clientData {-l | -g} -i <*ip*|*host*>

psconf add -O <*grupo_paquete_abierto*> <*nombre_paquete_abierto:versión*>

psconf delete -O <*grupo_paquete_abierto*> <*nombre_paquete_abierto:versión*>

psconf delete -O <*grupo_paquete_abierto*>

psconf delete -O ALL

psconf add -O <*grupo_paquete_abierto*> fspolicy=<*nombre_política_fs*>

psconf report -O ALL -o TEXT

| **psconf add -V <*grupo_ifix*> autoupdate=<yes|no>**

| **psconf reboot -i <*host*> last one**

Operaciones de cliente de TNC:

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

psconf mkclient tncport=<<*puerto*>> -T

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

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

psconf chclient attribute = *valor*

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

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

psconf import { **-S** | **-C -k** <*nombre_archivo_clave*> } **-f** <*nombre_archivo*>

Operaciones de IPRef de TNC:

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

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

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

psconf chipref attribute = *valor*

psconf { **import -k** <*nombre_archivo_claves*> | **export** } **-R -f** <*nombre_archivo*>

psconf list -R

Descripción

La tecnología TNC es una arquitectura basada en estándar abierta para la autenticación de punto final, la medición de la integridad de plataforma y la integración de sistemas de seguridad. La arquitectura TNC inspecciona puntos finales (clientes y servidores de red) para comprobar la conformidad con las políticas de seguridad antes de darles permiso en la red protegida. El IPRef de TNC informa al servidor de TNC sobre las nuevas IP que se detectan en el servidor de E/S virtual (VIOS).

SUMA ayuda a los administradores del sistema a salir de la tarea de recuperación manual de actualizaciones de mantenimiento de la web. Ofrece opciones flexibles que permiten al administrador de sistema configurar una interfaz automática para descargar los arreglos de un sitio web de distribución de arreglos en los sistemas.

El mandato **psconf** gestiona el servidor de red y los clientes añadiendo o suprimiendo políticas de seguridad, validando clientes como fiables o no fiables, generando informes y actualizando el servidor y el cliente.

Se pueden realizar las siguientes operaciones utilizando el mandato **psconf**:

Elemento	Descripción
add	Añade una política, un cliente o la información de correo electrónico en el servidor TNC.
apargrp	Especifica los nombres de grupo de APAR como parte de la política de conjunto de archivos que se utilizan para la verificación de los clientes de TNC.
aparlist	Especifica la lista de APAR que forman parte del grupo de APAR.
certadd	Marca el certificado como fiable o no fiable.
certdel	Suprime la información de cliente.
chclient	Cambia los atributos en el archivo `tnccs.conf`. Se necesita un mandato **start** explícito para que los cambios entren en vigor en el cliente de TNC. La sintaxis de atributo=valor será la misma que la de **mkclient**.
chipref	Cambia los atributos en el archivo `tnccs.conf`. Se necesita un mandato **start** explícito para que los cambios entren en vigor en IPRef. La sintaxis de atributo=valor es la misma que la de **mkipref**.
chserver	Cambia los atributos en el archivo `tnccs.conf`. Se necesita un mandato **start** explícito para que los cambios entren en vigor en el servidor de TNC. La sintaxis de atributo=valor es la misma que la de **mkserver**. **Nota:** El atributo **dbpath** no se puede cambiar utilizando el mandato **chserver**. Sólo se puede establecer al ejecutar **mkserver**.
clientData	Crea una instantánea de información (nivel de sistema operativo y conjuntos de archivos) acerca del cliente de TNC. La vía de acceso *vía_acceso_datos_cliente* identifica el lugar donde se almacena la información de recopilación de instantáneas. La ubicación predeterminada está en el directorio `/var/tnc/clientData/` en el servidor de TNC. Puede cambiar o establecer la vía de acceso *vía_acceso_datos_cliente* utilizando el submandato **chserver** o **mkserver**. Puede iniciar la recopilación de instantáneas de cliente de TNC desde la línea de mandatos ejecutando el submandato **clientData** desde el servidor de TNC. El submandato **clientData** que se ejecuta desde la línea de mandatos es independiente del intervalo **clientData_interval**.

Elemento	Descripción
clientData_interval	Puede utilizar el submandato **chserver** o **mkserver** para configurar que la recopilación de instantáneas se produzca a intervalos regulares especificando un valor para el intervalo **clientData_interval**. La recopilación de instantáneas se inicia automáticamente cuando el intervalo **clientData_interval** tiene un valor distinto de 0 (cero). De forma predeterminada, el planificador inhabilita la recopilación de instantáneas. Para habilitar el planificador, especifique un valor **clientData_interval** que sea mayor que o igual a 30. Para inhabilitar el planificador, especifique un valor **clientData_interval** de 0 (cero). El rango soportado para el intervalo **clientData_interval** es de 30 a 525600 minutos.
dbpath	Especifica la ubicación de base de datos de TNC. El valor predeterminado es `/var/tnc`.
default_policy	Habilita o inhabilita la verificación automática de los clientes de TNC para el arreglo interno (ifix) y los APAR en el mismo nivel que el cliente. Especifique *yes* para habilitar la verificación automática. Especifique *no* para inhabilitar la verificación automática. Para obtener más información sobre el submandato **default_policy**, consulte la tabla default_policy.
delete	Suprime una política o la información de cliente.
export	Exporta el certificado de servidor o cliente o la base de datos en el servidor de TNC.
fspolicy	Especifica la política de conjunto de archivos del release, el nivel de tecnología y el Service Pack que se utilizan para la verificación de clientes de TNC.
import	Importa un certificado en el cliente o el servidor o la base de datos en el servidor de TNC.
ipgroup	Especifica el grupo de Internet Protocol (IP) que contiene varias direcciones IP de cliente o nombres de host.
list	Muestra información sobre el servidor de TNC, el cliente de TNC o SUMA.
log	Establece el nivel de registro para los componentes de TNC.
mkclient	Configura el cliente de TNC.
mkipref	Configura el IPRef de TNC.
mkserver	Configura el servidor de TNC.
Openpkggrp	Especifica el nombre de grupo openpkg como parte de la política de conjunto de archivos que se utiliza para verificar los clientes.
pmport	Especifica el número de puerto en el que **pmserver** está a la escucha. El valor predeterminado es 38240.
pmserver	Especifica el nombre de host o la dirección IP del mandato **suma** que descarga los Service Pack y los arreglos de seguridad más recientes disponibles en el sitio web de IBM® ECC y en el sitio web de IBM Fix Central.
reboot	Rearranca el cliente TNC que se identifica por la dirección IP en la variable <*host*>.
recheck_interval	Especifica el intervalo en formato de minutos o d (días): h (horas): m (minutos) para que el servidor de TNC verifique los clientes de TNC. El rango soportado para el intervalo **recheck_interval** es de 30 a 525600 minutos. **Nota:** Un valor de **recheck_interval=0** significa que el planificador no inicia la verificación de los clientes a intervalos regulares y los clientes registrados se verifican automáticamente cuando se inician. En tales casos, el cliente puede verificarse manualmente.
report	Genera un informe que tiene una extensión de archivo .txt o .csv.
restart	Reinicia el cliente de TNC, el servidor de TNC o el IPRef de TNC.
rmclient	Desconfigura el cliente de TNC.
rmipref	Desconfigura el IPRef de TNC.

Elemento	Descripción
rmserver	Desconfigura el servidor de TNC.
start	Inicia el cliente de TNC, el servidor de TNC o el IPRef de TNC.
status	Muestra el estado de la configuración de TNC.
stop	Detiene el cliente de TNC, el servidor de TNC o el IPRef de TNC.
tncport	Especifica el número de puerto en el que el servidor de TNC escucha. El valor predeterminado es 42830.
tncserver	Especifica el servidor TNC que verifica o actualiza los clientes de TNC.
tssserver	Especifica la dirección IP o el nombre de host del servidor de Trusted Surveyor.
update	Instala parches en el cliente.
verify	Inicia una verificación manual del cliente.

La tabla siguiente muestra los resultados de la configuración del submandato **default_policy** en los valores *yes* o *no*:

Tabla 16. Resultados del submandato default_policy

FSpolicy (Política de conjunto de archivos)	**default policy=***yes*	**default policy=***no*
El cliente TNC pertenece a una política de conjunto de archivos con un arreglo temporal (iFix) y grupos de APAR definidos	La política predeterminada se sustituye por el iFix y los APAR proporcionados en la política de conjunto de archivos.	La política predeterminada no se utiliza. El iFix y los APAR proporcionados en la política de conjunto de archivos se tienen en cuenta durante el proceso de verificación para el cliente de TNC.
El cliente de TNC pertenece a una política de conjunto de archivos sin un iFix y grupos de APAR definidos	La política predeterminada se utiliza con el iFix y los APAR durante el proceso de verificación para el cliente de TNC. Sólo el iFix y los APAR que coinciden con el nivel del cliente de TNC se utilizan durante el proceso de verificación.	La política predeterminada no se utiliza.

Distintivos

Elemento	Descripción
-A <nombreAdvertencia>	Especifica el nombre de advertencia para el informe.
-B <infoCompilación>	Especifica la información de compilación para preparar un informe de parches.

-c	Muestra los atributos de usuario en registros separados por dos puntos como se indica a continuación:
	`# name: atributo1: atributo2: ...`
	`policy: valor1: valor2: ...`

-C	Especifica que la operación es para el componente de cliente.
-d *ubicación de archivo de base de datos/vía de acceso de directorio de base de datos*	Especifica la ubicación de vía de acceso de archivo para la importación de la base de datos/especifica la ubicación de vía de acceso de directorio para la exportación de la base de datos.
-D *aaaa-mm-dd*	Especifica la fecha para una entrada de cliente determinada del historial de registro, donde *aaaa* es el año, *mm* es el mes y *dd* es el día.
-e *id_correo_electrónico* **ipgroup=[±]***g1, g2...*	Especifica el ID de correo electrónico seguido de una lista de nombres de grupo de IP separados por comas.
-E | **FAIL** | **COMPLIANT** | **ALL** |	Especifica el suceso para el que los correos electrónicos necesitan enviarse al ID de correo electrónico configurado. FAIL - Los correos se envían cuando el estado de verificación del cliente es FAILED. COMPLIANT - Los correos se envían cuando el estado de verificación del cliente es COMPLIANT. ALL - Los correos se envían para todos los estados de la verificación del cliente.

Elemento	Descripción
-f *nombre_archivo*	Especifica el archivo en el que se debe leer el certificado en el caso de una operación de importación o especifica la ubicación en la que se debe grabar el certificado en caso de una operación de exportación.
F *política_sist_arch info_compilación*	Especifica el nombre de política del sistema de archivos, seguido de la información de compilación. La información de compilación se puede proporcionar en el formato siguiente: `6100-04-01`, donde `6100` representa la versión 6.1, `04` es el nivel de mantenimiento y `01` es el Service Pack.
-g	Ejecute el submandato **clientData** en el cliente de TNC especificado. Este distintivo sólo está disponible con el submandato **clientData**.
-G*nombregrupoip* **ip=[±]***ip1, ip2...*	Especifica el nombre de grupo de IP seguido de una lista de IP separadas por comas.
-H	Lista el registro histórico.
-i *host*	Especifica la dirección IP o el nombre de host.
-I ip=[±]*ip1, ip2...* | [±] host1,host2...	Especifica la IP/nombre de host que se debe ignorar durante la verificación.
-k *nombrearchivo*	Especifica el archivo del que se debe leer la clave de certificado en caso de una operación de importación.
-l	Lista los detalles de instantánea en el servidor de TNC para el cliente de TNC especificado. Este distintivo sólo está disponible con el submandato **clientData**.
-O <openpkggrp>	Especifica el nombre de grupo openpkg para la política.
-p	Previsualiza la actualización de cliente de TNC.
-P <nombre_política>	Especifica el nombre de política para preparar un informe de política de cliente.
-q	Suprime la información de cabecera.
-r *info_compilación*	Genera el informe basado en la información de compilación. La información de compilación se puede proporcionar en el formato siguiente: `6100-04-01`, donde `6100` representa la versión 6.1, `04` es el nivel de mantenimiento y `01` es el Service Pack.
-R	Especifica que la operación es para el componente IPRef.
-s COMPLIANT | IGNORE | FAILED | ALL	Muestra el cliente por estado como se indica a continuación: **COMPLIANT** Muestra los clientes activos. **IGNORE** Muestra los clientes que se excluyen de cualquier verificación. **FAILED** Muestra los clientes que no han realizado correctamente la verificación de acuerdo con la política configurada. **ALL** Muestra todos los clientes independientemente de los estados.
-S <host>	Especifica el nombre de host para preparar un informe de arreglos de seguridad de cliente.
-t TRUSTED | UNTRUSTED	Marca el cliente especificado como fiable (trusted) o no fiable (untrusted). **Nota:** Sólo los administradores de sistema pueden verificar el servidor o el cliente como fiable o no fiable.
-T	Especifica que el cliente puede aceptar solicitudes de cualquier servidor de TS que tenga un certificado válido.
-u	Desinstala un arreglo temporal que está instalado en un cliente de TNC.
-v<*CVEid*|*ALL*>	Muestra el exposiciones y vulnerabilidades comunes para los Service Pack registrados. **CVEid** **All** Visualiza todas las exposiciones y vulnerabilidades comunes para los Service Pack registrados.
-v<*ifix1, ifix2,...*>	Especifica una lista de arreglos temporales separados por comas.
-V<*grupo_ifix*>	Especifica el nombre de grupo de arreglo temporal.
-V <*grupo_ifix*> autoupdate=<yes|no>	Especifica si los arreglos temporales bajo el nombre de grupo de ifix especificado se actualizan automáticamente. **Yes** Actualiza la política definida para fspolicy automáticamente cuando se reciben nuevos arreglos temporales en el servidor de TNC. **No** Especifica que se asignarán manualmente los nuevos arreglos temporales a la política una vez recibidos en el servidor de TNC. No es el valor predeterminado.

Estado de salida

Este mandato devuelve los siguientes valores de salida:

Elemento	Descripción
0	El mandato se ha ejecutado correctamente y se han realizado todos los cambios solicitados.
>0	Se ha producido un error. El mensaje de error impreso incluye más detalles sobre el tipo de anomalía.

Ejemplos

1. Para iniciar el servidor de TNC, escriba el mandato siguiente:
   ```
   psconf start server
   ```
2. Para añadir una política de sistema de archivos denominada `71D_latest` para la compilación `7100-04-02`, especifique el siguiente mandato:
   ```
   psconf add -F 71D_latest 7100-04-02
   ```
3. Para suprimir una política del sistema de archivos denominada `71D_old`, especifique el siguiente mandato:
   ```
   psconf delete -F 71D_old
   ```
4. Para validar que el cliente que tiene una dirección IP de `11.11.11.11` es **trusted**, escriba el mandato siguiente:
   ```
   psconf certadd -i 11.11.11.11 -t TRUSTED
   ```
5. Para suprimir el cliente que tiene una dirección IP de `11.11.11.11` del servidor, escriba el mandato siguiente:
   ```
   psconf certdel -i 11.11.11.11
   ```
6. Para verificar la información del cliente que tiene una dirección IP de `11.11.11.11`, escriba el mandato siguiente:
   ```
   psconf verify -i 11.11.11.11
   ```
7. Para mostrar la información de cliente que tiene una dirección IP de `11.11.11.11`, escriba el siguiente mandato:
   ```
   psconf list -i 11.11.11.11
   ```
8. Para generar el informe para clientes que están en estado **COMPLIANT**, especifique el mandato siguiente:
   ```
   psconf list -s CPMPLIANT -i ALL
   ```
9. Para generar el informe para la compilación `7100-04-02`, especifique el siguiente mandato:
   ```
   psconf list -r 7100-04-02
   ```
10. Para visualizar el historial de conexiones de un cliente que tiene una dirección IP de `11.11.11.11`, especifique el siguiente mandato:
    ```
    psconf list -H -i 11.11.11.11
    ```
11. Para suprimir la entrada de un cliente que tiene una dirección IP de `11.11.11.11` del historial de registro anterior o igual al 1 de febrero de 2009, especifique el siguiente mandato:
    ```
    psconf delete -H -i 11.11.11.11 -D 2009-02-01
    ```
12. Para importar el certificado de cliente de un cliente que tiene una dirección IP de `11.11.11.11` desde el servidor, especifique el mandato siguiente:
    ```
    psconf import -C -i 11.11.11.11 -f /tmp/client.txt
    ```
13. Para exportar el certificado del servidor de un cliente, especifique el mandato siguiente:
    ```
    psconf export -S -f /tmp/server.txt
    ```
14. Para actualizar el cliente que tiene una dirección IP de `11.11.11.11` a un nivel apropiado desde el servidor, especifique el mandato siguiente:
    ```
    psconf update -i 11.11.11.11
    ```
15. Para visualizar los estados de cliente, especifique el siguiente mandato:

```
psconf status
```

16. Para visualizar el certificado de cliente, especifique el mandato siguiente:
    ```
    psconf list -C
    ```
17. Para iniciar el cliente, especifique el siguiente mandato:
    ```
    psconf start client
    ```
18. Para visualizar la información de instantánea que se ha reunido con el submandato **clientData**, escriba el mandato siguiente:
    ```
    psconf clientData -l [ip|host]
    ```
19. Para visualizar el historial para el cliente de TNC, escriba el mandato siguiente:
    ```
    psconf list –H –i [ip|ALL]
    ```

Seguridad

Usuarios de RBAC de atención y usuarios de AIX fiables:

Este mandato puede realizar operaciones con privilegios. Sólo los usuarios privilegiados pueden ejecutar operaciones con privilegios. Para obtener más información sobre autorizaciones y privilegios, consulte Base de datos de mandatos con privilegios en Seguridad. Para obtener una lista de privilegios y las autorizaciones asociadas con este mandato, consulte el mandato **lssecattr** o el submandato **getcmdattr**

Mandato pscuiserverctl

Finalidad

Se utiliza para configurar las opciones de servidor de la GUI de PowerSC.

Sintaxis

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]

Distintivos

-r Reinicia el servidor de la GUI de PowerSC después de que se aplique un valor de parámetro.

set
Establece u obtiene una opción de servidor de la GUI de PowerSC.

Parámetros

httpPort ***númPuertoHttp***
Ver o especificar el puerto predeterminado utilizado por la GUI de PowerSC.

httpsPort ***númPuertoHttps***
Ver o especificar el puerto seguro predeterminado utilizado por la GUI de PowerSC.

administratorGroupList ***grupounix1,grupounix2,...***
Ver o especificar los grupos UNIX a los que se les permite realizar funciones de administrador utilizando la GUI de PowerSC.

logonGroupList ***grupounix1,grupounix2,...***
Ver o especificar los grupos UNIX a los que se les permite iniciar la sesión en la GUI de PowerSC.

powervcKeystoneUrl ***urlAlmacénClavesPowervc***
Ver o especificar el URL del servidor de almacén de claves de PowerVC.

QRadarSyslogResponseEnabled on | off
Ver el valor actual de registro Syslog de la GUI de PowerSC o establecer el registro Syslog en on (activado) y off (desactivado).

tncServer ***servidortnc.abc.com***
Ver o especificar el nombre de host del servidor de TNC. Si cambia el nombre de host del servidor de TNC, debe reiniciar el servidor de GUI de PowerSC.

Estado de salida

Este mandato devuelve los siguientes valores de salida:

0 Finalización satisfactoria.

>0 Se ha producido un error.

Ejemplos

1. Para ver lo que está actualmente especificado como el puerto predeterminado utilizado por la GUI de PowerSC:
   ```
   pscuiserverctl set httpPort
   ```
2. Para establecer el puerto predeterminado utilizado por la GUI de PowerSC:
   ```
   pscuiserverctl set httpPort 80
   ```
3. Para ver lo que está actualmente especificado como el puerto de seguridad predeterminado utilizado por la GUI de PowerSC:
   ```
   pscuiserverctl set httpsPort
   ```
4. Para ver el puerto de seguridad predeterminado utilizado por la GUI de PowerSC:
   ```
   pscuiserverctl set httpsPort 483
   ```
5. Para ver a qué grupos UNIX se les permite realizar funciones de administrador utilizando la GUI de PowerSC:
   ```
   pscuiserverctl set administratorGroupList
   ```
6. Para establecer los grupos UNIX a los que se les permite realizar funciones de administrador utilizando la GUI de PowerSC:
   ```
   pscuiserverctl set administratorGroupList securitygroup1,admingrp1
   ```
7. Para ver a qué grupos UNIX se les permite iniciar la sesión en la GUI de PowerSC:
   ```
   pscuiserverctl set logonGroupList
   ```
8. Para establecer los grupos UNIX a los que se les permite iniciar la sesión en la GUI de PowerSC:
   ```
   pscuiserverctl set logonGroupList unixgroup1,unixgrp2
   ```
9. Para ver el URL del servidor de almacén de claves de PowerVC:
   ```
   pscuiserverctl set powervcKeystoneUrl
   ```
10. Para establecer el URL del servidor de almacén de claves de PowerVC:
    ```
    pscuiserverctl set powervcKeystoneUrl https://powervc/server/example/
    ```
11. Para ver si registro Syslog de la GUI de PowerSC está activado o desactivado:

```
pscuiserverctl set QRadarSyslogResponseEnabled
```

12. Para establecer el registro Syslog de la GUI de PowerSC en activado o desactivado:

```
pscuiserverctl set QRadarSyslogResponseEnabled on
pscuiserverctl set QRadarSyslogResponseEnabled off
```

13. Para ver el nombre de host del servidor de TNC:

```
pscuiserverctl set tncServer
```

14. Para establecer el nombre de host del servidor de TNC:

```
pscuiserverctl set tncServer tncserver.abc.com
```

15. Para establecer el nombre de host del servidor de TNC es necesario reiniciar el servidor de la GUI de PowerSC. Para reiniciar el servidor de la GUI de PowerSC :

```
pscuiserverctl -r set tncServer tncs1.rs.com
```

Mandato pscxpert

Finalidad

Ayuda al administrador del sistema a establecer la configuración de seguridad.

Sintaxis

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 <Nivel> **[-p]** <**-a** *Archivo1* | **-n** *Archivo2* | **-a** *Archivo3* **-n** *Archivo4*>

pscxpert -f Profile **-a** File **[-p]**

pscxpert -d

Descripción

El mandato **pscxpert** establece diversos valores de configuración de sistema para habilitar el nivel de seguridad especificado.

La ejecución del mandato **pscxpert** con sólo el conjunto de distintivos **-l** implementa los valores de seguridad inmediatamente sin permitir que el usuario configure los valores. Por ejemplo, la ejecución del mandato **pscxpert -l high** aplica automáticamente al sistema todos los valores de seguridad de alto nivel. Sin embargo, la ejecución del mandato **pscxpert -l** con los distintivos **-n** y **-a** guarda los valores de seguridad en un archivo especificado por el parámetro *File*. Entonces el distintivo **-f** se aplica a las nuevas configuraciones.

Tras la selección inicial, se visualiza un menú que desglosa todas las opciones de configuración de seguridad que están asociadas con el nivel de seguridad seleccionado. Estas opciones se pueden aceptar en su totalidad o se pueden poner desactivar y activar individualmente. Tras los cambios secundarios, el mandato **pscxpert** continúa aplicando los valores de seguridad en el sistema.

Ejecute el mandato **pscxpert** como usuario root del Virtual I/O Server de destino. Cuando no haya iniciado la sesión como usuario root del Virtual I/O Server de destino, ejecute el mandato **oem_setup_env** antes de ejecutar el mandato.

Si ejecuta el mandato **pscxpert** cuando ya se está ejecutando otra instancia del mandato **pscxpert**, el mandato **pscxpert** sale con un mensaje de error.

Nota: Vuelva a ejecutar el mandato **pscxpert** después de realizar cambios importantes en el sistema, por ejemplo la instalación de actualizaciones de software. Si no se selecciona un elemento de configuración de seguridad concreto cuando se vuelva a ejecutar el mandato **pscxpert**, se saltará dicho elemento de configuración.

Distintivos

Elemento	Descripción
-a	Los valores con las opciones de nivel de seguridad asociadas se graban en el archivo especificado en un formato abreviado.
-c	Comprueba los valores de seguridad en el conjunto de reglas aplicado anteriormente. Si falla la comprobación de una regla, también se comprueban las versiones anteriores de la regla. Este proceso continúa hasta que se pasa la comprobación o hasta que se han comprobado todas las instancias de la regla fallida del archivo `/etc/security/aixpert/core/appliedaixpert.xml`. Puede ejecutar esta comprobación en cualquier perfil predeterminado o perfil personalizado.
-d	Visualiza la definición de tipo de documento (DTD).

Elemento	Descripción
-f	Aplica los valores de seguridad que se proporcionan en el archivo *Profile* especificado. Los perfiles se encuentran en el directorio `/etc/security/aixpert/custom`. Los perfiles disponibles incluyen los siguientes perfiles estándares: **DataBase.xml** Este archivo contiene los requisitos para los valores de base de datos predeterminados. **DoD.xml** Este archivo contiene los requisitos para los valores de Department of Defense Security Technical Implementation Guide (STIG). **DoD_to_AIXDefault.xml** Esto cambia los valores a los valores de AIX predeterminados. **DoDv2.xml** Este archivo contiene los requisitos para la versión 2 de los valores de la publicación Department of Defense Security Technical Implementation Guide (STIG). **DoDv2_to_AIXDefault.xml** Esto cambia los valores a los valores de AIX predeterminados. **Hipaa.xml** Este archivo contiene los requisitos para los valores de Health Insurance Portability and Accountability Act (HIPAA). **NERC.xml** Este archivo contiene los requisitos para los valores de North American Electric Reliability Corporation (NERC). **NERC_to_AIXDefault.xml** Este archivo cambia los valores de NERC por los valores de AIX predeterminados. **PCI.xml** Este archivo contiene los requisitos para los valores de Payment Card Industry Data Security Standard. **PCIv3.xml** Este archivo contiene los requisitos para los valores de Payment Card Industry Data Security Standard Versión 3. **PCI_to_AIXDefault.xml** Este archivo cambia los valores por los valores predeterminados de AIX. **PCIv3_to_AIXDefault.xml** Este archivo cambia los valores por los valores predeterminados de AIX. **SOX-COBIT.xml** Este archivo contiene los requisitos para los valores de la ley Sarbanes-Oxley y COBIT. También puede crear perfiles personalizados en el mismo directorio y aplicarlos a los valores cambiando el nombre y modificando los archivos XML existentes. Por ejemplo, el mandato siguiente se aplica al perfil HIPAA del sistema: `pscxpert -f /etc/security/aixpert/custom/Hipaa.xml` Cuando se especifica el distintivo **-f**, los valores de seguridad se aplican de forma coherente de sistema a sistema transfiriendo y aplicando de forma segura un archivo **appliedaixpert.xml** de sistema a sistema. Todas las reglas aplicadas correctamente se graban en el archivo `/etc/security/aixpert/core/appliedaixpert.xml` y las correspondientes reglas de acción `undo` se graban en el archivo `/etc/security/aixpert/core/undo.xml`.

Elemento	Descripción
-l	Establece los valores de seguridad de sistema en el nivel especificado. Este distintivo tiene las opciones siguientes: **h | high** Especifica las opciones de seguridad de alto nivel. **m | medium** Especifica las opciones de seguridad de nivel medio. **l | low** Especifica las opciones de seguridad de nivel bajo. **d | default** Especifica las opciones de seguridad de nivel estándar de AIX. **s | sox-cobit** Especifica las opciones de seguridad de la ley Sarbanes-Oxley y COBIT. Si especifica los distintivos **-l** y **-n**, los valores de seguridad no se implementa en el sistema; sin embargo, sólo se graban en el archivo especificado. Todas las reglas aplicadas correctamente se graban en el archivo `/etc/security/aixpert/core/appliedaixpert.xml` y las correspondientes reglas de acción de deshacer se graban en el archivo `/etc/security/aixpert/core/undo.xml`. **Atención:** Cuando se utiliza el distintivo **d | default**, el distintivo puede sobrescribir los valores de seguridad configurados que ha establecido previamente utilizando el mandato **pscxpert** o de forma independiente y restaura el sistema a su configuración abierta tradicional.
-n	Graba los valores con las opciones de nivel de seguridad asociadas en el archivo especificado.
-p	Especifica que la salida de las reglas de seguridad se mostrará utilizando la salida detallada. El distintivo **-p** registra las reglas que se procesan en el subsistema de auditoría si se activa la opción **auditing**. Esta opción se puede utilizar con cualquiera de los distintivos **-l**, **-u** **-c** y **-f**. El distintivo **-p** habilita la salida detallada en la terminal y el archivo aixpert.log.
-P	Acepta el nombre de perfil como entrada. Esta opción se utiliza junto con los distintivos **-c**. Los distintivos **-c** y **-P** se utilizan para comprobar la compatibilidad del sistema con el perfil pasado.
-r	Graba los valores existentes del sistema al archivo `/etc/security/aixpert/check_report.txt`. Puede utilizar la salida en informes de auditoría de seguridad o de conformidad. El informe describe cada valor, cómo puede relacionarse con un requisito de conformidad normativo, y si la comprobación ha sido correcta o ha fallado. **Nota:** • El distintivo -r sólo soporta la operación aplicar para los perfiles. No soporta la operación aplicar para los niveles. • La opción -r muestra el mensaje completo (uno o más líneas) para una regla.
-R	Produce la misma salida que el distintivo **-r**. Además, este distintivo también añade una descripción del script de regla o programa que se utiliza para implementar el valor de configuración. **Nota:** • El distintivo -R sólo soporta la operación aplicar para los perfiles. No soporta la operación aplicar para los niveles.
-t	Muestra el tipo del perfil que se aplica en el sistema.
-u	Deshace los valores de seguridad que se aplican. **Nota:** • No puede utilizar el distintivo **-u** para revertir la aplicación de los perfiles de DoD, DoDv2, NERC, PCI o PCIv3. Para eliminar estos perfiles una vez que se hayan añadido, aplique el perfil que finaliza con `_AIXDefault.xml`. Por ejemplo, para eliminar el perfil NERC.xml, debe aplicar el perfil NERC_to_AIXDefault.xml. • Los cambios en el sistema después de una operación aplicar se pierden con una operación de deshacer. Los valores vuelven al valor que existía antes de la operación aplicar.

Parámetros

Elemento	Descripción
Archivo	El archivo de salida que almacena los valores de seguridad. Se requiere permiso de root para acceder a este archivo.
Nivel	El nivel personalizado para comprobar los valores aplicados anteriormente.
Perfil	El nombre de archivo del perfil que proporciona reglas de conformidad para el sistema. Se requiere permiso de root para acceder a este archivo.

Seguridad

El mandato **pscxpert** sólo lo puede ejecutar root.

Ejemplos

1. Para grabar todas las opciones de seguridad de alto nivel en un archivo de salida, especifique el mandato siguiente:

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

   Después de ejecutar este mandato, se puede editar el archivo de salida y se pueden comentar roles de seguridad específicos escribiéndolos dentro de la serie de comentario de XML estándar (`<--` empieza el comentario y `-\>` cierra el comentario).
2. Para aplicar los valores de seguridad del archivo de configuración de Department of Defense STIG, especifique el mandato siguiente:

   ```
   pscxpert -f /etc/security/aixpert/custom/DoD.xml
   ```
3. Para aplicar los valores de seguridad desde el archivo de configuración HIPAA, especifique el mandato siguiente:

   ```
   pscxpert -f /etc/security/aixpert/custom/Hipaa.xml
   ```
4. Para comprobar los valores de seguridad del sistema y para registrar las reglas que han fallado en el subsistema de auditoría, especifique el mandato siguiente:

   ```
   pscxpert -c -p
   ```
5. Para comprobar el nivel personalizado de los valores de seguridad para el perfil de NERC en el sistema y para registrar las reglas que han fallado en el subsistema de auditoría, especifique el mandato siguiente:

   ```
   pscxpert -c -p -l NERC
   ```
6. Para generar informes y grabarlos en el archivo `/etc/security/aixpert/check_report.txt`, especifique el mandato siguiente:

   ```
   pscxpert -c -r
   ```

Ubicación

Elemento	Descripción
/usr/sbin/pscxpert	Contiene el mandato **pscxpert**.

Archivos

Elemento	Descripción
/etc/security/aixpert/log/aixpert.log	Contiene un registro de rastreo de los valores de seguridad aplicados. Este archivo no utiliza el estándar de syslog. El mandato **pscxpert** graba directamente en el archivo, tiene permisos de lectura y escritura y requiere seguridad root.
/etc/security/aixpert/log/firstboot.log	Contiene un registro de rastreo de los valores de seguridad que se han aplicado durante el primer arranque de una instalación de Secure by Default (SbD).
/etc/security/aixpert/core/undo.xml	Contiene un listado XML de valores de seguridad, que se puede deshacer.

Mandato rmvfilt

Finalidad

Elimina las reglas de filtro de cruce de LAN virtual de la tabla de filtros.

Sintaxis

rmvfilt -n [fid | all>]

Descripción

El mandato **rmvfilt** se utiliza para eliminar las reglas de filtro de cruce de LAN virtual de la tabla de filtros.

Distintivos

-n Especifica el ID de la regla de filtro que se eliminará. La opción **all** se utiliza para eliminar todas las reglas de filtro.

Estado de salida

Este mandato devuelve los siguientes valores de salida:

0 Finalización satisfactoria.

>0 Se ha producido un error.

Ejemplos

1. Para eliminar todas las reglas de filtro o desactivar todas las reglas de filtro del kernel, escriba el mandato como se indica a continuación:

   ```
   rmvfilt -n all
   ```

Conceptos relacionados:

"Desactivación de reglas" en la página 125
Puede desactivar las reglas que permiten el direccionamiento de VLAN cruzadas en la característica Cortafuegos fiable.

Mandato vlantfw

Finalidad

Muestra o borra la información de correlación de IP y Control de accesos a soporte (MAC) y controla la función de registro.

Sintaxis

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

Descripción

El mandato **vlantfw** visualiza o borra las entradas de correlación de IP y MAC. También proporciona la posibilidad de iniciar o detener el recurso de registro cortafuegos fiable.

Distintivos

-d Visualiza toda la información de correlación de IP.

-D Visualiza los datos de conexión recopilados.

-E Visualiza los datos de conexión entre las particiones lógicas (LPAR) en distintos complejos de procesador central.

-f Elimina toda la información de correlación de IP.

-F Borra la memoria caché de datos de conexión.

-G Visualiza las reglas de filtro que se pueden configurar para direccionar el tráfico internamente utilizando el cortafuegos fiable.

-I Visualiza los datos de conexión entre los LPAR que están asociados con distintos ID de VLAN, pero que comparten los mismos complejos de procesador centrales.

-l Inicia el recurso de registro de cortafuegos fiable.

-L Detiene el recurso de registro de cortafuegos fiable y redirige el contenido del archivo de rastreo al archivo `/home/padmin/svm/svm.log`.

-m Habilita la supervisión del cortafuegos fiable.

-M Inhabilita la supervisión del cortafuegos fiable.

-q Consulta el estado de máquina virtual segura.

-s Inicia el cortafuegos fiable.

-t Detiene el cortafuegos fiable.

Parámetros

-N *entero*
Visualiza la regla de filtro que se corresponde al entero que se especifica.

Estado de salida

Este mandato devuelve los siguientes valores de salida:

0 Finalización satisfactoria.

>0 Se ha producido un error.

Ejemplos

1. Para visualizar todas las correlaciones de IP, escriba el mandato como se indica a continuación:
   ```
   vlantfw -d
   ```
2. Para eliminar todas las correlaciones de IP, escriba el mandato como se indica a continuación:
   ```
   vlantfw -f
   ```
3. Para iniciar la función de registro de cortafuegos fiable, escriba el mandato como se indica a continuación:
   ```
   vlantfw -l
   ```
4. Para comprobar el estado de una máquina virtual segura, escriba el mandato como se indica a continuación:
   ```
   vlantfw -q
   ```
5. Para iniciar el cortafuegos fiable, escriba el mandato como se indica a continuación:
   ```
   vlantfw -s
   ```
6. Para detener el cortafuegos fiable, escriba el mandato como se indica a continuación:
   ```
   vlantfw -t
   ```
7. Para visualizar las reglas correspondientes que se pueden utilizar para generar filtros que direccionen el tráfico en el complejo de procesador central, escriba el mandato tal como se indica a continuación:
   ```
   vlantfw -G
   ```

Referencia relacionada:
"Mandato genvfilt" en la página 168

Avisos

Esta información se ha desarrollado para productos y servicios ofrecidos en los EE.UU.

Es posible que en otros países IBM no ofrezca los productos, servicios o características que se describen en este documento. Póngase en contacto con el representante de IBM para obtener información de los productos y servicios disponibles actualmente en su área. Las referencias a programas, productos o servicios de IBM no pretenden afirmar ni implicar que sólo puedan utilizarse dichos productos, programas o servicios de IBM. En su lugar, se puede utilizar cualquier producto, programa o servicio funcionalmente equivalente que no infrinja ningún derecho de propiedad intelectual de IBM. Sin embargo, es responsabilidad del usuario evaluar y verificar el funcionamiento de cualquier producto, programa o servicio que no sea de IBM.

IBM puede tener patentes o solicitudes de patentes pendientes que cubran la materia descrita en este documento. La entrega de este documento no le otorga ninguna licencia sobre estas patentes. Puede enviar consultas sobre licencias, por escrito, a:

IBM Director of Licensing
IBM Corporation
North Castle Drive, MD-NC119
Armonk, NY 10504-1785
EE.UU.

Para realizar consultas sobre licencias relativas a la información de juego de caracteres de doble byte (DBCS), póngase en contacto con el departamento de propiedad intelectual de IBM de su país o envíe las consultas, por escrito, a:

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

INTERNATIONAL BUSINESS MACHINES CORPORATION PROPORCIONA ESTA PUBLICACIÓN "TAL CUAL", SIN GARANTÍAS DE NINGUNA CLASE, NI EXPLÍCITAS NI IMPLÍCITAS, INCLUIDAS, PERO SIN LIMITARSE A, LAS GARANTÍAS IMPLÍCITAS DE NO INFRACCIÓN, COMERCIALIZACIÓN O IDONEIDAD PARA UNA FINALIDAD DETERMINADA. Algunas jurisdicciones no permiten la renuncia a las garantías explícitas o implícitas en determinadas transacciones; por lo tanto, es posible que esta declaración no sea aplicable en su caso.

Esta información puede contener imprecisiones técnicas o errores tipográficos. Periódicamente se efectúan cambios en la información aquí contenida; estos cambios se incorporarán en nuevas ediciones de la publicación. IBM puede realizar mejoras y/o cambios en los productos y/o programas descritos en esta publicación en cualquier momento, sin previo aviso.

Las referencias contenidas en esta información a sitios web no IBM sólo se proporcionan por comodidad del usuario y de ningún modo constituyen un respaldo de dichos sitios web. El material de esos sitios web no forma parte del material correspondiente a este producto de IBM y el uso de esos sitios web se realiza por cuenta y riesgo del usuario.

IBM puede utilizar o distribuir la información que se le proporcione del modo que considere conveniente sin incurrir por ello en ninguna obligación con el remitente.

Los titulares de licencia de este programa que deseen obtener información acerca del mismo con el fin de: (i) intercambiar la información entre programas creados de forma independiente y otros programas (incluido éste) y (ii) utilizar mutuamente la información que se ha intercambiado, deben ponerse en contacto con:

IBM Director of Licensing
IBM Corporation
North Castle Drive, MD-NC119
Armonk, NY 10504-1785
EE.UU.

Esta información puede estar disponible, sujeta a los términos y condiciones pertinentes, lo que incluye en algunos casos el pago de una cuota.

IBM proporciona el programa bajo licencia descrito en este documento y todo el material bajo licencia disponible para el mismo bajo los términos del Acuerdo de cliente de IBM, el Acuerdo internacional de programas bajo licencia de IBM o cualquier acuerdo equivalente entre las partes.

Los ejemplos de datos de rendimiento y de clientes citados se presentan solamente a efectos ilustrativos. Los resultados reales de rendimiento pueden variar en función de las configuraciones y las condiciones de funcionamiento específicas.

La información relativa a productos que no son de IBM se ha obtenido de los proveedores de esos productos, sus anuncios publicados y otras fuentes disponibles públicamente. IBM no ha probado esos productos y no puede confirmar la precisión de su rendimiento, su compatibilidad ni ningún otro aspecto. Las preguntas sobre las funciones de productos que no sean de IBM se deben dirigir a los proveedores de dichos productos.

Las declaraciones relacionadas con futuras tendencias o intenciones de IBM están sujetas a cambios o pueden retirarse sin previo aviso y representan únicamente metas y objetivos.

Todos los precios de IBM mostrados son precios de venta al detalle sugeridos por IBM, son actuales y están sujetos a cambio sin previo aviso. Los precios de los distribuidores pueden ser diferentes.

Esta información está destinada a utilizarse para la planificación. La información aquí contenida está sujeta a cambios antes de que los productos descritos estén disponibles.

Esta información contiene ejemplos de datos e informes utilizados en operaciones comerciales diarias. Para ilustrarlos de la manera más completa posible, los ejemplos incluyen nombres de personas, compañías, marcas y productos. Todos estos nombres son ficticios y cualquier parecido con personas o empresas comerciales es pura coincidencia.

LICENCIA DE COPYRIGHT:

Esta información contiene programas de aplicación de muestra en lenguaje fuente que ilustran las técnicas de programación en diversas plataformas operativas. Puede copiar, modificar y distribuir estos programas de muestra de cualquier forma sin pagar ninguna cuota a IBM, con el fin de desarrollar, usar, comercializar o distribuir programas de aplicación que se ajusten a la interfaz de programación de aplicaciones para la plataforma operativa para la que se han escrito los programas de muestra. Estos ejemplos no se han probado exhaustivamente bajo todas las condiciones. Por lo tanto, IBM no puede garantizar ni dar por implícita la fiabilidad, la capacidad de servicio o la funcionalidad de estos programas. Los programas de muestra se proporcionan "TAL CUAL", sin garantía de ninguna clase. IBM no será responsable de ningún daño resultante del uso de los programas de muestra.

Cada copia o parte de estos programas de muestra o cualquier trabajo derivado debe incluir una nota de copyright como la siguiente:

© (nombre de la empresa) (año).

Partes de este código proceden de programas de muestra de IBM Corp.

© Copyright IBM Corp. _escriba el año o los años_.

Consideraciones sobre la política de privacidad

Los productos de software de IBM, incluido el software que se ofrece como soluciones de servicio, ("Ofertas de software") pueden utilizar cookies u otras tecnologías para recopilar información de uso de producto, para ayudar a mejorar la experiencia de usuario final, para adaptar las interacciones con el usuario final o para otros propósitos. En muchos casos, las Ofertas de software no recopilan información de identificación personal. Algunas de nuestras Ofertas de software pueden ayudarle a habilitar la recopilación de información de identificación personal. Si esta Oferta de software utiliza cookies para recopilar información de identificación personal, a continuación se describe información específica sobre el uso de cookies por parte de esta oferta.

Esta oferta de software no utiliza cookies ni otras tecnologías para recopilar información de identificación personal.

Si las configuraciones desplegadas para esta Oferta de software le proporciona como cliente la posibilidad de recopilar información de identificación personal de los usuarios finales mediante cookies y otras tecnología, debe buscar asesoramiento jurídico sobre las leyes aplicables como la recopilación de datos, así como tener noción de los requisitos expresos de notificación y consentimiento.

Si desea obtener más información sobre el uso de varias tecnologías, incluyendo el uso de las cookies, para estos fines, consulte la Política de privacidad de IBM en http://www.ibm.com/privacy y las declaraciones de privacidad en línea de IBM en http://www.ibm.com/privacy/details, sección denominada “Cookies, Web Beacons and Other Technologies” e “IBM Software Products and Software-as-a-Service Privacy Statement” en http://www.ibm.com/software/info/product-privacy.

Marcas registradas

IBM, el logotipo de IBM e ibm.com son marcas registradas de International Business Machines Corp., registradas en muchas jurisdicciones en todo el mundo. Otros nombres de servicios y productos pueden ser marcas registradas de IBM u otras empresas. Una lista actual de marcas registradas de IBM está disponible en la web en Copyright and trademark information en www.ibm.com/legal/copytrade.shtml.

Linux es una marca registrada de Linus Torvalds en EE.UU. y/o en otros países.

Java y todas las marcas registradas y logotipos basados en Java son marcas registradas de Oracle y/o sus afiliados.

Índice

A

C

G

H

I

L

M

N

P

R

S

T

V

Impreso en España