IBM PowerSC

Standard Edition

1.1.6. változat

PowerSC Standard Edition

IBM PowerSC

Standard Edition

1.1.6. változat

PowerSC Standard Edition

Megjegyzés

A kiadvány és termék használata előtt olvassa el a “Nyilatkozatok” oldalszám: 171 rész információit.

Ez a kiadás az IBM PowerSC Standard Edition 1.1.6. változatára és az összes ezt követő kiadásra és módosításra vonatkozik, amíg azt a következő kiadások másképp nem jelzik.

Tartalom

A kiadványról

Ez a dokumentum átfogó fájl, rendszer és hálózati biztonsági információkat tartalmaz a rendszeradminisztrátorok számára.

Kiemelés

A dokumentum az alábbi kiemelési megállapodásokat használja:

Félkövér	Parancsokat, szubrutinokat, kulcsszavakat, fájlokat szerkezeteket, könyvtárakat és a rendszer által előre meghatározott nevű egyéb elemeket jelöl. Felhasználó által kijelölt grafikus objektumokat, például nyomógombokat, címkéket és ikonokat is azonosít.
Dőlt	Olyan paramétereket jelöl, amelyek tényeleges nevét vagy értékét a felhasználónak kell megadnia.
Monospace betűtípus	Adott adatértékekre vonatkozó példákat, a ténylegesen megjelenő szövegekhez hasonló mintaszövegeket, a programozók által felhasználható kódrészleteket, rendszerüzeneteket vagy ténylegesen begépelt információkat jelöl.

Kis- és nagybetűk megkülönböztetése az AIX rendszeren

Az AIX operációs rendszeren a kis- és nagybetűk mindenhol különbözőknek számítanak. Például a fájlokat az **ls** parancscsal listázhatjuk ki. Ha beírja az LS parancsot, akkor a rendszer azt a választ adja, hogy a parancs nem található. Ugyanígy a FILEA, FiLea és filea három különböző fájlnév még akkor is, ha ugyanabban a könyvtárban találhatók. Nemkívánatos események elkerülésének érdekében mindig ügyeljen a betűk írására.

ISO 9000

A termék fejlesztése és gyártása az ISO 9000 regisztrált minőségbiztosítási rendszerek felhasználásával történt.

PowerSC Standard Edition újdonságai

Ismerje meg a PowerSC Standard Edition változat témakörgyűjteményének új vagy jelentősen megváltozott információit.

Ebben a PDF fájlban az új és módosított információk mellett függőleges vonal (|) látható a bal oldalon.

2017. szeptember

A PowerSC grafikus felületéhez a következő szolgáltatások lettek hozzáadva:

- Hozzáadásra kerül egy felső szintű Biztonsági és megfelelési műszerfal, amely biztosítja az összes megfelelési és valós idejű fájlintegritási állapotinformációk azonnali összegzését.
- Hozzáadott integráció olyan virtualizációkezelőkkel, mint például a PowerVC nyílt verem integráción keresztül, amely a végpontok automatikus és biztonságos feltérképezését biztosítja. Ezenkívül az integráció támogatja a felhős környezetet biztonsági láthatósággal a VM létrehozás első pillanatától kezdve.
- Hozzáadott jelentéskészítési képességek a felülvizsgálatok támogatásához. Áttekintő és részletes megfelelési és fájlintegritási jelentések érhetők el formázott HTML és CSV fájlként. A jelentések terjesztése ütemezhető azonnal vagy naponta.
- Bővített profilszerkesztő növeli a megfelelési szabályok és profilok személyre szabási képességét. A szabályok most már több forrásból is kombinálhatók és módosíthatók a grafikus felületen keresztül.
- Hozzáadott integráció olyan Biztonsági esemény információs kezelővel, mint például a QRadar. A rendszernapló bejegyzések biztosítása a jelentős megfelelési és fájlintegritási eseményekhez lehetővé teszi az egyszerű integrációt.
- Tökéletesített VISSZAVONÁS képességek segítenek az alkalmazott profil visszavonási összetett feladat leegyszerűsítésében. A PowerSC 1.1.6 jelentős lépéseket tett a zökkenőmentes VISSZAVONÁS képességért a PCI profillal.
- Tökéletesített grafikus felület méretezhetőség a megfelelés érdekében. A grafikus felület szerver vízszintesen méretezhető, és minden egyes példány legalább 1000 vagy több végpontot támogat.

A következő szolgáltatások lettek hozzáadva a Megbízható hálózati kapcsolat javításkezeléshez (TNCPM):

- Proxy szerver, amely további biztonsági réteget biztosít a TNCPM elkülöníthetőségével az Internettől.
- A köztes javítások (iFixes) integrációja a TNCPM-be most már teljesen automatikus. A TNCPM anélkül tudja figyelni és javítani az operációs rendszerre vonatkozó sebezhetőségeket, hogy felhasználói beavatkozásra lenne szükség.
- A nyílt forrású csomagok letöltése most már a TNCPM-be van integrálva, körvonalazva a nyílt forrású munkafolyamatot.

A megfelelési képességek kibővítéséhez a következő szolgáltatások lettek hozzáadva:

- Olyan jelentési opció, amely részleteket nyújt a profilban tartalmazott szabályokról a profil alkalmazásakor.

PowerSC Standard Edition PDF fájljai

A PowerSC Standard Edition dokumentációja megtekinthető PDF fájlként.

- PowerSC Standard Edititon
- PowerSC Standard Edition kiadási tájékoztató

PowerSC Standard Edition fogalmak

A PowerSC Standard Edition jelen áttekintése a szolgáltatásokat, összetevőket és a PowerSC Standard Edition szolgáltatásra vonatkozó hardvertámogatást mutatja be.

A PowerSC Standard Edition egy felhőn belül vagy virtualizált adatközpontokban működő rendszerek biztonságát és vezérlését biztosítja, valamint egy vállalati nézetet és felügyeleti képességeket nyújt. A PowerSC Standard Edition egy Biztonság és megfelelés automatizálás, Megbízható rendszerbetöltés, Megbízható tűzfal, Megbízható naplózás valamint Megbízható hálózati kapcsolat és javításkezelés összetevőket tartalmazó szolgáltatáscsomag. A virtualizációs rétegben elhelyezett biztonsági technológia további biztonságot nyújt önálló rendszereknek.

A következő táblázat bemutatja az egyes kiadások részleteit, a kiadásokban tartalmazott szolgáltatásokat, valamint a processzor alapú hardvert, amelyen az egyes összetevők elérhetők.

1. táblázat: PowerSC Standard Edition összetevők, leírás, operációs rendszer támogatás és hardvertámogatás

Összetevők	Leírás	Támogatott operációs rendszer	Támogatott hardver
Biztonság és megfelelés automatizálás	A következő szabványok esetén automatizálja a biztonsági és megfelelési konfiguráció beállításait, megfigyelését és felülvizsgálatát: • Fizetőkártya ipari adatbiztonsági szabvány (PCI DSS) • Sarbanes-Oxley törvény és COBIT szabvány (SOX/COBIT) • USA Védelmi minisztérium (DoD) STIG • Az egészségbiztosítás hordozhatóságát és elszámoltathatóságát előíró törvény (HIPAA)	• AIX 5.3 • AIX 6.1 • AIX 7.1 • AIX 7.2	• POWER5 • POWER6 • POWER7 • POWER8
Megbízható rendszerbetöltés	A rendszerbetöltési képfájlt, az operációs rendszert és az alkalmazásokat méri, és ezek megbízhatóságát a Virtuális megbízható platform modul (TPM) technológia használatával hitelesíti.	• AIX 6 with 6100-07 vagy újabb • AIX 7 with 7100-01 vagy újabb	POWER7 firmware eFW7.4 vagy újabb
Megbízható tűzfal	Időt és erőforrásokat takarít meg azzal, hogy lehetővé teszi a közvetlen továbbítást megadott virtuális helyi hálózatok (VLAN) között, amelyeket ugyanaz a Virtual I/O Server vezérel.	• AIX 6.1 • AIX 7.1 • AIX 7.2 • VIOS 2.2.1.4 vagy újabb változat	• POWER6 • POWER7 • POWER8 • Virtual I/O Server 6.1S vagy újabb változat
Megbízható naplózás	Az AIX naplói központilag, valós időben a Virtuális I/O szerveren (VIOS) találhatók. Ez a szolgálatás hamisíthatatlan naplózást és a naplók kényelmes biztonsági mentését és kezelését biztosítja.	• AIX 5.3 • AIX 6.1 • AIX 7.1 • AIX 7.2	• POWER5 • POWER6 • POWER7 • POWER8

1. táblázat: PowerSC Standard Edition összetevők, leírás, operációs rendszer támogatás és hardvertámogatás (Folytatás)

Összetevők	Leírás	Támogatott operációs rendszer	Támogatott hardver
Megbízható hálózati kapcsolat és javításkezelés	Ellenőrzi, hogy a virtuális környezetben lévő minden AIX rendszer a megadott szoftver- és javítási szinten van-e, és felügyeleti eszközöket nyújt annak biztosításához, hogy minden AIX rendszer a megadott szoftver szinten legyen. Riasztásokat biztosít, ha egy alacsonyabb szintű virtuális rendszer hozzáadásra kerül a hálózathoz, vagy ha a rendszereket érintő biztonsági javítás jelenik meg.	• AIX 5.3 • AIX 6.1 • AIX 7.1 • AIX 7.2	• POWER5 • POWER6 • POWER7 • POWER8
Megbízható hálózati kapcsolat kliens	A Megbízható hálózati kapcsolat klienshez az operációs rendszerrel felsorolt összetevők egyike szükséges:	• AIX 6.1 with 6100-06 vagy újabb • AIX 7.1 változatú Szolgáltatásfrissítés-kezelő segéd (SUMA) konzol rendszer a SUMA környezeten belül, a javításkezeléshez • AIX 7.2.1 változatú Szolgáltatásfrissítés-kezelő segéd (SUMA) konzol rendszer a SUMA környezeten belül, a javításkezeléshez	

PowerSC Standard Edition telepítése

A PowerSC Standard Edition minden egyes adott funkciójához telepítenie kell egy fájlkészletet.

A PowerSC Standard Edition és PowerSC grafikus felhasználói felület (GUI) termékhez a következő fájlkészletek érhetők el:

- powerscStd.ice: Olyan AIX rendszereken telepíthető, amelyek igénylik a PowerSC Standard Edition Biztonság és megfelelés automatizálása szolgáltatást. A megfelelési program legalább 5 MB szabad lemezterületet igényel a(z) "/" fájlrendszeren.
- powerscStd.vtpm: Olyan AIX rendszereken van telepítve, amelyek a PowerSC Standard Edition Megbízható rendszerbetöltés szolgáltatását igénylik. A powerscStd.vtpm fájlkészlet megtalálható az AIX alapmédián vagy a https://www-01.ibm.com/marketing/iwm/iwm/web/preLogin.do?source=aixbp&S_PKG=vtpm webhelyen.
- powerscStd.vlog: Olyan AIX rendszereken van telepítve, amelyek a PowerSC Standard Edition Megbízható naplózás szolgáltatását igénylik.
- powerscStd.tnc_pm: AIX 7.1. változat TL4 vagy újabb rendszeren telepíthető a Service Update Management Assistant (SUMA) konzolrendszerrel együtt SUMA környezetben, a 7.2.1.0-ás javításkezeléshez. A Curl 7.52.1-1 a TNC javításkezelőn telepíthető az ifix-ek sikeres átviteléhez az IBM biztonsági webhelyéről.
- powerscStd.svm: Olyan AIX rendszereken van telepítve, amelyek számára hasznos lehet a PowerSC Standard Edition útválasztási szolgáltatása.
- powerscStd.rtc: Olyan AIX rendszereken telepíthető, amelyek a PowerSC Standard Edition Valós idejű megfelelés szolgáltatását igénylik.
- powerscStd.uiAgent.rte: Olyan AIX rendszereken telepíthető, amelyek kezelése az PowerSC grafikus felhasználói felület (GUI) használatával történik. A powerscStd.uiAgent.rte 116 telepítéséhez a powerscStd.ice 115 vagy újabb fájlkészlet szükséges.
- powerscStd.uiServer.rte: Olyan AIX rendszeren telepíthető, amely specifikusan az PowerSC grafikus felhasználói felület (GUI) szerver futtatására lett beállítva.

A PowerSC Standard Edition és PowerSC grafikus felhasználói felület (GUI) az alábbi felületek egyikével telepíthető:

- Az **installp** parancs a parancssori felületről (CLI)
- Az SMIT felület

A PowerSC Standard Edition telepítéséhez az SMIT felület használatával, tegye a következőket:

1. Futtassa a következő parancsot:
   ```
   % smitty installp
   ```
2. Válassza ki a **Szoftver telepítése** beállítást.
3. Válassza ki a bemeneti eszközt vagy könyvtárat a szoftverhez az IBM Compliance Expert telepítőkészlet helyének és telepítési fájljának megadásához. Ha például a telepítőkészlet könyvtárútvonala és fájlneve /usr/sys/inst.images/powerscStd.vtpm, akkor a **BEMENET** mezőben a fájlútvonalat kell megadnia.
4. Tekintse meg és fogadja el a licencszerződést. A licencszerződés elfogadásához a lefelé mutató nyíl használatával jelölje ki az **Új licencszerződések ELFOGADÁSA** beállítást, majd a Tab billentyű lenyomásával váltson át az **Igen** értékre.
5. A telepítés indításához nyomja meg az **Enter** billentyűt.
6. A telepítés befejeződése után győződjön meg róla, hogy a parancs állapota **OK**.

További információkért tekintse meg a “PowerSC GUI telepítése” oldalszám: 126 részt az PowerSC grafikus felhasználói felület (GUI) telepítésével kapcsolatban.

Szoftverlicenc megtekintése

A szoftverlicenc a CLI felületen a következő parancs használatával tekinthető meg:

```
% installp –lE –d
útvonal/fájlnév
```

Ahol *útvonal/fájlnév* a PowerSC Standard Edition telepítőkészletet adja meg.

Például a CLI felületen a következő parancsot írhatja be a PowerSC Standard Edition termék licencinformációinak megadásához:

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

Kapcsolódó fogalmak:

“PowerSC Standard Edition fogalmak” oldalszám: 5
A PowerSC Standard Edition jelen áttekintése a szolgáltatásokat, összetevőket és a PowerSC Standard Edition szolgáltatásra vonatkozó hardvertámogatást mutatja be.

“Megbízható rendszerbetöltés telepítése” oldalszám: 95
A Megbízható rendszerbetöltés telepítéséhez szükségesek bizonyos hardver- és szoftverkonfigurációk.

Kapcsolódó feladatok:

“Megbízható tűzfal telepítése” oldalszám: 101
A PowerSC Megbízható tűzfal telepítése hasonló a többi PowerSC szolgáltatás telepítéséhez.

“Megbízható naplózás telepítése” oldalszám: 108
A PowerSC Megbízható naplózás szolgáltatását a parancssori felület vagy az SMIT eszköz használatával telepítheti.

“TNC összetevők beállítása” oldalszám: 114
A Megbízható hálózati kapcsolat (TNC) összetevőit be kell állítani egy adott környezetben történő futtatásra.

Biztonság és megfelelés automatizálása

Az AIX Profile Manager kezeli az előre meghatározott profilokat a biztonság és a megfelelés érdekében. A PowerSC Real Time Compliance folyamatosan figyeli a támogatással rendelkező AIX rendszereket és biztosítja, hogy konzisztensen és biztonságosan legyenek beállítva.

Az XML profilok automatizálják az IBM által javasolt AIX rendszerkonfigurációt, hogy az konzisztens legyen a Fizetőkártya adatbiztonsági szabvánnyal, a Sarbanes-Oxley törvénnyel és az Amerikai Department of Defense UNIX biztonságtechnikai megvalósítási kézikönyvvel, valamint a Health Insurance Portability and Accountability Act (HIPAA) törvénnyel. A biztonsági szabványoknak megfelelő szervezeteknek az előre meghatározott rendszerbiztonsági beállításokat kell használni.

Az AIX Profile Manager úgy működik, mint egy IBM® Systems Director bedolgozó, amely leegyszerűsíti a biztonsági beállítások alkalmazását, a biztonsági beállítások figyelését és a biztonsági beállítások felülvizsgálatát az AIX operációs rendszeren és a Virtual I/O Server (VIOS) rendszereken. A biztonsági megfelelési szolgáltatás használatához a PowerSC alkalmazásnak telepítve kell lenni az AIX felügyelt rendszereken, amelyek megfelelnek a biztonsági szabványoknak. A biztonság és megfelelés automatizálása szolgáltatást tartalmazza a PowerSC Standard Edition.

A PowerSC Standard Edition 5765-PSE telepítőcsomagot kell telepíteni az AIX felügyelt rendszereken. A telepítőcsomag telepíti a powerscStd.ice fájlkészletet, amely a rendszeren az AIX Profile Manager vagy a **pscxpert** parancs használatával valósítható meg. A PowerSC számára az IBM Compliance Expert Express (ICEE) megfeleléssel engedélyezett az XML profilok kezelése és továbbfejlesztése. Az XML profilokat az AIX Profile Manager kezeli.

Megjegyzés: A biztonsági profil alkalmazása előtt az összes alkalmazást telepítse a rendszeren.

Biztonság és megfelelés automatizálásának alapelvei

A PowerSC biztonsági és megfelelési szolgáltatás egy automatizált módszer az AIX rendszerek konfigurálására és megfigyelésére az Amerikai Department of Defense (DoD) Security Technical Implementation Guide (STIG), a Fizetőkártya iparág (PCI) adatbiztonsági szabvány (DSS), a Sarbanes-Oxley törvény, a COBIT megfelelés (SOX/COBIT), valamint a Health Insurance Portability and Accountability Act (HIPAA) előírásainak megfelelően.

A PowerSC segít automatizálni a rendszerek beállítását és megfigyelését, amelyeknek meg kell felelni a Payment Card Industry (PCI) data security standard (DSS) 1.2, 2.0. vagy 3.0. változatának. A PowerSC biztonsági és megfelelési szolgáltatás egy pontos és teljes módszere a biztonsági konfiguráció automatizálásának, amely az IT megfelelési követelmények teljesítésére szolgál a DoD UNIX STIG, PCI DSS, Sarbanes-Oxley törvény, COBIT megfelelés (SOX/COBIT) és a Health Insurance Portability and Accountability Act (HIPAA) rendelkezései szerint.

Megjegyzés: A PowerSC biztonság és megfelelés frissíti az IBM Compliance Expert Express (ICEE) kiadás által használt XML profilokat. A PowerSC Standard Edition XML profilokat használhatja a **pscxpert** paranccsal az ICEE-hez hasonlóan.

A PowerSC Standard Edition termékkel együtt szállított előre beállított megfelelési profilok, mint specifikus rendszerkonfigurációs paraméterek, csökkentik a megfelelési dokumentáció értelmezésének és a szabványok megvalósításának adminisztrációs terhelését. Ez a technológia a folyamatok automatizálásával csökkenti a megfelelési konfiguráció és auditálás költségeit. Az IBMPowerSC Standard Edition úgy lett tervezve, hogy hatékonyan segítse a külső szabvány megfeleléssel társított rendszerkövetelmények kezelését, amely jelentősen csökkenti a költségeket és növeli a megfelelést.

Department of Defense STIG megfelelés

Az USA Védelmi minisztériuma (DoD) megköveteli a biztonságos számítógéprendszereket. Ez a DoD által meghatározott biztonsági és minőségi szint megfelel az AIX on Power Systems szerver minőségének és ügyfélkezelési alapjának.

A biztonságos operációs rendszert, például az AIX operációs rendszert pontosan kell beállítani annak érdekében, hogy megfeleljen a megadott biztonsági céloknak. A DoD meghatározta az összes operációs rendszer biztonsági beállításának szükségességét a 8500.1-es direktívában. Ez a direktíva kialakította az irányelvet és kiutalta a felelősséget az USA Defense Information Security Agency (DISA) ügynökségének, akik meghatározták a biztonsági konfigurációs segédletet.

A DISA kifejlesztette és meghatározta az alapelveket és irányelveket a UNIX Security Technical Implementation Guide (STIG) útmutatóban, amely a DoD rendszerek biztonsági követelményeinek megfelelő vagy őket meghaladó környezetet biztosít. Ezek a rendszerek érzékeny információkat tartalmazó Mission Assurance Category (MAC) II érzékenységi szinten működnek. Az USA DoD részlege szigorú IT biztonsági követelményeket támaszt és felsorolja a szükséges konfigurációs beállításokat, amelyek biztosítják a rendszerek biztonságos működtetését. A szükséges szakértői segédlet hozzáférhető. A PowerSC Standard Edition segít a beállítások konfigurálásának automatizálási folyamatában, a DoD által meghatározottak alapján.

Megjegyzés: Az összes olyan egyéni parancsfájl, amely a DoD megfelelés teljesítésének céljából lett megadva, a /etc/security/pscexpert/dodv2 könyvtárban található.

A PowerSC Standard Edition támogatja az AIX DoD STIG 1. változat 2. kiadásának követelményeit. A követelmények összegzése és a megfelelés teljesítésének módja az alábbi táblázatokban található.

2. táblázat: DoD általános követelmények

Department of Defense STIG ellenőrzési pont azonosító	**STIG szabály kategóriája**	**Leírás**	**A parancsfájl helye, ahol a művelet meg van határozva, valamint a művelet eredménye, amely lehetővé teszi a megfelelést**
AIX00020	2	Meg kell valósítani az AIX Megbízható számítástechnikai alapkörnyezet szoftvert.	**Hely** /etc/security/pscexpert/dodv2/trust **Megfelelési művelet** Biztosítja, hogy a rendszer megfeleljen a megadott követelményeknek.
AIX00040	2	A **securetcpip** parancsot kell használni.	**Hely** /etc/security/pscexpert/dodv2/dodsecuretcpip **Megfelelési művelet** Biztosítja, hogy a rendszer megfeleljen a megadott követelményeknek.
AIX00060	2	A rendszeren hetente kell ellenőrizni a jogosulatlan setuid fájlokat, valamint a jogosulatlan módosításokat a hitelesített setuid fájlokban.	**Hely** /etc/security/pscexpert/dodv2/trust **Megfelelési művelet** Heti ellenőrzés a megadott fájlokban végzett módosítások azonosításához.
AIX00080	1	A SYSTEM attribútumot tilos *none* értékre beállítani az összes fiók esetében.	**Hely** /etc/security/pscexpert/dodv2/SYSattr **Megfelelési művelet** Biztosítja, hogy a megadott attribútum ne *none* értékre kerüljön beállításra. **Megjegyzés:** Ez a beállítás nem módosul automatikusan, ha az irányelv visszaállításra kerül az AIX alapértelmezett irányelvre, a DoDv2_to_ használatával az AIXDefault.xml fájlhoz. Ezt a beállítást kézzel kell módosítani.
AIX00200	2	A rendszer nem engedélyezheti a közvetlen üzenetszórás áthaladását az átjárón keresztül.	**Hely** /etc/security/pscexpert/dodv2/ntwkoptsdod **Megfelelési művelet** A direct_broadcast hálózati opció beállítása *0* értékre.

2. táblázat: DoD általános követelmények (Folytatás)

Department of Defense STIG ellenőrzési pont azonosító	**STIG szabály kategóriája**	**Leírás**	**A parancsfájl helye, ahol a művelet meg van határozva, valamint a művelet eredménye, amely lehetővé teszi a megfelelést**
AIX00210	2	A rendszernek védelmet kell nyújtani az Internet vezérlőüzenet protokoll (ICMP) támadások ellen a TCP kapcsolatokon.	**Hely** /etc/security/pscexpert/dodv2/ntwkoptsdod **Megfelelési művelet** A tcp_icmpsecure hálózati opció beállítása *1* értékre.
AIX00220	2	A rendszernek védelmet kell nyújtani a TCP veremhez a kapcsolati visszaállítások, szinkronizálások (SYN) és a kódbeszúrásos támadások ellen.	**Hely** /etc/security/pscexpert/dodv2/ntwkoptsdod **Megfelelési művelet** Biztosítja, hogy a tcp_tcpsecure hálózati opció *7* értékre legyen beállítva.
AIX00230	2	A rendszernek védelmet kell nyújtani az IP felosztási támadások ellen.	**Hely** /etc/security/pscexpert/dodv2/ntwkoptsdod **Megfelelési művelet** Az ip_nfrag hálózati opció beállítása *200* értékre.
AIX00300	1,2,3	A rendszeren nem lehet aktív a bootp szolgáltatás.	**Hely** /etc/security/pscexpert/dodv2/inetdservices **Megfelelési művelet** A megadott szolgáltatás letiltása.
AIX00310	2	Az /etc/ftpaccess.ctl fájloknak létezni kell.	**Hely** /etc/security/pscexpert/dodv2/dodv2loginherald **Megfelelési művelet** Biztosítja, hogy a fájl létezzen.
GEN000020	2	A rendszernek hitelesítést kell megkövetelni egyetlen felhasználós módban.	**Hely** /etc/security/pscexpert/dodv2/rootpasswd_home **Megfelelési művelet** Biztosítja, hogy a root fiókhoz minden betölthető partícióhoz be legyen állítva egy jelszó az /etc/security/passwd fájlban. **Megjegyzés:** Ez a beállítás nem módosul automatikusan, ha az irányelv visszaállításra kerül az AIX alapértelmezett irányelvre, a DoDv2_to_ használatával az AIXDefault.xml fájlhoz. Ezt a beállítást kézzel kell módosítani.
GEN000100	1	Az operációs rendszernek támogatott kiadásnak kell lenni.	**Hely** /etc/security/pscexpert/dodv2/dodv2cat1 **Megfelelési művelet** A megadott szabálytesztelések eredményeinek megjelenítése.
GEN000120	2	Telepítve kell lenni a legújabb rendszerbiztonsági javításoknak és frissítéseknek.	**Hely** /usr/sbin/instfix -i /etc/security/pscexpert/dodv2/dodv2cat1 **Megfelelési művelet** Ez a Trusted Network Connect (megbízható hálózati kapcsolat) szolgáltatással állítható be.
GEN000140	2	A rendszeren hetente kell ellenőrizni a jogosulatlan setuid fájlokat, valamint a jogosulatlan módosításokat a hitelesített setuid fájlokban.	**Hely** /etc/security/pscexpert/dodv2/trust **Megfelelési művelet** Heti ellenőrzés a megadott fájlokban végzett módosítások azonosításához.

2. táblázat: DoD általános követelmények (Folytatás)

Department of Defense STIG ellenőrzési pont azonosító	**STIG szabály kategóriája**	**Leírás**	**A parancsfájl helye, ahol a művelet meg van határozva, valamint a művelet eredménye, amely lehetővé teszi a megfelelést**
GEN000220	2	A rendszeren hetente kell ellenőrizni a jogosulatlan setuid fájlokat, valamint a jogosulatlan módosításokat a hitelesített setuid fájlokban.	**Hely** /etc/security/pscexpert/dodv2/trust **Megfelelési művelet** Heti ellenőrzés a megadott fájlokban végzett módosítások azonosításához.
GEN000240	2	A rendszerórát szinkronizálni kell egy hiteles Department of Defense (DoD) időforrással.	**Hely** /etc/security/pscexpert/dodv2/dodv2cmntrows **Megfelelési művelet** A rendszeróra szabványi megfelelésének biztosítása.
GEN000241	2	A rendszerórát folyamatosan szinkronizálni kell, vagy legalább naponta.	**Hely** /etc/security/pscexpert/dodv2/dodv2cmntrows **Megfelelési művelet** A rendszeróra szabványi megfelelésének biztosítása.
GEN000242	2	A rendszernek az óraszinkronizáláshoz legalább két időforrást kell használni.	**Hely** /etc/security/pscexpert/dodv2/dodv2netrules **Megfelelési művelet** Biztosítja, hogy több időforrás is felhasználásra kerüljön az óra szinkronizálásához.
GEN000280	2	A közvetlen bejelentkezés nem engedélyezhető a következő fióktípusokba: • alkalmazás • alapértelmezett • osztott • segédprogram	**Hely** /etc/security/pscexpert/dodv2/lockacc_rlogin **Megfelelési művelet** A közvetlen bejelentkezések megakadályozása a megadott fiókokba.
GEN000290	2	A rendszeren nem lehetnek szükségtelen fiókok.	**Hely** /etc/security/pscexpert/dodv2/lockacc_rlogin **Megfelelési művelet** Biztosítja, hogy ne legyenek használaton kívüli fiókok.
GEN000300 (a következőkhöz kapcsolódik: GEN000320, GEN000380, GEN000880)	2	A rendszeren minden fióknak egyedi felhasználói- vagy fióknévvel, illetve egyedi felhasználói- vagy fiók jelszóval kell rendelkezni.	**Hely** /etc/security/pscexpert/dodv2/grpusrpass_chk **Megfelelési művelet** Biztosítja, hogy minden fiók megfeleljen a megadott követelményeknek. **Megjegyzés:** Ez a beállítás nem módosul automatikusan, ha az irányelv visszaállításra kerül az AIX alapértelmezett irányelvre, a DoDv2_to_ használatával az AIXDefault.xml fájlhoz. Ezt a beállítást kézzel kell módosítani.
GEN000320 (a következőkhöz kapcsolódik: GEN000300, GEN000380, GEN000880)	2	A rendszeren minden fióknak egyedi felhasználói- vagy fióknévvel, illetve egyedi felhasználói- vagy fiók jelszóval kell rendelkezni.	**Hely** /etc/security/pscexpert/dodv2/grpusrpass_chk **Megfelelési művelet** Biztosítja, hogy minden fiók megfeleljen a megadott követelményeknek. **Megjegyzés:** Ez a beállítás nem módosul automatikusan, ha az irányelv visszaállításra kerül az AIX alapértelmezett irányelvre, a DoDv2_to_ használatával az AIXDefault.xml fájlhoz. Ezt a beállítást kézzel kell módosítani.

2. táblázat: DoD általános követelmények (Folytatás)

Department of Defense STIG ellenőrzési pont azonosító	STIG szabály kategóriája	Leírás	A parancsfájl helye, ahol a művelet meg van határozva, valamint a művelet eredménye, amely lehetővé teszi a megfelelést
GEN000340	2	A rendszerfiókokhoz fenntartott felhasználói azonosítók (UID-k) és csoportazonosítók (GID-ek) nem rendelhetők hozzá nem rendszer fiókokhoz és nem rendszer csoportokhoz.	**Hely** /etc/security/pscexpert/dodv2/account **Megfelelési művelet** Ez a beállítás automatikusan engedélyezett a szabály betartatása érdekében.
GEN000360	2	A rendszerfiókokhoz fenntartott UID-k és GID-ek nem rendelhetők hozzá nem rendszer fiókokhoz és nem rendszer csoportokhoz.	**Hely** /etc/security/pscexpert/dodv2/account **Megfelelési művelet** Ez a beállítás automatikusan engedélyezett a szabály betartatása érdekében.
GEN000380 (a következőkhöz kapcsolódik: GEN000300, GEN000320, GEN000880)	2	A rendszeren minden fióknak egyedi felhasználói- vagy fióknévvel, illetve egyedi felhasználói- vagy fiók jelszóval kell rendelkezni.	**Hely** /etc/security/pscexpert/dodv2/grpusrpass_chk **Megfelelési művelet** Biztosítja, hogy minden fiók megfeleljen a megadott követelményeknek.
GEN000400	2	A Department of Defense (DoD) bejelentkezési fejléccsíknak meg kell jelenni közvetlenül a konzol bejelentkezési parancssorai előtt vagy annak részeként.	**Hely** /etc/security/pscexpert/dodv2/dodv2loginherald **Megfelelési művelet** A szükséges fejléccsík megjelenítése.
GEN000402	2	A DoD bejelentkezési fejléccsíknak meg kell jelenni közvetlenül a grafikus asztali környezet bejelentkezési parancssorai előtt vagy annak részeként.	**Hely** /etc/security/pscexpert/dodv2/dodv2loginherald **Megfelelési művelet** A bejelentkezési fejléccsík a Department of Defense fejléccsíkra van beállítva.
GEN000410	2	A rendszeren a Fájlátviteli protokoll SSL-en keresztül (FTPS) és a Fájlátviteli protokoll (FTP) szolgáltatást a DoD bejelentkezési fejléccsíkkal kell beállítani.	**Hely** /etc/security/pscexpert/dodv2/dodv2loginherald **Megfelelési művelet** A fejléccsík megjelenítése FTP használata esetén.
GEN000440	2	A bejelentkezés és a kijelentkezés sikeres és sikertelen kísérleteit rögzíteni kell.	**Hely** /etc/security/pscexpert/dodv2/loginout **Megfelelési művelet** A szükséges naplózás engedélyezése.
GEN000452	2	A rendszernek minden egyes bejelentkezéskor meg kell jeleníteni az utolsó sikeres fiókba történő bejelentkezés dátumát és időpontját.	**Hely** /etc/security/pscexpert/dodv2/sshDoDconfig **Megfelelési művelet** A szükséges információk megjelenítése.

2. táblázat: DoD általános követelmények (Folytatás)

Department of Defense STIG ellenőrzési pont azonosító	STIG szabály kategóriája	Leírás	A parancsfájl helye, ahol a művelet meg van határozva, valamint a művelet eredménye, amely lehetővé teszi a megfelelést
GEN000460	2	Ez a szabály letiltja a fiókot három egymást követő sikertelen bejelentkezési kísérlet után.	**Hely** /etc/security/pscexpert/dodv2/chusrattrdod **Megfelelési művelet** A bejelentkezési kísérlet korlátjának beállítása a megadott értékre.
GEN000480	2	Ez a szabály beállítja a bejelentkezés késleltetési idejét 4 másodpercre.	**Hely** /etc/security/pscexpert/dodv2/chdefstanzadod **Megfelelési művelet** A bejelentkezés késleltetési idejének beállítása a szükséges értékre.
GEN000540	2	Ez a szabály biztosítja, hogy a rendszer globális jelszó konfigurációs fájljai a szabálykövetelmények szerint kerüljenek beállításra.	**Hely** /etc/security/pscexpert/dodv2/chusrattrdod **Megfelelési művelet** A szükséges jelszóbeállítások megadása.
GEN000560	1	A rendszeren minden fióknak érvényes jelszóval kell rendelkezni.	**Hely** /etc/security/pscexpert/dodv2/grpusrpass_chk **Megfelelési művelet** Biztosítja, hogy a fiókokhoz tartozzon jelszó.
GEN000580	2	Ez a szabály biztosítja, hogy minden jelszó minimum 14 karaktert tartalmazzon.	**Hely** /etc/security/pscexpert/dodv2/chusrattrdod **Megfelelési művelet** A minimális jelszóhossz beállítása 14 karakterre.
GEN000585	2	A rendszernek a fiók jelszókivonatainak előállításához a Federal Information Processing Standards (FIPS) 140-2-es jóváhagyott kriptográfiai kivonatolási algoritmust kell használni.	**Hely** /etc/security/pscexpert/dodv2/fipspasswd **Megfelelési művelet** Biztosítja, hogy a jelszókivonatok jóváhagyott kivonatolási algoritmust használjanak.
GEN000590	2	A rendszernek a fiók jelszókivonatainak előállításához a FIPS 140-2-es jóváhagyott kriptográfiai kivonatolási algoritmust kell használni.	**Hely** /etc/security/pscexpert/dodv2/fipspasswd **Megfelelési művelet** Biztosítja, hogy a jelszókivonatok jóváhagyott kivonatolási algoritmust használjanak.
GEN000595	2	A rendszeren tárolt jelszókivonatok előállításához használjon FIPS 140-2-es jóváhagyott kriptográfiai kivonatolási algoritmust.	**Hely** /etc/security/pscexpert/dodv2/fipspasswd **Megfelelési művelet** Biztosítja, hogy a jelszókivonatok jóváhagyott kivonatolási algoritmust használjanak.
GEN000640	2	Ez a szabály megköveteli minimum egy nem alfabetikus karakter használatát a jelszóban.	**Hely** /etc/security/pscexpert/dodv2/chusrattrdod **Megfelelési művelet** A jelszóban a nem alfabetikus karakterek minimális számának beállítása 1 értékre.

2. táblázat: DoD általános követelmények (Folytatás)

Department of Defense STIG ellenőrzési pont azonosító	STIG szabály kategóriája	Leírás	A parancsfájl helye, ahol a művelet meg van határozva, valamint a művelet eredménye, amely lehetővé teszi a megfelelést
GEN000680	2	Ez a szabály biztosítja, hogy a jelszó ne tartalmazhasson több, mint három egymást követő ismétlődő karaktert	**Hely** /etc/security/pscexpert/dodv2/chusrattrdod **Megfelelési művelet** A jelszóban az ismétlődő karakterek maximális számának beállítása 3 értékre.
GEN000700	2	Ez a szabály biztosítja, hogy a rendszer globális jelszó konfigurációs fájljai a szabálykövetelmények szerint kerüljenek beállításra.	**Hely** /etc/security/pscexpert/dodv2/chusrattrdod **Megfelelési művelet** Biztosítja, hogy a jelszó konfigurációs fájljai megfeleljenek a követelményeknek.
GEN000740	2	Az összes beavatkozást nem igénylő és automatikus feldolgozású fiókjelszót zárolni kell (GEN000280). A közvetlen bejelentkezéseket tilos engedélyezni az osztott, alapértelmezett, alkalmazás és segédprogram fiókokba. (GEN002640) Az alapértelmezett rendszerfiókokat le kell tiltani vagy el kell távolítani.	**Hely** /etc/security/pscexpert/dodv2/loginout /etc/security/pscexpert/dodv2/lockacc_rlogin **Megfelelési művelet** Ez a beállítás automatikusan engedélyezett.
GEN000740	2	Az összes beavatkozást nem igénylő és automatikus feldolgozású fiókjelszót meg kell változtatni legalább évente egyszer vagy zárolni kell.	**Hely** /etc/security/pscexpert/dodv2/lockacc_rlogin **Megfelelési művelet** Biztosítja, hogy a megadott jelszavak évente módosítva legyenek vagy zárolásra kerüljenek.
GEN000750	2	Ez a szabály megköveteli, hogy az új jelszavak minimum 4 olyan karaktert tartalmazzanak, amely nem volt benne az előző jelszóban.	**Hely** /etc/security/pscexpert/dodv2/chusrattrdod **Megfelelési művelet** Az új jelszóban megadandó új karakterek minimális számának beállítása 4-es értékre.
GEN000760	2	A fiókokat 35 nap inaktivitás után zárolni kell.	**Hely** /etc/security/pscexpert/dodv2/disableacctdod **Megfelelési művelet** A fiókok zárolása 35 nap inaktivitás után.
GEN000790	2	A rendszernek meg kell akadályozni a szótárban szereplő szavak használatát a jelszavakhoz.	**Hely** /etc/security/pscexpert/dodv2/chuserstanzadod **Megfelelési művelet** Biztosítja, hogy a beállítás alatt álló jelszó ne legyen gyenge.
GEN000800	2	Ez a szabály biztosítja, hogy a legutóbbi öt jelszó ne kerüljön újrafelhasználásra.	**Hely** /etc/security/pscexpert/dodv2/chusrattrdod **Megfelelési művelet** Biztosítja, hogy az új jelszó ne egyezzen meg a legutóbbi 5 jelszó egyikével sem.

2. táblázat: DoD általános követelmények (Folytatás)

Department of Defense STIG ellenőrzési pont azonosító	**STIG szabály kategóriája**	**Leírás**	**A parancsfájl helye, ahol a művelet meg van határozva, valamint a művelet eredménye, amely lehetővé teszi a megfelelést**
GEN000880 (a következőhöz kapcsolódik: GEN000300, GEN000320, GEN000380)	2	A rendszeren minden fióknak egyedi felhasználói- vagy fióknévvel, illetve egyedi felhasználói- vagy fiók jelszóval kell rendelkezni.	**Hely** /etc/security/pscexpert/dodv2/grpusrpass_chk **Megfelelési művelet** Biztosítja, hogy minden fiók megfeleljen a megadott követelményeknek.
GEN000900	3	A root felhasználó saját könyvtára nem lehet az alapkönyvtár (/).	**Hely** /etc/security/pscexpert/dodv2/rootpasswd_home **Megfelelési művelet** Biztosítja, hogy a rendszer megfeleljen a megadott követelménynek. **Megjegyzés:** Ez a beállítás nem módosul automatikusan, ha az irányelv visszaállításra kerül az AIX alapértelmezett irányelvre, a DoDv2_to_ használatával az AIXDefault.xml fájlhoz. Ezt a beállítást kézzel kell módosítani.
GEN000940	2	A root fiók végrehajtható fájlja keresési útvonalának a kereskedő alapértelmezett fiókútvonalának kell lenni és csak abszolút útvonalakat tartalmazhat.	**Hely** /etc/security/pscexpert/dodv2/fixpathvars **Megfelelési művelet** Biztosítja, hogy a rendszer megfeleljen a megadott követelményeknek. **Megjegyzés:** Ez a beállítás nem módosul automatikusan, ha az irányelv visszaállításra kerül az AIX alapértelmezett irányelvre, a DoDv2_to_ használatával az AIXDefault.xml fájlhoz. Ezt a beállítást kézzel kell módosítani.
GEN000945	2	A root fiók könyvtára keresési útvonalának a rendszer alapértelmezett útvonalának kell lenni és csak abszolút útvonalakat tartalmazhat.	**Hely** /etc/security/pscexpert/dodv2/fixpathvars **Megfelelési művelet** Biztosítja, hogy a rendszer megfeleljen a megadott követelményeknek. **Megjegyzés:** Ez a beállítás nem módosul automatikusan, ha az irányelv visszaállításra kerül az AIX alapértelmezett irányelvre, a DoDv2_to_ használatával az AIXDefault.xml fájlhoz. Ezt a beállítást kézzel kell módosítani.
GEN000950	2	A root fiók előre betöltött könyvtárai listájának üresnek kell lenni.	**Hely** /etc/security/pscexpert/dodv2/fixpathvars **Megfelelési művelet** Biztosítja, hogy a rendszer megfeleljen a megadott követelményeknek. **Megjegyzés:** Ez a beállítás nem módosul automatikusan, ha az irányelv visszaállításra kerül az AIX alapértelmezett irányelvre, a DoDv2_to_ használatával az AIXDefault.xml fájlhoz. Ezt a beállítást kézzel kell módosítani.
GEN000960 (a következőhöz kapcsolódik: GEN003000, GEN003020, GEN003160, GEN003360, GEN003380)	2	A root fióknak a végrehajtható fájl keresési útvonalán írható könyvtáraknak kell lenni.	**Hely** /etc/security/pscexpert/dodv2/rmwwpaths **Megfelelési művelet** Biztosítja, hogy a rendszer megfeleljen a megadott követelményeknek. **Megjegyzés:** Ez a beállítás nem módosul automatikusan, ha az irányelv visszaállításra kerül az AIX alapértelmezett irányelvre, a DoDv2_to_ használatával az AIXDefault.xml fájlhoz. Ezt a beállítást kézzel kell módosítani.

2. táblázat: DoD általános követelmények (Folytatás)

Department of Defense STIG ellenőrzési pont azonosító	STIG szabály kategóriája	Leírás	A parancsfájl helye, ahol a művelet meg van határozva, valamint a művelet eredménye, amely lehetővé teszi a megfelelést
GEN000980	2	A rendszernek meg kell akadályozni, hogy a root fiókba közvetlenül be lehessen jelentkezni, kivéve a rendszerkonzolról.	**Hely** /etc/security/pscexpert/dodv2/chuserstanzadod **Megfelelési művelet** Biztosítja, hogy a rendszer megfeleljen a megadott követelményeknek.
GEN001000	2	A távoli konzoloknak tiltottnak kell lenni vagy védve kell lenni a jogosulatlan hozzáférés ellen.	**Hely** /etc/security/pscexpert/dodv2/remoteconsole **Megfelelési művelet** Biztosítja, hogy a megadott konzolok tiltottak legyenek.
GEN001020	2	A root fiók nem használható közvetlen bejelentkezéshez.	**Hely** /etc/security/pscexpert/dodv2/sshDoDconfig **Megfelelési művelet** A root fiók letiltása a közvetlen bejelentkezéshez.
GEN001060	2	A rendszernek naplózni kell a sikeres és a sikertelen kísérleteket a root fiókok elérésére.	**Hely** /etc/security/pscexpert/dodv2/loginout **Megfelelési művelet** Biztosítja, hogy a rendszer megfeleljen a megadott követelményeknek.
GEN001100	1	A root jelszavak soha nem adhatók át a hálózaton szöveges formátumban.	**Hely** /etc/security/pscexpert/dodv2/chuserstanzadod **Megfelelési művelet** Biztosítja, hogy a rendszer megfeleljen a megadott követelményeknek.
GEN001120	2	A rendszer nem engedélyezheti a root bejelentkezést az SSH protokoll használatával.	**Hely** /etc/security/pscexpert/dodv2/sshDoDconfig **Megfelelési művelet** A root bejelentkezés letiltása az SSH protokollhoz.
GEN001440	3	Minden interaktív felhasználóhoz hozzárendelve kell lenni egy saját könyvtárnak az /etc/passwd fájlban.	**Hely** /etc/security/pscexpert/dodv2/grpusrpass_chk **Megfelelési művelet** Biztosítja, hogy minden interaktív felhasználó rendelkezzen a megadott könyvtárral.
GEN001475	2	Az /etc/group fájl nem tartalmazhat csoport jelszókivonatokat.	**Hely** /etc/security/pscexpert/dodv2/passwdhash **Megfelelési művelet** Biztosítja, hogy ne legyen csoport jelszókivonat a megadott fájlban. **Megjegyzés:** Ez a beállítás nem módosul automatikusan, ha az irányelv visszaállításra kerül az AIX alapértelmezett irányelvre, a DoDv2_to_ használatával az AIXDefault.xml fájlhoz. Ezt a beállítást kézzel kell módosítani.
GEN001600	2	A futtatásvezérlő parancsfájlok végrehajtható fájljának keresési útvonalai csak abszolút útvonalakat tartalmazhatnak.	**Hely** /etc/security/pscexpert/dodv2/fixpathvars **Megfelelési művelet** Biztosítja, hogy a rendszer megfeleljen a megadott követelményeknek. **Megjegyzés:** Ez a beállítás nem módosul automatikusan, ha az irányelv visszaállításra kerül az AIX alapértelmezett irányelvre, a DoDv2_to_ használatával az AIXDefault.xml fájlhoz. Ezt a beállítást kézzel kell módosítani.

2. táblázat: DoD általános követelmények (Folytatás)

Department of Defense STIG ellenőrzési pont azonosító	STIG szabály kategóriája	Leírás	A parancsfájl helye, ahol a művelet meg van határozva, valamint a művelet eredménye, amely lehetővé teszi a megfelelést
GEN001605	2	A futtatásvezérlő parancsfájlok könyvtárának keresési útvonalai csak abszolút útvonalakat tartalmazhatnak.	**Hely** /etc/security/pscexpert/dodv2/fixpathvars **Megfelelési művelet** Biztosítja, hogy a rendszer megfeleljen a megadott követelményeknek. **Megjegyzés:** Ez a beállítás nem módosul automatikusan, ha az irányelv visszaállításra kerül az AIX alapértelmezett irányelvre, a DoDv2_to_ használatával az AIXDefault.xml fájlhoz. Ezt a beállítást kézzel kell módosítani.
GEN001610	2	A futtatásvezérlő parancsfájlok előre betöltött könyvtárainak listái csak abszolút útvonalakat tartalmazhatnak.	**Hely** /etc/security/pscexpert/dodv2/fixpathvars **Megfelelési művelet** Biztosítja, hogy a rendszer megfeleljen a megadott követelményeknek. **Megjegyzés:** Ez a beállítás nem módosul automatikusan, ha az irányelv visszaállításra kerül az AIX alapértelmezett irányelvre, a DoDv2_to_ használatával az AIXDefault.xml fájlhoz. Ezt a beállítást kézzel kell módosítani.
GEN001840	2	Minden globális inicializálási fájl végrehajtható fájljának keresési útvonalai csak abszolút útvonalakat tartalmazhatnak.	**Hely** /etc/security/pscexpert/dodv2/fixpathvars **Megfelelési művelet** Biztosítja, hogy a rendszer megfeleljen a megadott követelményeknek. **Megjegyzés:** Ez a beállítás nem módosul automatikusan, ha az irányelv visszaállításra kerül az AIX alapértelmezett irányelvre, a DoDv2_to_ használatával az AIXDefault.xml fájlhoz. Ezt a beállítást kézzel kell módosítani.
GEN001845	2	Minden globális inicializálási fájl könyvtárának keresési útvonalai csak abszolút útvonalakat tartalmazhatnak.	**Hely** /etc/security/pscexpert/dodv2/fixpathvars **Megfelelési művelet** Biztosítja, hogy a rendszer megfeleljen a megadott követelményeknek. **Megjegyzés:** Ez a beállítás nem módosul automatikusan, ha az irányelv visszaállításra kerül az AIX alapértelmezett irányelvre, a DoDv2_to_ használatával az AIXDefault.xml fájlhoz. Ezt a beállítást kézzel kell módosítani.
GEN001850	2	Minden globális inicializálási fájl előre betöltött könyvtárainak listái csak abszolút útvonalakat tartalmazhatnak.	**Hely** /etc/security/pscexpert/dodv2/fixpathvars **Megfelelési művelet** Biztosítja, hogy a rendszer megfeleljen a megadott követelményeknek. **Megjegyzés:** Ez a beállítás nem módosul automatikusan, ha az irányelv visszaállításra kerül az AIX alapértelmezett irányelvre, a DoDv2_to_ használatával az AIXDefault.xml fájlhoz. Ezt a beállítást kézzel kell módosítani.
GEN001900	2	Minden helyi inicializálási fájl végrehajtható fájljának keresési útvonalai csak abszolút útvonalakat tartalmazhatnak.	**Hely** /etc/security/pscexpert/dodv2/fixpathvars **Megfelelési művelet** Biztosítja, hogy a rendszer megfeleljen a megadott követelményeknek. **Megjegyzés:** Ez a beállítás nem módosul automatikusan, ha az irányelv visszaállításra kerül az AIX alapértelmezett irányelvre, a DoDv2_to_ használatával az AIXDefault.xml fájlhoz. Ezt a beállítást kézzel kell módosítani.

2. táblázat: DoD általános követelmények (Folytatás)

Department of Defense STIG ellenőrzési pont azonosító	STIG szabály kategóriája	Leírás	A parancsfájl helye, ahol a művelet meg van határozva, valamint a művelet eredménye, amely lehetővé teszi a megfelelést
GEN001901	2	Minden helyi inicializálási fájl könyvtárának keresési útvonalai csak abszolút útvonalakat tartalmazhatnak.	**Hely** /etc/security/pscexpert/dodv2/fixpathvars **Megfelelési művelet** Biztosítja, hogy a rendszer megfeleljen a megadott követelményeknek. **Megjegyzés:** Ez a beállítás nem módosul automatikusan, ha az irányelv visszaállításra kerül az AIX alapértelmezett irányelvre, a DoDv2_to_ használatával az AIXDefault.xml fájlhoz. Ezt a beállítást kézzel kell módosítani.
GEN001902	2	Minden helyi inicializálási fájl előre betöltött könyvtárainak listái csak abszolút útvonalakat tartalmazhatnak.	**Hely** /etc/security/pscexpert/dodv2/fixpathvars **Megfelelési művelet** Biztosítja, hogy a rendszer megfeleljen a megadott követelményeknek. **Megjegyzés:** Ez a beállítás nem módosul automatikusan, ha az irányelv visszaállításra kerül az AIX alapértelmezett irányelvre, a DoDv2_to_ használatával az AIXDefault.xml fájlhoz. Ezt a beállítást kézzel kell módosítani.
GEN001940	2	A felhasználói inicializálási fájlok nem futtathatnak írható programokat.	**Hely** /etc/security/pscexpert/dodv2/rmwwpaths **Megfelelési művelet** Biztosítja, hogy a rendszer megfeleljen a megadott követelményeknek.
GEN001980	2	Az .rhosts, .shosts, hosts.equiv, shosts.equiv, /etc/passwd, /etc/shadow és az /etc/group fájl nem tartalmazhat plusz jelet (+) a bejegyzések meghatározása nélkül a NIS+ hálózati csoportokhoz.	**Hely** /etc/security/pscexpert/dodv2/dodv2netrules **Megfelelési művelet** Biztosítja, hogy a megadott fájlok megfeleljenek a megadott követelményeknek.
GEN002000	2	A rendszeren nem lehet .netrc fájl.	**Hely** /etc/security/pscexpert/dodv2/dodv2netrules **Megfelelési művelet** Biztosítja, hogy a megadott fájlok egyike se legyen a rendszeren. **Megjegyzés:** Ez a beállítás nem módosul automatikusan, ha az irányelv visszaállításra kerül az AIX alapértelmezett irányelvre, a DoDv2_to_ használatával az AIXDefault.xml fájlhoz. Ezt a beállítást kézzel kell módosítani.
GEN002020	2	Minden .rhosts, .shosts és hosts.equiv fájl csak megbízható hoszt-felhasználó párt tartalmazhat.	**Hely** /etc/security/pscexpert/dodv2/dodv2netrules **Megfelelési művelet** Biztosítja, hogy a megadott fájlok megfeleljenek a követelménynek.
GEN002040	1	A szabály letiltja az .rhosts, .shosts és hosts.equiv fájlt, valamint az shosts.equiv fájlokat.	**Hely** /etc/security/pscexpert/dodv2/mvhostsfilesdod **Megfelelési művelet** A megadott fájlok letiltása.

2. táblázat: DoD általános követelmények (Folytatás)

Department of Defense STIG ellenőrzési pont azonosító	STIG szabály kategóriája	Leírás	A parancsfájl helye, ahol a művelet meg van határozva, valamint a művelet eredménye, amely lehetővé teszi a megfelelést
GEN002120	1,2	Ez a szabály ellenőrzi és konfigurálja a felhasználói parancsértelmezőket.	**Hely** /etc/security/pscexpert/dodv2/usershells **Megfelelési művelet** Létrehozza a szükséges parancsértelmezőket. **Megjegyzés:** Ez a beállítás nem módosul automatikusan, ha az irányelv visszaállításra kerül az AIX alapértelmezett irányelvre, a DoDv2_to_ használatával az AIXDefault.xml fájlhoz. Ezt a beállítást kézzel kell módosítani.
GEN002140	1,2	Az /etc/passwd listán hivatkozott összes parancsértelmezőt fel kell sorolni az /etc/shells fájlban, kivéve azokat, amelyek a bejelentkezések megakadályozása érdekében lettek megadva.	**Hely** /etc/security/pscexpert/dodv2/usershells **Megfelelési művelet** Biztosítja, hogy a parancsértelmezők a megfelelő fájlokban kerüljenek felsorolásra. **Megjegyzés:** Ez a beállítás nem módosul automatikusan, ha az irányelv visszaállításra kerül az AIX alapértelmezett irányelvre, a DoDv2_to_ használatával az AIXDefault.xml fájlhoz. Ezt a beállítást kézzel kell módosítani.
GEN002280	2	Az eszközfájloknak és a könyvtáraknak csak a rendszerfiókkal rendelkező felhasználók számra kell írhatóknak lenni, vagy ahogy a rendszert a gyártó beállította.	**Hely** /etc/security/pscexpert/dodv2/wwdevfiles **Megfelelési művelet** Megjeleníti az írható eszközfájlokat, könyvtárakat és az összes olyan fájlt a rendszeren, amely nem nyilvános könyvtárakban található.
GEN002300	2	A biztonsági mentéshez használt eszközfájloknak olvashatónak, írhatónak vagy mindkettőnek kell lenni a root felhasználó és a biztonsági mentési felhasználó számára.	**Hely** /etc/security/pscexpert/dodv2/wwdevfiles **Megfelelési művelet** Megjeleníti az írható eszközfájlokat, könyvtárakat és az összes olyan fájlt a rendszeren, amely nem nyilvános könyvtárakban található.
GEN002400	2	A rendszeren hetente kell ellenőrizni a jogosulatlan setuid fájlokat, valamint a jogosulatlan módosításokat a hitelesített setuid fájlokban.	**Hely** /etc/security/pscexpert/dodv2/trust **Megfelelési művelet** Heti ellenőrzés a megadott fájlokban végzett módosítások azonosításához. **Megjegyzés:** Hasonlítsa össze a két legújabb heti naplót, amely a /var/security/pscexpert könyvtárban lett létrehozva, és ellenőrizze, hogy nem volt jogosulatlan tevékenység.
GEN002420	2	A cserélhető adathordozókat, távoli fájlrendszereket és azokat a fájlrendszereket, amelyek nem tartalmaznak jóváhagyott setuid fájlokat, a *nosuid* paraméterrel kell felépíteni.	**Hely** /etc/security/pscexpert/dodv2/fsmntoptions **Megfelelési művelet** Biztosítja, hogy a távolról felépített fájlrendszerek rendelkezzenek a megadott beállításokkal. **Megjegyzés:** Ez a beállítás nem módosul automatikusan, ha az irányelv visszaállításra kerül az AIX alapértelmezett irányelvre, a DoDv2_to_ használatával az AIXDefault.xml fájlhoz. Ezt a beállítást kézzel kell módosítani.

2. táblázat: DoD általános követelmények (Folytatás)

Department of Defense STIG ellenőrzési pont azonosító	STIG szabály kategóriája	Leírás	A parancsfájl helye, ahol a művelet meg van határozva, valamint a művelet eredménye, amely lehetővé teszi a megfelelést
GEN002430	2	A cserélhető adathordozókat, távoli fájlrendszereket és azokat a fájlrendszereket, amelyek nem tartalmaznak jóváhagyott eszközfájlokat, a *nodev* paraméterrel kell felépíteni.	**Hely** /etc/security/pscexpert/dodv2/fsmntoptions **Megfelelési művelet** Biztosítja, hogy a távolról felépített fájlrendszerek rendelkezzenek a megadott beállításokkal. **Megjegyzés:** Ez a beállítás nem módosul automatikusan, ha az irányelv visszaállításra kerül az AIX alapértelmezett irányelvre, a DoDv2_to_ használatával az AIXDefault.xml fájlhoz. Ezt a beállítást kézzel kell módosítani.
GEN002480	2	Csak a nyilvános könyvtárak lehetnek írható könyvtárak, és az írható fájlok csak nyilvános könyvtárakban helyezhetők el.	**Hely** /etc/security/pscexpert/dodv2/wwdevfiles /etc/security/pscexpert/dodv2/fpmdodfiles **Megfelelési művelet** Jelentéskészítés, ha az írható fájlok nem nyilvános könyvtárakban helyezkednek el.
GEN002640	2	Az alapértelmezett rendszerfiókokat le kell tiltani vagy el kell távolítani.	**Hely** /etc/security/pscexpert/dodv2/lockacc_rlogin /etc/security/pscexpert/dodv2/loginout **Megfelelési művelet** Az alapértelmezett rendszerfiókok letiltása.
GEN002660	2	A megfigyelésnek engedélyezettnek kell lenni.	**Hely** /etc/security/pscexpert/dodv2/dodaudit **Megfelelési művelet** A dodaudit parancs engedélyezése, amely engedélyezi a megfigyelést.
GEN002720	2	A megfigyelési rendszert be kell állítani a fájlok és programok elérésére tett sikertelen kísérletek figyelésére.	**Hely** /etc/security/pscexpert/dodv2/dodaudit **Megfelelési művelet** A megadott megfigyelés automatikus engedélyezése.
GEN002740	2	A megfigyelési rendszert be kell állítani a fájltörlések figyelésére.	**Hely** /etc/security/pscexpert/dodv2/dodaudit **Megfelelési művelet** A megadott megfigyelés automatikus engedélyezése.
GEN002750	3	A megfigyelési rendszert be kell állítani a fióklétrehozás figyelésére.	**Hely** /etc/security/pscexpert/dodv2/dodaudit **Megfelelési művelet** A megadott megfigyelés automatikus engedélyezése.
GEN002751	3	A megfigyelési rendszert be kell állítani a fiókmódosítás figyelésére.	**Hely** /etc/security/pscexpert/dodv2/dodaudit **Megfelelési művelet** A megadott megfigyelés automatikus engedélyezése.
GEN002752	3	A megfigyelési rendszert be kell állítani a tiltott fiókok figyelésére.	**Hely** /etc/security/pscexpert/dodv2/dodaudit **Megfelelési művelet** A megadott megfigyelés automatikus engedélyezése.
GEN002753	3	A megfigyelési rendszert be kell állítani a fióklezárás figyelésére.	**Hely** /etc/security/pscexpert/dodv2/dodaudit **Megfelelési művelet** A megadott megfigyelés automatikus engedélyezése.

2. táblázat: DoD általános követelmények (Folytatás)

Department of Defense STIG ellenőrzési pont azonosító	**STIG szabály kategóriája**	**Leírás**	**A parancsfájl helye, ahol a művelet meg van határozva, valamint a művelet eredménye, amely lehetővé teszi a megfelelést**
GEN002760	2	A megfigyelési rendszert be kell állítani az összes adminisztrációs, privilegizált és biztonsági művelet figyelésére.	**Hely** /etc/security/pscexpert/dodv2/dodaudit **Megfelelési művelet** A megadott megfigyelés automatikus engedélyezése.
GEN002800	2	A megfigyelési rendszert be kell állítani a bejelentkezés, kijelentkezés és a munkamenet kezdeményezés figyelésére.	**Hely** /etc/security/pscexpert/dodv2/dodaudit **Megfelelési művelet** A megadott megfigyelés automatikus engedélyezése.
GEN002820	2	A megfigyelési rendszert be kell állítani az összes diszkrecionális hozzáférés-felügyeleti engedély módosításának figyelésére.	**Hely** /etc/security/pscexpert/dodv2/dodaudit **Megfelelési művelet** A megadott megfigyelés automatikus engedélyezése.
GEN002825	2	A megfigyelési rendszert be kell állítani a dinamikus kernelmodulok betöltésének és letávolításának figyelésére.	**Hely** /etc/security/pscexpert/dodv2/dodaudit **Megfelelési művelet** A megadott megfigyelés automatikus engedélyezése.
GEN002860	2	A megfigyelési naplókat naponta kell forgatni.	**Hely** /etc/security/pscexpert/dodv2/rotateauditdod **Megfelelési művelet** Biztosítja a megfigyelési naplók forgatását.
GEN002960	2	A cron segédprogram hozzáférését szabályozni kell a cron.allow fájllal vagy a cron.deny fájllal, vagy mindkettővel.	**Hely** /etc/security/pscexpert/dodv2/limitsysacc **Megfelelési művelet** Biztosítja, hogy a szabványnak való megfelelési korlátok engedélyezettek legyenek.
GEN003000 (a következőhöz kapcsolódik: GEN000960, GEN003020, GEN003160, GEN003360, GEN003380)	2	A Cron nem futtathat csoport által írható és bárki által írható programokat.	**Hely** /etc/security/pscexpert/dodv2/rmwwpaths **Megfelelési művelet** Biztosítja, hogy a szabványnak való megfelelési korlátok engedélyezettek legyenek. **Megjegyzés:** Ez a beállítás nem módosul automatikusan, ha az irányelv visszaállításra kerül az AIX alapértelmezett irányelvre, a DoDv2_to_ használatával az AIXDefault.xml fájlhoz. Ezt a beállítást kézzel kell módosítani.
GEN003020 (a következőhöz kapcsolódik: GEN000960, GEN003000, GEN003160, GEN003360, GEN003380)	2	A Cron nem futtathat programokat a bárki számára írható könyvtárakban vagy ezek leszármazottaiban.	**Hely** /etc/security/pscexpert/dodv2/rmwwpaths **Megfelelési művelet** Eltávolítja a bárki számára írható engedélyt a cron programkönyvtárakból. **Megjegyzés:** Ez a beállítás nem módosul automatikusan, ha az irányelv visszaállításra kerül az AIX alapértelmezett irányelvre, a DoDv2_to_ használatával az AIXDefault.xml fájlhoz. Ezt a beállítást kézzel kell módosítani.

2. táblázat: DoD általános követelmények (Folytatás)

Department of Defense STIG ellenőrzési pont azonosító	STIG szabály kategóriája	Leírás	A parancsfájl helye, ahol a művelet meg van határozva, valamint a művelet eredménye, amely lehetővé teszi a megfelelést
GEN003060	2	Az alapértelmezett rendszerfiókok (a root kivételével) nem sorolhatók fel a cron.allow fájlban, vagy benne kell lenniük a cron.deny fájlban, ha a cron.allow fájl nem létezik.	**Hely** cron.allow vagy cron.deny **Megfelelési művelet** Biztosítja, hogy a rendszer megfeleljen a megadott követelményeknek.
GEN003160 (a következőhöz kapcsolódik: GEN000960, GEN003000, GEN003020, GEN003360, GEN003380)	2	A Cron naplózásnak futni kell.	**Hely** /etc/security/pscexpert/dodv2/rmwwpaths **Megfelelési művelet** Biztosítja, hogy a rendszer megfeleljen a megadott követelményeknek.
GEN003280	2	Az at segédprogram hozzáférését szabályozni kell az at.allow és az at.deny fájllal.	**Hely** /etc/security/pscexpert/dodv2/chcronfilesdod **Megfelelési művelet** Biztosítja, hogy a rendszer megfeleljen a megadott követelményeknek.
GEN003300	2	Az at.deny fájl nem lehet üres, ha létezik.	**Hely** /etc/security/pscexpert/dodv2/chcronfilesdod **Megfelelési művelet** Biztosítja, hogy a rendszer megfeleljen a megadott követelményeknek.
GEN003320	2	A nem root alapértelmezett rendszerfiókok nem sorolhatók fel az at.allow fájlban, vagy benne kell lenniük az at.deny fájlban, ha az at.allow fájl nem létezik.	**Hely** /etc/security/pscexpert/dodv2/chcronfilesdod **Megfelelési művelet** Biztosítja, hogy a rendszer megfeleljen a megadott követelményeknek.
GEN003360 (a következőhöz kapcsolódik: GEN000960, GEN003000, GEN003020, GEN003160, GEN003380)	2	Az at démon nem futtathat csoport által vagy bárki által írható programokat.	**Hely** /etc/security/pscexpert/dodv2/rmwwpaths **Megfelelési művelet** Biztosítja, hogy a rendszer megfeleljen a megadott követelményeknek. **Megjegyzés:** Ez a beállítás nem módosul automatikusan, ha az irányelv visszaállításra kerül az AIX alapértelmezett irányelvre, a DoDv2_to_ használatával az AIXDefault.xml fájlhoz. Ezt a beállítást kézzel kell módosítani.
GEN003380 (a következőhöz kapcsolódik: GEN000960, GEN003000, GEN003020, GEN003160, GEN003360)	2	Az at démon nem futtathat programokat a bárki számára írható könyvtárakban vagy ezek leszármazottaiban.	**Hely** /etc/security/pscexpert/dodv2/rmwwpaths **Megfelelési művelet** Biztosítja, hogy a rendszer megfeleljen a megadott követelményeknek. **Megjegyzés:** Ez a beállítás nem módosul automatikusan, ha az irányelv visszaállításra kerül az AIX alapértelmezett irányelvre, a DoDv2_to_ használatával az AIXDefault.xml fájlhoz. Ezt a beállítást kézzel kell módosítani.
GEN003510	2	A kernel tárkiíratásokat le kell tiltani, hacsak nem szükségesek.	**Hely** /etc/security/pscexpert/dodv2/coredumpdev **Megfelelési művelet** Kernel tárkiíratások letiltása.

2. táblázat: DoD általános követelmények (Folytatás)

Department of Defense STIG ellenőrzési pont azonosító	**STIG szabály kategóriája**	**Leírás**	**A parancsfájl helye, ahol a művelet meg van határozva, valamint a művelet eredménye, amely lehetővé teszi a megfelelést**
GEN003540	2	A rendszernek nem végrehajtható programveremeket kell használni.	**Hely** /etc/security/pscexpert/dodv2/sedconfigdod **Megfelelési művelet** Nem végrehajtható programveremek használatának kikényszerítése.
GEN003600	2	A rendszer nem továbbíthat IPv4 forráshoz továbbított csomagokat.	**Hely** /etc/security/pscexpert/dodv2/ntwkoptsdod **Megfelelési művelet** Az ipsrcforward hálózati opció értékének beállítása *0* értékre.
GEN003601	2	A TCP háttérnapló sorméreteket megfelelően kell beállítani.	**Hely** /etc/security/pscexpert/dodv2/ntwkoptsdod **Megfelelési művelet** A clean_partial_ conns hálózati opció értékének beállítása *1* értékre.
GEN003603	2	A rendszer nem válaszolhat az üzenetszórási címre küldött Internet vezérlőüzenet protokoll 4. változat (ICMPv4) visszhangokra.	**Hely** /etc/security/pscexpert/dodv2/ntwkoptsdod **Megfelelési művelet** A bcastping hálózati opció értékének beállítása *0* értékre.
GEN003604	2	A rendszer nem válaszolhat az üzenetszórási címre küldött ICMP időpecsét kérésekre.	**Hely** /etc/security/pscexpert/dodv2/ntwkoptsdod **Megfelelési művelet** A bcastping hálózati opció értékének beállítása *0* értékre.
GEN003605	2	A rendszer nem alkalmazhat fordított forrástovábbítást a TCP válaszokra.	**Hely** /etc/security/pscexpert/dodv2/ntwkoptsdod **Megfelelési művelet** A nonlocsrcroute hálózati opció értékének beállítása *0* értékre.
GEN003606	2	A rendszernek meg kell akadályozni, hogy a helyi alkalmazások forráshoz irányított csomagokat állítsanak elő.	**Hely** /etc/security/pscexpert/dodv2/ntwkoptsdod **Megfelelési művelet** Az ipsrcroutesend hálózati opció értékének beállítása *0* értékre.
GEN003607	2	A rendszernek tilos elfogadni a forráshoz irányított IPv4 csomagokat.	**Hely** /etc/security/pscexpert/dodv2/ntwkoptsdod **Megfelelési művelet** A forráshoz irányított IPv4 csomagok elfogadásának Letiltása.
GEN003609	2	A rendszernek figyelmen kívül kell hagyni az IPv4 ICMP átirányítási üzeneteket.	**Hely** /etc/security/pscexpert/dodv2/ntwkoptsdod **Megfelelési művelet** Az ipignoreredirects hálózati opció beállítása *1* értékre.
GEN003610	2	A rendszer nem küldhet IPv4 ICMP átirányítási üzeneteket.	**Hely** /etc/security/pscexpert/dodv2/ntwkoptsdod **Megfelelési művelet** Az ipsendredirects hálózati opció értékének beállítása *0* értékre.
GEN003612	2	A rendszert be kell állítani TCP syncookie-k használatára, amikor TCP SYN elárasztás történik.	**Hely** /etc/security/pscexpert/dodv2/ntwkoptsdod **Megfelelési művelet** A clean_partial _conns hálózati opció beállítása *1* értékre.

2. táblázat: DoD általános követelmények (Folytatás)

Department of Defense STIG ellenőrzési pont azonosító	STIG szabály kategóriája	Leírás	A parancsfájl helye, ahol a művelet meg van határozva, valamint a művelet eredménye, amely lehetővé teszi a megfelelést
GEN003640	2	A fájlrendszer konzisztenciájának biztosítása érdekében a gyökér fájlrendszernek naplózást vagy más módszert kell használni.	**Hely** /etc/security/pscexpert/dodv2/chkjournal **Megfelelési művelet** Naplózás engedélyezése a gyökér fájlrendszeren.
GEN003660	2	A rendszernek naplózni kell a hitelesítési információs adatokat.	**Hely** /etc/security/pscexpert/dodv2/chsyslogdod **Megfelelési művelet** Az auth és info adatok naplózásának engedélyezése.
GEN003700	2	Az inetd és a xinetd elemet el kell távolítani, ha nem használja hálózati szolgáltatás.	**Hely** /etc/security/pscexpert/dodv2/dodv2services **Megfelelési művelet** Biztosítja, hogy a rendszer megfeleljen a megadott követelményeknek.
GEN003810	2	A portmap vagy az rpcbind szolgáltatás nem futtatható, hacsak nincs rá szükség.	**Hely** /etc/security/pscexpert/dodv2/dodv2services **Megfelelési művelet** Biztosítja, hogy a rendszer megfeleljen a megadott követelményeknek.
GEN003815	2	A portmap és az rpcbind szolgáltatást nem lehet telepíteni, hacsak nincsenek használatban.	**Hely** /etc/security/pscexpert/dodv2/dodv2services **Megfelelési művelet** Biztosítja, hogy a rendszer megfeleljen a megadott követelményeknek.
GEN003820-3860	1,2,3	A rsh, rexexec és telnet démon, valamint az rlogind szolgáltatás nem futtatható.	**Hely** /etc/security/pscexpert/dodv2/inetdservices **Megfelelési művelet** Letiltja a szükséges démonokat és szolgáltatásokat a bejegyzések kikommentezésével az /etc/inetd.conf fájlban.
GEN003865	2	Hálózati elemző eszközöket nem lehet telepíteni.	**Hely** /etc/security/pscexpert/dodv2/dodv2services **Megfelelési művelet** Biztosítja, hogy a rendszer megfeleljen a megadott követelményeknek.
GEN003900	2	A hosts.lpd fájl (vagy egyenértékű) nem tartalmazhat plusz jelet (+).	**Hely** /etc/security/pscexpert/dodv2/printers **Megfelelési művelet** Biztosítja, hogy a rendszer megfeleljen a megadott követelményeknek.
GEN004220	1	Az adminisztrátori fiókok nem futtathatnak webböngészőt, kivéve, ha a helyi szolgáltatás adminisztrációnak szüksége van rá.	**Hely** /etc/security/pscexpert/dodv2/dodv2cat1 **Megfelelési művelet** A megadott szabálytesztelések eredményeinek megjelenítése.
GEN004460	2	A szabály naplóza az auth és az info adatokat.	**Hely** /etc/security/pscexpert/dodv2/chsyslogdod **Megfelelési művelet** Az auth és info adatok naplózásának engedélyezése.

2. táblázat: DoD általános követelmények (Folytatás)

Department of Defense STIG ellenőrzési pont azonosító	**STIG szabály kategóriája**	**Leírás**	**A parancsfájl helye, ahol a művelet meg van határozva, valamint a művelet eredménye, amely lehetővé teszi a megfelelést**
GEN004540	2	Ez a szabály letiltja a sendmail súgóparancsot.	**Hely** /etc/security/pscexpert/dodv2/sendmailhelp /etc/security/pscexpert/dodv2/dodv2cmntrows **Megfelelési művelet** A megadott parancs letiltása.
GEN004580	2	A rendszernek .forward fájlokat kell használni.	**Hely** /etc/security/pscexpert/dodv2/forward **Megfelelési művelet** A megadott fájlok letiltása. **Megjegyzés:** Ez a beállítás nem módosul automatikusan, ha az irányelv visszaállításra kerül az AIX alapértelmezett irányelvre, a DoDv2_to_ használatával az AIXDefault.xml fájlhoz. Ezt a beállítást kézzel kell módosítani.
GEN004600	1	Az SMTP szolgáltatásnak a legújabb változatát kell használni.	**Hely** /etc/security/pscexpert/dodv2/SMTP_ver **Megfelelési művelet** Biztosítja, hogy a megadott szolgáltatás legújabb változata legyen futtatva. **Megjegyzés:** Ez a beállítás nem módosul automatikusan, ha az irányelv visszaállításra kerül az AIX alapértelmezett irányelvre, a DoDv2_to_ használatával az AIXDefault.xml fájlhoz. Ezt a beállítást kézzel kell módosítani.
GEN004620	2	A sendmail szerveren a hibakeresési szolgáltatásnak tiltottnak kell lenni.	**Hely** /etc/security/pscexpert/dodv2/SMTP_ver **Megfelelési művelet** A sendmail hibakeresési szolgáltatás letiltása.
GEN004640	1	Az SMTP szolgáltatás nem rendelkezhet aktív uudecode álnévvel.	**Hely** /etc/security/pscexpert/dodv2/SMTPuucode **Megfelelési művelet** Az uudecode álnév letiltása.
GEN004710	2	A levéltovábbítást korlátozni kell.	**Hely** /etc/security/pscexpert/dodv2/sendmaildod **Megfelelési művelet** Levéltovábbítás korlátozása.
GEN004800	1,2,3	Nem titkosított FTP nem használható a rendszeren.	**Hely** /etc/security/pscexpert/dodv2/inetdservices **Megfelelési művelet** Letiltja a szükséges démonokat és szolgáltatásokat a bejegyzések kikommentezésével az /etc/inetd.conf fájlban.
GEN004820	2	Anonim FTP nem lehet aktív a rendszeren, hacsak nem hitelesített.	**Hely** /etc/security/pscexpert/dodv2/anonuser **Megfelelési művelet** Anonim FTP letiltása a rendszeren. **Megjegyzés:** Ez a beállítás nem módosul automatikusan, ha az irányelv visszaállításra kerül az AIX alapértelmezett irányelvre, a DoDv2_to_ használatával az AIXDefault.xml fájlhoz. Ezt a beállítást kézzel kell módosítani.
GEN004840	2	Ha a rendszer egy anonim FTP szerver, akkor el kell különíteni a Demilitarized Zone (DMZ) hálózatra.	**Hely** /etc/security/pscexpert/dodv2/anonuser **Megfelelési művelet** Biztosítja, hogy az anonim FTP a rendszeren a DMZ hálózaton legyen.

2. táblázat: DoD általános követelmények (Folytatás)

Department of Defense STIG ellenőrzési pont azonosító	STIG szabály kategóriája	Leírás	A parancsfájl helye, ahol a művelet meg van határozva, valamint a művelet eredménye, amely lehetővé teszi a megfelelést
GEN004880	2	Az ftpusers fájlnak létezni kell.	**Hely** /etc/security/pscexpert/dodv2/chdodftpusers **Megfelelési művelet** Biztosítja, hogy a megadott fájl a rendszeren legyen.
GEN004900	2	Az ftpusers fájlnak tartalmazni kell a fiókneveket, amelyek számára nem engedélyezett az FTP protokoll használata.	**Hely** /etc/security/pscexpert/dodv2/chdodftpusers **Megfelelési művelet** Biztosítja, hogy a fájl tartalmazza a szükséges fiókneveket.
GEN005000	1	Az anonim FTP fiókok nem rendelkezhetnek működő parancsértelmezővel.	**Hely** /etc/security/pscexpert/dodv2/usershells **Megfelelési művelet** Parancsértelmezők eltávolítása az anonim FTP fiókokról. **Megjegyzés:** Ez a beállítás nem módosul automatikusan, ha az irányelv visszaállításra kerül az AIX alapértelmezett irányelvre, a DoDv2_to_ használatával az AIXDefault.xml fájlhoz. Ezt a beállítást kézzel kell módosítani.
GEN005080	1	A TFTP démonnak biztonságos módban kell működnie, amely csak egyetlen könyvtárhoz biztosít hozzáférést a hoszt fájlrendszeren.	**Hely** /etc/security/pscexpert/dodv2/tftpdod **Megfelelési művelet** Biztosítja, hogy a démon megfeleljen a megadott követelményeknek.
GEN005120	2	Az TFTP démont be kell állítani a gyártói specifikációkra, beleértve a dedikált TFTP felhasználói fiókot, a nem bejelentkezési parancsértelmezőt, mint például a /bin/false, valamint egy saját könyvtárat, amelynek a TFTP felhasználó a tulajdonosa.	**Hely** /etc/security/pscexpert/dodv2/tftpdod **Megfelelési művelet** Biztosítja, hogy a rendszer megfeleljen a megadott követelményeknek.
GEN005140	1,2,3	Minden aktív TFTP démonnak hitelesítve és jóváhagyva kell lenni a rendszer akkreditációs csomagjában.	**Hely** /etc/security/pscexpert/dodv2/inetdservices **Megfelelési művelet** Biztosítja a démon hitelesítését.
GEN005160	1,2	Minden X Window System hosztnak írni kell .Xauthority fájlokat.	**Hely** /etc/security/pscexpert/dodv2/dodv2disableX **Megfelelési művelet** Biztosítja, hogy a hoszt megírja a megadott fájlokat.
GEN005200	1,2	Bármely X Window System képernyő nem exportálható nyilvánosan.	**Hely** /etc/security/pscexpert/dodv2/dodv2disableX **Megfelelési művelet** Megadott programok terjesztésének letiltása.
GEN005220	1,2	Az X Window System szerver hozzáférésének korlátozásához az .Xauthority vagy az X*.hosts (vagy egyenértékű) fájlt kell használni.	**Hely** /etc/security/pscexpert/dodv2/dodv2disableX **Megfelelési művelet** Biztosítja, hogy a megadott fájlok elérhetők legyenek a szerver elérésének korlátozásához.

2. táblázat: DoD általános követelmények (Folytatás)

Department of Defense STIG ellenőrzési pont azonosító	STIG szabály kategóriája	Leírás	A parancsfájl helye, ahol a művelet meg van határozva, valamint a művelet eredménye, amely lehetővé teszi a megfelelést
GEN005240	1,2	Az .Xauthority segédprogram a hozzáférést csak hitelesített hosztokhoz engedélyezheti.	**Hely** /etc/security/pscexpert/dodv2/dodv2disableX **Megfelelési művelet** Biztosítja, hogy a hozzáférés csak hitelesített hosztokra legyen korlátozva.
GEN005260	2	Ez a szabály letiltja az X Window System kapcsolatokat és az XServer bejelentkezés-kezelőt.	**Hely** /etc/security/pscexpert/dodv2/dodv2cmntrows **Megfelelési művelet** A szükséges kapcsolatok és a bejelentkezés-kezelő letiltása.
GEN005280	1,2,3	A rendszeren az UUCP szolgáltatásnak aktívnak kell lenni.	**Hely** /etc/security/pscexpert/dodv2/inetdservices **Megfelelési művelet** Letiltja a szükséges démonokat és szolgáltatásokat a bejegyzések kikommentezésével az /etc/inetd.conf fájlban.
GEN005300	2	Az SNMP közösségeket meg kell változtatni az alapértelmezett beállításokról.	**Hely** /etc/security/pscexpert/dodv2/chsnmp **Megfelelési művelet** Biztosítja, hogy a rendszer megfeleljen a megadott követelményeknek.
GEN005305	2	SNMP szolgáltatásnak csak SNMPv3 vagy újabb változatot lehet használni.	**Hely** /etc/security/pscexpert/dodv2/chsnmp **Megfelelési művelet** Biztosítja, hogy a rendszer megfeleljen a megadott követelményeknek.
GEN005306	2	Az SNMP szolgáltatásnak meg kell követelni a FIPS 140-2-es használatát.	**Hely** /etc/security/pscexpert/dodv2/chsnmp **Megfelelési művelet** Biztosítja, hogy a rendszer megfeleljen a megadott követelményeknek.
GEN005440	2	A rendszernek távoli syslog szervert (naplózási hoszt) kell használni.	**Hely** /etc/security/pscexpert/dodv2/EnableTrustedLogging **Megfelelési művelet** Biztosítja, hogy a rendszer távoli syslog szervert használjon.
GEN005450	2	A rendszernek távoli syslog szervert (naplózási hoszt) kell haszálni.	**Hely** /etc/security/pscexpert/dodv2/ EnableTrustedLogging **Megfelelési művelet** Biztosítja, hogy a rendszer távoli syslog szervert használjon.
GEN005460	2	A rendszernek távoli syslog szervert (naplózási hoszt) kell használni.	**Hely** /etc/security/pscexpert/dodv2/ EnableTrustedLogging **Megfelelési művelet** Biztosítja, hogy a rendszer távoli syslog szervert használjon.
GEN005480	2	A rendszernek távoli syslog szervert (naplózási hoszt) kell használni.	**Hely** /etc/security/pscexpert/dodv2/EnableTrustedLogging **Megfelelési művelet** Biztosítja, hogy a rendszer távoli syslog szervert használjon.
GEN005500	2	Az SSH démont úgy kell beállítani, hogy csak a Biztonságos parancsértelmező 2. változat (SSHv2) protokollt használja.	**Hely** /etc/security/pscexpert/dodv2/sshDoDconfig **Megfelelési művelet** Biztosítja, hogy a rendszer megfeleljen a megadott követelményeknek.

2. táblázat: DoD általános követelmények (Folytatás)

Department of Defense STIG ellenőrzési pont azonosító	STIG szabály kategóriája	Leírás	A parancsfájl helye, ahol a művelet meg van határozva, valamint a művelet eredménye, amely lehetővé teszi a megfelelést
GEN005501	2	Az SSH ügyfelet úgy kell beállítani, hogy csak az SSHv2 protokollt használja.	**Hely** /etc/security/pscexpert/dodv2/sshDoDconfig **Megfelelési művelet** Biztosítja, hogy a rendszer megfeleljen a megadott követelményeknek.
GEN005504	2	Az SSH démon csak a felügyeleti hálózati címeken figyelhet, hacsak nem jogosult más felhasználási módokra a felügyeleten kívül.	**Hely** /etc/security/pscexpert/dodv2/sshDoDconfig **Megfelelési művelet** Biztosítja, hogy a rendszer megfeleljen a megadott követelményeknek.
GEN005505	2	Az SSH démont csak olyan rejtjelek használatára lehet beállítani. amelyek megfelelnek a Federal Information Processing Standards (FIPS) 140-2-es szabványoknak.	**Hely** /etc/security/pscexpert/dodv2/sshDoDconfig **Megfelelési művelet** Biztosítja, hogy a rendszer megfeleljen a megadott követelményeknek.
GEN005506	2	Az SSH démont csak olyan rejtjelek használatára lehet beállítani. amelyek megfelelnek a FIPS 140-2-es szabványoknak.	**Hely** /etc/security/pscexpert/dodv2/sshDoDconfig **Megfelelési művelet** Biztosítja, hogy a rendszer megfeleljen a megadott követelményeknek.
GEN005507	2	Az SSH démont csak FIPS 140-2-es szabványoknak megfelelő kriptográfiai kivonatolási algoritmusokat tartalmazó Üzenethitelesítési kódok (MAC-ek) használatára lehet beállítani.	**Hely** /etc/security/pscexpert/dodv2/sshDoDconfig **Megfelelési művelet** Biztosítja, hogy a rendszer megfeleljen a megadott követelményeknek.
GEN005510	2	Az SSH ügyfelet FIPS 140-2-es szabványnak megfelelő rejtjeleket tartalmazó MAC-ek használatára lehet beállítani.	**Hely** /etc/security/pscexpert/dodv2/sshDoDconfig **Megfelelési művelet** Biztosítja, hogy a rendszer megfeleljen a megadott követelményeknek.
GEN005511	2	Az SSH ügyfelet FIPS 140-2-es szabványnak megfelelő rejtjeleket tartalmazó MAC-ek használatára lehet beállítani.	**Hely** /etc/security/pscexpert/dodv2/sshDoDconfig **Megfelelési művelet** Biztosítja, hogy a rendszer megfeleljen a megadott követelményeknek.
GEN005512	2	Az SSH démont csak FIPS 140-2-es szabványoknak megfelelő kriptográfiai kivonatolási algoritmusokat tartalmazó MAC-ek használatára lehet beállítani.	**Hely** /etc/security/pscexpert/dodv2/sshDoDconfig **Megfelelési művelet** Biztosítja, hogy a rendszer megfeleljen a megadott követelményeknek.

2. táblázat: DoD általános követelmények (Folytatás)

Department of Defense STIG ellenőrzési pont azonosító	STIG szabály kategóriája	Leírás	A parancsfájl helye, ahol a művelet meg van határozva, valamint a művelet eredménye, amely lehetővé teszi a megfelelést
GEN005521	2	Az SSH démonnak korlátozni kell a bejelentkezést specifikus felhasználókra, csoportokra vagy mindkettőre.	**Hely** /etc/security/pscexpert/dodv2/sshDoDconfig **Megfelelési művelet** Biztosítja, hogy a rendszer megfeleljen a megadott követelményeknek.
GEN005536	2	Az SSH démonnak szigorú ellenőrzést kell végrehajtani a saját könyvtár konfigurációs fájljain.	**Hely** /etc/security/pscexpert/dodv2/sshDoDconfig **Megfelelési művelet** Biztosítja, hogy a rendszer megfeleljen a megadott követelményeknek.
GEN005537	2	Az SSH démonnak jogosultság elkülönítést kell használni.	**Hely** /etc/security/pscexpert/dodv2/sshDoDconfig **Megfelelési művelet** Biztosítja, hogy a rendszer megfeleljen a megadott követelményeknek.
GEN005538	2	Az SSH démon nem engedélyezheti az rhosts számára a hitelesítést Rivest-Shamir-Adleman (RSA) titkosítási rendszer használatával.	**Hely** /etc/security/pscexpert/dodv2/sshDoDconfig **Megfelelési művelet** Biztosítja, hogy a rendszer megfeleljen a megadott követelményeknek.
GEN005539	2	Az SSH démon nem engedélyezheti a tömörítést vagy csak sikeres hitelesítés után engedélyezheti.	**Hely** /etc/security/pscexpert/dodv2/sshDoDconfig **Megfelelési művelet** Biztosítja, hogy a rendszer megfeleljen a megadott követelményeknek.
GEN005550	2	Az SSH démont a DoD bejelentkezési fejléccsíkkal kell beállítani.	**Hely** /etc/security/pscexpert/dodv2/sshDoDconfig **Megfelelési művelet** Biztosítja, hogy a rendszer megfeleljen a megadott követelményeknek.
GEN005560	2	Meghatározza, hogy van-e olyan alapértelmezett átjáró, amely IPv4-hez van beállítva.	**Hely** /etc/security/pscexpert/dodv2/chkgtway **Megfelelési művelet** Biztosítja, hogy a rendszer megfeleljen a megadott követelményeknek. **Megjegyzés:** Ez a beállítás nem módosul automatikusan, ha az irányelv visszaállításra kerül az AIX alapértelmezett irányelvre, a DoDv2_to_ használatával az AIXDefault.xml fájlhoz. Ezt a beállítást kézzel kell módosítani. **Megjegyzés:** Ha a saját rendszere IPv6 protokollt futtat. akkor gondoskodjon róla, hogy az *ipv6_enabled* beállítás az /etc/security/pscexpert/ipv6.conf fájlban yes értékre legyen beállítva. Ha a rendszer nem IPv6 protokollt használ, akkor gondoskodjon róla, hogy az *ipv6_enabled* no értékre legyen beállítva.

2. táblázat: DoD általános követelmények (Folytatás)

Department of Defense STIG ellenőrzési pont azonosító	STIG szabály kategóriája	Leírás	A parancsfájl helye, ahol a művelet meg van határozva, valamint a művelet eredménye, amely lehetővé teszi a megfelelést
GEN005570	2	Meghatározza, hogy van-e olyan alapértelmezett átjáró, amely IPv6-hoz van beállítva.	**Hely** /etc/security/pscexpert/dodv2/chkgtway **Megfelelési művelet** Biztosítja, hogy a rendszer megfeleljen a megadott követelményeknek. **Megjegyzés:** Ez a beállítás nem módosul automatikusan, ha az irányelv visszaállításra kerül az AIX alapértelmezett irányelvre, a DoDv2_to_ használatával az AIXDefault.xml fájlhoz. Ezt a beállítást kézzel kell módosítani. **Megjegyzés:** Ha a saját rendszere IPv6 protokollt futtat. akkor gondoskodjon róla, hogy az *ipv6_enabled* beállítás az /etc/security/pscexpert/ipv6.conf fájlban yes értékre legyen beállítva. Ha a rendszer nem IPv6 protokollt használ, akkor gondoskodjon róla, hogy az *ipv6_enabled* no értékre legyen beállítva.
GEN005590	2	A rendszer nem futtathat semmilyen útválasztási protokoll démont, hacsak a rendszer nem útválasztó.	**Hely** /etc/security/pscexpert/dodv2/dodv2cmntrows **Megfelelési művelet** Biztosítja, hogy a rendszer megfeleljen a megadott követelményeknek.
GEN005590	2	A rendszer nem futtathat semmilyen útválasztási protokoll démont, hacsak a rendszer nem útválasztó.	**Hely** /etc/security/pscexpert/dodv2/dodv2cmntrows **Megfelelési művelet** Biztosítja, hogy a rendszer megfeleljen a megadott követelményeknek.
GEN005600	2	Az IP továbbításnak az IPv4-hez engedélyezettnek kell lenni, hacsak a rendszer nem útválasztó.	**Hely** /etc/security/pscexpert/dodv2/ntwkoptsdod **Megfelelési művelet** Az ipforwarding hálózati opció beállítása *0* értékre.
GEN005610	2	A rendszer IP továbbítása az IPv6-hoz nem lehet engedélyezett, hacsak a rendszer nem IPv6 útválasztó.	**Hely** /etc/security/pscexpert/dodv2/ntwkoptsdod **Megfelelési művelet** Az ip6forwarding hálózati opció beállítása *1* értékre.
GEN005820	2	Az NFS anonim UID és GID azonosítót engedélyeket nem tartalmazó értékekre kell beállítani.	**Hely** /etc/security/pscexpert/dodv2/nfsoptions **Megfelelési művelet** Biztosítja, hogy a megadott azonosítóknak ne legyenek engedélyeik.
GEN005840	2	Az NFS szervert be kell állítani a fájlrendszer elérésének korlátozására helyi hosztokra.	**Hely** /etc/security/pscexpert/dodv2/nfsoptions **Megfelelési művelet** NFS szerver beállítása a hozzáférés korlátozására helyi hosztokra.
GEN005880	2	Az NFS szerver nem engedélyezhet távoli root hozzáférést.	**Hely** /etc/security/pscexpert/dodv2/nfsoptions **Megfelelési művelet** Távoli root hozzáférés letiltása az NFS szerveren.
GEN005900	2	A *nosuid* opciót engedélyezni kell minden NFS kliens felépítésen.	**Hely** /etc/security/pscexpert/dodv2/nosuid **Megfelelési művelet** A *nosuid* opció engedélyezése minden NFS kliens felépítésen.

2. táblázat: DoD általános követelmények (Folytatás)

Department of Defense STIG ellenőrzési pont azonosító	STIG szabály kategóriája	Leírás	A parancsfájl helye, ahol a művelet meg van határozva, valamint a művelet eredménye, amely lehetővé teszi a megfelelést
GEN006060	2	A rendszer nem futtathat Samba programot, hacsak nem szükséges.	**Hely** /etc/security/pscexpert/dodv2/dodv2services **Megfelelési művelet** Biztosítja, hogy a rendszer megfeleljen a megadott követelményeknek.
GEN006380	1	A rendszer nem használhat UDP-t NIS és NIS+-hoz.	**Hely** /etc/security/pscexpert/dodv2/dodv2cat1 **Megfelelési művelet** A megadott szabálytesztelések eredményeinek megjelenítése.
GEN006400	2	A hálózati információs rendszer (NIS) protokoll nem használható.	**Hely** /etc/security/pscexpert/dodv2/nisplus **Megfelelési művelet** A megadott protokoll letiltása. **Megjegyzés:** Ez a beállítás nem módosul automatikusan, ha az irányelv visszaállításra kerül az AIX alapértelmezett irányelvre, a DoDv2_to_ használatával az AIXDefault.xml fájlhoz. Ezt a beállítást kézzel kell módosítani.
GEN006420	2	A NIS leképezéseket nehezen kitalálható tartománynevekkel kell védeni.	**Hely** /etc/security/pscexpert/dodv2/nisplus **Megfelelési művelet** Biztosítja, hogy a tartománynevek ne legyenek könnyen megállapíthatóak.
GEN006460	2	Minden NIS+ szervernek 2-es biztonsági szinten kell működni.	**Hely** /etc/security/pscexpert/dodv2/nisplus **Megfelelési művelet** Biztosítja, hogy a szerver a megadott minimális biztonsági szinten legyen. **Megjegyzés:** Ez a beállítás nem módosul automatikusan, ha az irányelv visszaállításra kerül az AIX alapértelmezett irányelvre, a DoDv2_to_ használatával az AIXDefault.xml fájlhoz. Ezt a beállítást kézzel kell módosítani.
GEN006480	2	A rendszeren hetente kell ellenőrizni a jogosulatlan setuid fájlokat, valamint a jogosulatlan módosításokat a hitelesített setuid fájlokban.	**Hely** /etc/security/pscexpert/dodv2/trust **Megfelelési művelet** Heti ellenőrzés a megadott fájlokban végzett módosítások azonosításához.
GEN006560	2	A rendszeren hetente kell ellenőrizni a jogosulatlan setuid fájlokat, valamint a jogosulatlan módosításokat a hitelesített setuid fájlokban.	**Hely** /etc/security/pscexpert/dodv2/trust **Megfelelési művelet** Heti ellenőrzés a megadott fájlokban végzett módosítások azonosításához.
GEN006580	2	A rendszernek hozzáférés-felügyeleti programot kell használni.	**Hely** /etc/security/pscexpert/dodv2/checktcpd **Megfelelési művelet** Biztosítja, hogy a rendszer megfeleljen a megadott követelményeknek.
GEN006600	2	A rendszer hozzáférés-felügyeleti programjának naplózni kell minden egyes hozzáférési kísérletet.	**Hely** /etc/security/pscexpert/dodv2/chsyslogdod **Megfelelési művelet** Biztosítja a hozzáférési kísérletek naplózását.

2. táblázat: DoD általános követelmények (Folytatás)

Department of Defense STIG ellenőrzési pont azonosító	STIG szabály kategóriája	Leírás	A parancsfájl helye, ahol a művelet meg van határozva, valamint a művelet eredménye, amely lehetővé teszi a megfelelést
GEN006620	2	A rendszer hozzáférés-felügyeleti programját úgy kell beállítani, hogy bizonyos hosztokhoz adjon rendszerhozzáférést vagy tagadja meg őket.	**Hely** /etc/security/pscexpert/dodv2/chetchostsdod **Megfelelési művelet** A hosts.deny és a hosts.allow fájl beállítása a szükséges beállításokra.
GEN007020	2	A Folyamvezérlő átviteli protokollt (SCTP) le kell tiltani.	**Hely** /etc/security/pscexpert/dodv2/dodv2netrules **Megfelelési művelet** A megadott protokoll letiltása.
GEN007700	2	Az IPv6 protokollkezelő nem köthető a hálózati veremhez, hacsak nincs rá szükség.	**Hely** /etc/security/pscexpert/dodv2/rminet6 **Megfelelési művelet** Letiltja az IPv6 protokollkezelőt a hálózati veremből, hacsak a kezelő meg nincs adva az /etc/ipv6.conf fájlban. **Megjegyzés:** Ha a rendszer IPv6 protokollt futtat, akkor gondoskodjon róla, hogy az *ipv6_enabled* beállítás az /etc/security/pscexpert/ipv6.conf fájlban yes értékre legyen beállítva. Ha a rendszer nem IPv6 protokollt használ, akkor gondoskodjon róla, hogy az *ipv6_enabled* beállítás no értékre legyen beállítva.
GEN007780	2	A rendszeren nem lehet engedélyezett 6to4 alagút.	**Hely** /etc/security/pscexpert/dodv2/rmiface **Megfelelési művelet** A megadott alagutak letiltása. **Megjegyzés:** Ez a beállítás nem módosul automatikusan, ha az irányelv visszaállításra kerül az AIX alapértelmezett irányelvre, a DoDv2_to_ használatával az AIXDefault.xml fájlhoz. Ezt a beállítást kézzel kell módosítani.
GEN007820	2	A rendszeren nem lehet beállítva IP alagút.	**Hely** /etc/security/pscexpert/dodv2/rmtunnel **Megfelelési művelet** IP alagutak letiltása. **Megjegyzés:** Ez a beállítás nem módosul automatikusan, ha az irányelv visszaállításra kerül az AIX alapértelmezett irányelvre, a DoDv2_to_ használatával az AIXDefault.xml fájlhoz. Ezt a beállítást kézzel kell módosítani.
GEN007840	2	A DHCP ügyfelet le kell tiltani, ha nincs használatban.	**Hely** /etc/security/pscexpert/dodv2/dodv2services **Megfelelési művelet** Biztosítja, hogy a rendszer megfeleljen a megadott követelményeknek.
GEN007850	2	A DHCP ügyfél nem küldhet dinamikus DNS frissítéseket.	**Hely** /etc/security/pscexpert/dodv2/dodv2services **Megfelelési művelet** Biztosítja, hogy a rendszer megfeleljen a megadott követelményeknek.
GEN007860	2	A rendszernek figyelmen kívül kell hagyni az IPv6 ICMP átirányítási üzeneteket.	**Hely** /etc/security/pscexpert/dodv2/ntwkoptsdod **Megfelelési művelet** Az ipignoreredirects hálózati opció beállítása *1* értékre.

2. táblázat: DoD általános követelmények (Folytatás)

Department of Defense STIG ellenőrzési pont azonosító	**STIG szabály kategóriája**	**Leírás**	**A parancsfájl helye, ahol a művelet meg van határozva, valamint a művelet eredménye, amely lehetővé teszi a megfelelést**
GEN007880	2	A rendszer nem küldhet IPv6 ICMP átirányításokat.	**Hely** /etc/security/pscexpert/dodv2/ntwkoptsdod **Megfelelési művelet** Az ipsendredirects hálózati opció értékének beállítása *0* értékre.
GEN007900	2	A rendszernek megfelelő fordított útvonal szűrőt kell használni az IPv6 hálózati forgalomhoz, ha a rendszer IPv6 protokollt használ.	**Hely** /etc/security/pscexpert/dodv2/chuserstanzadod **Megfelelési művelet** Biztosítja, hogy a rendszer megfeleljen a megadott követelményeknek.
GEN007920	2	A rendszer nem továbbíthat IPv6 forráshoz irányított csomagokat.	**Hely** /etc/security/pscexpert/dodv2/ntwkoptsdod **Megfelelési művelet** Az ip6srcrouteforward hálózati opció beállítása *0* értékre.
GEN007940: GEN003607	2	A rendszer nem fogadhatja el a forráshoz irányított IPv4 és IPv6 csomagokat.	**Hely** /etc/security/pscexpert/dodv2/ntwkoptsdod **Megfelelési művelet** Az ipsrcrouterecv hálózati opció beállítása *0* értékre.
GEN007950	2	A rendszer nem válaszolhat az üzenetszórási címre küldött ICMPv6 visszhang kérésekre.	**Hely** /etc/security/pscexpert/dodv2/ntwkoptsdod **Megfelelési művelet** A bcastping hálózati opció értékének beállítása *0* értékre.
GEN008000	2	Ha a rendszer Egyszerűsített címtárhozzáférési protokollt (LDAP) használ a hitelesítéshez vagy a fiókinformációkhoz, akkor az LDAP szerverre történő hitelesítéshez használt tanúsítványokat a DoD PKI vagy a DoD-approved metódusból kell megadni.	**Hely** /etc/security/pscexpert/dodv2/ldap_config **Megfelelési művelet** Biztosítja, hogy a rendszer megfeleljen a megadott követelményeknek.
GEN008020	2	Ha a rendszer LDAP protokollt használ a hitelesítéshez vagy a fiókinformációkhoz, akkor az LDAP Szállítási réteg biztonság (TLS) kapcsolatnak meg kell követelni, hogy a szerver érvényes megbízható útvonallal adja meg a tanúsítványt.	**Hely** /etc/security/pscexpert/dodv2/ldap_config **Megfelelési művelet** Biztosítja, hogy a rendszer megfeleljen a megadott követelményeknek.
GEN008050	2	Ha a rendszer LDAP protokollt használ a hitelesítéshez vagy a fiókinformációkhoz, akkor az /etc/ldap.conf fájl (vagy egyenértékű) nem tartalmazhat jelszót.	**Hely** /etc/security/pscexpert/dodv2/ldap_config **Megfelelési művelet** Biztosítja, hogy a rendszer megfeleljen a megadott követelményeknek.

2. táblázat: DoD általános követelmények (Folytatás)

Department of Defense STIG ellenőrzési pont azonosító	STIG szabály kategóriája	Leírás	A parancsfájl helye, ahol a művelet meg van határozva, valamint a művelet eredménye, amely lehetővé teszi a megfelelést
GEN008380	2	A rendszeren hetente kell ellenőrizni a jogosulatlan setuid fájlokat, valamint a jogosulatlan módosításokat a hitelesített setuid fájlokban.	**Hely** /etc/security/pscexpert/dodv2/trust **Megfelelési művelet** Heti ellenőrzés a megadott fájlokban végzett módosítások azonosításához.
GEN008520	2	A rendszeren helyi tűzfalat kell alkalmazni, amely megvédi a hosztot a portelemzésekkel szemben. A tűzfalnak el kell kerülnie a támadható portokat 5 percig, hogy megvédje a hosztot a portelemzésekkel szemben.	**Hely** /etc/security/pscexpert/dodv2/ipsecshunports **Megfelelési művelet** Biztosítja, hogy a rendszer megfeleljen a megadott követelményeknek.
GEN008540	2	A rendszer helyi tűzfalának meg kell valósítani az *összes visszautasítása*, *engedélyezés kivétel alapján* irányelvet.	**Hely** /etc/security/pscexpert/dodv2/ipsecshunhosthls **Megfelelési művelet** Biztosítja, hogy a rendszer megfeleljen a megadott követelményeknek. **Megjegyzés:** További szűrőszabályokat is megadhat az /etc/security/aixpert/bin/filter.txt fájlban. Ezeket a szabályokat az ipsecshunhosthls.sh parancsfájl integrálja a profil alkalmazásakor. A bejegyzéseknek a következő formátumban kell lenni: *portszám*:*ip_cím*: *művelet* Ahol a *művelet* lehetséges értékei az Allow és a Deny.
GEN008600	1	A rendszert úgy kell beállítani, hogy csak a rendszerbetöltési konfigurációból induljon.	**Hely** /etc/security/pscexpert/dodv2/dodv2cat1 **Megfelelési művelet** Biztosítja, hogy a rendszer indítása csak a rendszerbetöltési konfigurációt használja.
GEN008640	1	A rendszer nem használhat cserélhető adathordozót rendszerbetöltőként.	**Hely** /etc/security/pscexpert/dodv2/dodv2cat1 **Megfelelési művelet** Biztosítja, hogy a rendszer ne kerüljön betöltésre cserélhető meghajtóból.
GEN009140	1,2,3	A rendszeren nem lehet aktív a chargen szolgáltatás.	**Hely** /etc/security/pscexpert/dodv2/inetdservices **Megfelelési művelet** Letiltja a szükséges démonokat és szolgáltatásokat a bejegyzések kikommentezésével az /etc/inetd.conf fájlban.
GEN009160	1,2,3	A rendszeren nem lehet aktív a Calendar Management Service Daemon (CMSD) szolgáltatás.	**Hely** /etc/security/pscexpert/dodv2/inetdservices **Megfelelési művelet** Letiltja a szükséges démonokat és szolgáltatásokat a bejegyzések kikommentezésével az /etc/inetd.conf fájlban.
GEN009180	1,2,3	A rendszeren nem lehet aktív a tool-talk database server (ttdbserver) szolgáltatás.	**Hely** /etc/security/pscexpert/dodv2/inetdservices **Megfelelési művelet** Letiltja a szükséges démonokat és szolgáltatásokat a bejegyzések kikommentezésével az /etc/inetd.conf fájlban.

2. táblázat: DoD általános követelmények (Folytatás)

Department of Defense STIG ellenőrzési pont azonosító	**STIG szabály kategóriája**	**Leírás**	**A parancsfájl helye, ahol a művelet meg van határozva, valamint a művelet eredménye, amely lehetővé teszi a megfelelést**
GEN009190	1,2,3	A rendszeren nem lehet aktív a comsat szolgáltatás.	**Hely** /etc/security/pscexpert/dodv2/inetdservices **Megfelelési művelet** Letiltja a szükséges démonokat és szolgáltatásokat a bejegyzések kikommentezésével az /etc/inetd.conf fájlban.
GEN009200-9330	1,2,3	A rendszeren nem lehet aktív más szolgáltatás és démon.	**Hely** /etc/security/pscexpert/dodv2/inetdservices **Megfelelési művelet** Letiltja a szükséges démonokat és szolgáltatásokat a bejegyzések kikommentezésével az /etc/inetd.conf fájlban.
GEN009210	2	A rendszeren nem lehet aktív a discard szolgáltatás.	**Hely** /etc/security/pscexpert/dodv2/inetdservices **Megfelelési művelet** Letiltja a szükséges démonokat és szolgáltatásokat a bejegyzések kikommentezésével az /etc/inetd.conf fájlban.
GEN009220	2	A rendszeren nem lehet aktív a dtspc szolgáltatás.	**Hely** /etc/security/pscexpert/dodv2/inetdservices **Megfelelési művelet** Letiltja a szükséges démonokat és szolgáltatásokat a bejegyzések kikommentezésével az /etc/inetd.conf fájlban.
GEN009230	2	A rendszeren nem lehet aktív az echo szolgáltatás.	**Hely** /etc/security/pscexpert/dodv2/inetdservices **Megfelelési művelet** Letiltja a szükséges démonokat és szolgáltatásokat a bejegyzések kikommentezésével az /etc/inetd.conf fájlban.
GEN009240	2	A rendszeren nem lehet aktív az Internet Message Access Protocol (IMAP) szolgáltatás.	**Hely** /etc/security/pscexpert/dodv2/inetdservices **Megfelelési művelet** Letiltja a szükséges démonokat és szolgáltatásokat a bejegyzések kikommentezésével az /etc/inetd.conf fájlban.
GEN009250	2	A rendszeren nem lehet aktív a PostOffice Protocol (POP3) szolgáltatás.	**Hely** /etc/security/pscexpert/dodv2/inetdservices **Megfelelési művelet** Letiltja a szükséges démonokat és szolgáltatásokat a bejegyzések kikommentezésével az /etc/inetd.conf fájlban.
GEN009260	2	A rendszeren nem lehet aktív a talk és ntalk szolgáltatás.	**Hely** /etc/security/pscexpert/dodv2/inetdservices **Megfelelési művelet** Letiltja a szükséges démonokat és szolgáltatásokat a bejegyzések kikommentezésével az /etc/inetd.conf fájlban.
GEN009270	2	A rendszer nem aktiválhatja a netstat szolgáltatást az InetD folyamaton.	**Hely** /etc/security/pscexpert/dodv2/inetdservices **Megfelelési művelet** Letiltja a szükséges démonokat és szolgáltatásokat a bejegyzések kikommentezésével az /etc/inetd.conf fájlban.
GEN009280	2	A rendszeren nem lehet aktív a PCNFS szolgáltatás.	**Hely** /etc/security/pscexpert/dodv2/inetdservices **Megfelelési művelet** Letiltja a szükséges démonokat és szolgáltatásokat a bejegyzések kikommentezésével az /etc/inetd.conf fájlban.

2. táblázat: DoD általános követelmények (Folytatás)

Department of Defense STIG ellenőrzési pont azonosító	STIG szabály kategóriája	Leírás	A parancsfájl helye, ahol a művelet meg van határozva, valamint a művelet eredménye, amely lehetővé teszi a megfelelést
GEN009290	2	A rendszeren nem lehet aktív a systat szolgáltatás.	**Hely** /etc/security/pscexpert/dodv2/inetdservices **Megfelelési művelet** Letiltja a szükséges démonokat és szolgáltatásokat a bejegyzések kikommentezésével az /etc/inetd.conf fájlban.
GEN009300	2	Az inetd time szolgáltatás nem lehet aktív a rendszeren, az inetd démonon.	**Hely** /etc/security/pscexpert/dodv2/inetdservices **Megfelelési művelet** Letiltja a szükséges démonokat és szolgáltatásokat a bejegyzések kikommentezésével az /etc/inetd.conf fájlban.
GEN009310	2	A rendszeren nem lehet aktív az rusersd szolgáltatás.	**Hely** /etc/security/pscexpert/dodv2/inetdservices **Megfelelési művelet** Letiltja a szükséges démonokat és szolgáltatásokat a bejegyzések kikommentezésével az /etc/inetd.conf fájlban.
GEN009320	2	A rendszeren nem lehet aktív az sprayd szolgáltatás.	**Hely** /etc/security/pscexpert/dodv2/inetdservices **Megfelelési művelet** Letiltja a szükséges démonokat és szolgáltatásokat a bejegyzések kikommentezésével az /etc/inetd.conf fájlban.
GEN009330	2	A rendszeren nem lehet aktív az rstatd szolgáltatás.	**Hely** /etc/security/pscexpert/dodv2/inetdservices **Megfelelési művelet** Letiltja a szükséges démonokat és szolgáltatásokat a bejegyzések kikommentezésével az /etc/inetd.conf fájlban.
GEN009340	2	Az X server bejelentkezéskezelők nem futtathatók, hacsak nem szükségesek az X11 munkamenet-kezeléshez.	**Hely** /etc/security/pscexpert/dodv2/dodv2cmntrows **Megfelelési művelet** Ez a szabály letiltja az X Window System kapcsolatokat és az XServer bejelentkezés-kezelőt.

3. táblázat: DoD tulajdonjog követelmények

Department of Defense STIG ellenőrzési pont azonosító	Leírás	A parancsfájl helye, ahol a művelet meg van határozva, valamint a művelet eredménye, amely lehetővé teszi a megfelelést
AIX00085	Az /etc/netsvc.conf fájl tulajdonosának root felhasználónak kell lenni.	**Hely** /etc/security/pscexpert/dodv2/chowndodfiles **Megfelelési művelet** Biztosítja, hogy a megadott fájl tulajdonosa root legyen.
AIX00090	Az /etc/netsvc.conf fájl csoportosan legyen birtokolva a bin, sys és system által.	**Hely** /etc/security/pscexpert/dodv2/chowndodfiles **Megfelelési művelet** Biztosítja, hogy a megadott fájl csoportosan legyen birtokolva a bin, sys és system által.
AIX00320	Az /etc/ftpaccess.ctl fájl tulajdonosának root felhasználónak kell lenni.	**Hely** /etc/security/pscexpert/dodv2/chowndodfiles **Megfelelési művelet** Biztosítja, hogy a megadott fájl tulajdonosa root legyen.

3. táblázat: DoD tulajdonjog követelmények (Folytatás)

Department of Defense STIG ellenőrzési pont azonosító	**Leírás**	**A parancsfájl helye, ahol a művelet meg van határozva, valamint a művelet eredménye, amely lehetővé teszi a megfelelést**
AIX00330	Az /etc/ftpaccess.ctl fájl csoportosan legyen birtokolva a bin, sys és system által.	**Hely** /etc/security/pscexpert/dodv2/chowndodfiles **Megfelelési művelet** Biztosítja, hogy a megadott fájl csoportosan legyen birtokolva a bin, sys és system által.
GEN000250	Az időszinkronizálási konfigurációs fájl (például /etc/ntp.conf) tulajdonosának root felhasználónak kell lenni.	**Hely** /etc/security/pscexpert/dodv2/chowndodfiles **Megfelelési művelet** Biztosítja, hogy a megadott fájl tulajdonosa root legyen.
GEN000251	Az időszinkronizálási konfigurációs fájl (például /etc/ntp.conf) csoportosan legyen birtokolva a bin, sys és system által.	**Hely** /etc/security/pscexpert/dodv2/chowndodfiles **Megfelelési művelet** Biztosítja, hogy a megadott fájl csoportosan legyen birtokolva a bin, sys és system által.
GEN001160	Minden fájlnak és könyvtárnak érvényes tulajdonossal kell rendelkeznie.	**Hely** /etc/security/pscexpert/dodv2/chowndodfiles **Megfelelési művelet** Biztosítja, hogy minden fájlnak és könyvtárnak érvényes tulajdonosa legyen.
GEN001170	Minden fájlnak és könyvtárnak érvényes csoport tulajdonossal kell rendelkeznie.	**Hely** /etc/security/pscexpert/dodv2/chowndodfiles **Megfelelési művelet** Biztosítja, hogy minden fájlnak és könyvtárnak érvényes tulajdonosa legyen.
GEN001220	Minden rendszerfájl, program és könyvtár tulajdonosának rendszerfióknak kell lenni.	**Hely** /etc/security/pscexpert/dodv2/chowndodfiles **Megfelelési művelet** Biztosítja, hogy a rendszerfájlok, programok és könyvtárat tulajdonosa a rendszerfiók legyen.
GEN001240	A rendszerfájlokat, programokat és könyvtárakat csoportosan kell birtokolni egy rendszercsoportnak.	**Hely** /etc/security/pscexpert/dodv2/chowndodfiles **Megfelelési művelet** Minden rendszerfájlt, programot és könyvtárat csoportosan birtokol egy rendszercsoport.
GEN001320	A hálózati információs rendszerek (NIS)/NIS+/yp fájljait root, sys vagy bin birtokolhatja.	**Hely** /etc/security/pscexpert/dodv2/chowndodfiles **Megfelelési művelet** Biztosítja, hogy a megadott fájlokat root, sys vagy bin birtokolja.
GEN001340	A NIS/NIS+/yp fájlok csoportosan legyenek birtokolva a sys, bin, other vagy system által.	**Hely** /etc/security/pscexpert/dodv2/chowndodfiles **Megfelelési művelet** Biztosítja, hogy a megadott fájlokat a sys, bin, other, vagy system birtokolja.
GEN001362	Az /etc/resolv.conf fájl tulajdonosának root felhasználónak kell lenni.	**Hely** /etc/security/pscexpert/dodv2/chowndodfiles **Megfelelési művelet** Biztosítja, hogy a megadott fájl tulajdonosa root legyen.
GEN001363	Az /etc/resolv.conf fájl csoportosan legyen birtokolva a bin, sys és system által.	**Hely** /etc/security/pscexpert/dodv2/chowndodfiles **Megfelelési művelet** Biztosítja, hogy a megadott fájl csoportosan legyen birtokolva a bin, sys és system által.

3. táblázat: DoD tulajdonjog követelmények (Folytatás)

Department of Defense STIG ellenőrzési pont azonosító	**Leírás**	**A parancsfájl helye, ahol a művelet meg van határozva, valamint a művelet eredménye, amely lehetővé teszi a megfelelést**
GEN001366	Az /etc/hosts fájl tulajdonosának root felhasználónak kell lenni.	**Hely** /etc/security/pscexpert/dodv2/chowndodfiles **Megfelelési művelet** Biztosítja, hogy a megadott fájl tulajdonosa root legyen.
GEN001367	Az /etc/hosts fájl csoportosan legyen birtokolva a bin, sys és system által.	**Hely** /etc/security/pscexpert/dodv2/chowndodfiles **Megfelelési művelet** Biztosítja, hogy a megadott fájl csoportosan legyen birtokolva a bin, sys és system által.
GEN001371	Az /etc/nsswitch.conf fájl tulajdonosának root felhasználónak kell lenni.	**Hely** /etc/security/pscexpert/dodv2/chowndodfiles **Megfelelési művelet** Biztosítja, hogy a megadott fájl tulajdonosa root legyen.
GEN001372	Az /etc/nsswitch.conf fájl csoportosan legyen birtokolva a root, bin, sys és system által.	**Hely** /etc/security/pscexpert/dodv2/chowndodfiles **Megfelelési művelet** Biztosítja, hogy a megadott fájl csoportosan legyen birtokolva a root, bin, sys és system által.
GEN001378	Az /etc/passwd fájl tulajdonosának root felhasználónak kell lenni.	**Hely** /etc/security/pscexpert/dodv2/chowndodfiles **Megfelelési művelet** Biztosítja, hogy a megadott fájl tulajdonosa root legyen.
GEN001379	Az /etc/passwd fájl csoportosan legyen birtokolva a bin, security, sys és system által.	**Hely** /etc/security/pscexpert/dodv2/chowndodfiles **Megfelelési művelet** Biztosítja, hogy a megadott fájl csoportosan legyen birtokolva a bin, security, sys és system által.
GEN001391	Az /etc/group fájl tulajdonosának root felhasználónak kell lenni.	**Hely** /etc/security/pscexpert/dodv2/chowndodfiles **Megfelelési művelet** Biztosítja, hogy a megadott fájl tulajdonosa root legyen.
GEN001392	Az /etc/group fájl csoportosan legyen birtokolva a bin, security, sys és system által.	**Hely** /etc/security/pscexpert/dodv2/chowndodfiles **Megfelelési művelet** Biztosítja, hogy a megadott fájl csoportosan legyen birtokolva a bin, security, sys és system által.
GEN001400	Az /etc/security/passwd fájl tulajdonosának root felhasználónak kell lenni.	**Hely** /etc/security/pscexpert/dodv2/chowndodfiles **Megfelelési művelet** Biztosítja, hogy a megadott fájl tulajdonosa root legyen.
GEN001410	Az /etc/security/passwd fájl csoportosan legyen birtokolva a bin, security, sys és system által.	**Hely** /etc/security/pscexpert/dodv2/chowndodfiles **Megfelelési művelet** Biztosítja, hogy a megadott fájl csoportosan legyen birtokolva a bin, security, sys és system által.
GEN001500	Minden interaktív felhasználó saját könyvtárát a vonatkozó felhasználónak kell birtokolnia.	**Hely** /etc/security/pscexpert/dodv2/chowndodfiles **Megfelelési művelet** Biztosítja, hogy minden interaktív felhasználó saját könyvtárát a vonatkozó felhasználó birtokolja.

3. táblázat: DoD tulajdonjog követelmények (Folytatás)

Department of Defense STIG ellenőrzési pont azonosító	**Leírás**	**A parancsfájl helye, ahol a művelet meg van határozva, valamint a művelet eredménye, amely lehetővé teszi a megfelelést**
GEN001520	Minden interaktív felhasználó saját könyvtárát csoportosan kell birtokolni a könyvtár tulajdonosának elsődleges csoportja által.	**Hely** /etc/security/pscexpert/dodv2/chowndodfiles **Megfelelési művelet** Biztosítja, hogy minden interaktív felhasználó saját könyvtárát csoportosan birtokolja a könyvtár tulajdonosának elsődleges csoportja.
GEN001540	Az interaktív felhasználó saját könyvtárában tartalmazott összes fájl és könyvtár tulajdonosának a saját könyvtár tulajdonosának kell lenni.	**Hely** /etc/security/pscexpert/dodv2/chowndodfiles **Megfelelési művelet** Biztosítja, hogy az interaktív felhasználó saját könyvtárában tartalmazott összes fájl és könyvtár tulajdonosa a saját könyvtár tulajdonosa legyen.
GEN001550	A felhasználó saját könyvtáraiban tartalmazott összes fájl és könyvtár tulajdonosának olyan csoportnak kell lenni, amelyben a saját könyvtár tulajdonosa tag.	**Hely** /etc/security/pscexpert/dodv2/chowndodfiles **Megfelelési művelet** Biztosítja, hogy a felhasználó saját könyvtáraiban tartalmazott összes fájl és könyvtár tulajdonosa olyan csoport legyen, amelyben a saját könyvtár tulajdonosa tag.
GEN001660	Minden rendszerindítási fájl tulajdonosának root felhasználónak kell lenni.	**Hely** /etc/security/pscexpert/dodv2/chowndodfiles **Megfelelési művelet** Biztosítja, hogy a megadott fájlok tulajdonosa root felhasználó legyen.
GEN001680	Minden rendszerindítási fájl csoportosan legyenek birtokolva a sys, bin, other vagy system által.	**Hely** /etc/security/pscexpert/dodv2/chowndodfiles **Megfelelési művelet** Biztosítja, hogy a megadott fájlokat a sys, bin, other, vagy system csoportosan birtokolja.
GEN001740	Minden globális inicializálási fájl tulajdonosának root felhasználónak kell lenni.	**Hely** /etc/security/pscexpert/dodv2/chowndodfiles **Megfelelési művelet** Biztosítja, hogy a megadott fájlok tulajdonosa root felhasználó legyen.
GEN001760	Minden globális inicializálási fájl csoportosan legyen birtokolva a sys, bin, system vagy security által.	**Hely** /etc/security/pscexpert/dodv2/chowndodfiles **Megfelelési művelet** Biztosítja, hogy a megadott fájlokat a sys, bin, system, vagy security csoportosan birtokolja.
GEN001820	Minden váz fájl és könyvtár (jellemzően az /etc/skel fájlban) tulajdonosának root vagy bin felhasználónak kell lenni.	**Hely** /etc/security/pscexpert/dodv2/chowndodfiles **Megfelelési művelet** Biztosítja, hogy a megadott fájlok és könyvtárak tulajdonosa root vagy bin felhasználó legyen.
GEN001830	Minden váz fájl (jellemzően az /etc/skel fájlban) csoportosan legyen birtokolva a security által.	**Hely** /etc/security/pscexpert/dodv2/chowndodfiles **Megfelelési művelet** Biztosítja, hogy a megadott fájlokat csoportosan birtokolja a security.
GEN001860	Minden helyi inicializálási fájl tulajdonosának felhasználónak vagy root felhasználónak kell lenni.	**Hely** /etc/security/pscexpert/dodv2/chowndodfiles **Megfelelési művelet** Biztosítja, hogy a megadott fájlok tulajdonosa felhasználó vagy root felhasználó legyen.

3. táblázat: DoD tulajdonjog követelmények (Folytatás)

Department of Defense STIG ellenőrzési pont azonosító	Leírás	A parancsfájl helye, ahol a művelet meg van határozva, valamint a művelet eredménye, amely lehetővé teszi a megfelelést
GEN001870	A helyi inicializálási fájlokat csoportosan kell birtokolni a felhasználó elsődleges csoportja vagy a root felhasználó által.	**Hely** /etc/security/pscexpert/dodv2/chowndodfiles **Megfelelési művelet** Biztosítja, hogy a helyi inicializálási fájlokat csoportosan birtokolja a felhasználó elsődleges csoportja vagy a root felhasználó.
GEN002060	Minden .rhosts, .shosts, .netrc és hosts.equiv fájlhoz csak a root felhasználó vagy a fájl tulajdonosa férhet hozzá.	**Hely** /etc/security/pscexpert/dodv2/chowndodfiles /etc/security/pscexpert/dodv2/fpmdodfiles **Megfelelési művelet** Biztosítja, hogy csak a root felhasználó vagy a tulajdonos férjen hozzá a megadott fájlokhoz.
GEN002100	Az .rhosts fájlt nem támogathatja a cserélhető hitelesítési modul (PAM).	**Hely** /etc/security/pscexpert/dodv2/chowndodfiles **Megfelelési művelet** Biztosítja, hogy a megadott fájl ne legyen elérhető PAM használatával.
GEN002200	Minden parancsértelmező fájl tulajdonosának root vagy bin felhasználónak kell lenni.	**Hely** /etc/security/pscexpert/dodv2/chowndodfiles **Megfelelési művelet** Biztosítja, hogy a megadott fájlok tulajdonosa root vagy bin felhasználó legyen.
GEN002210	Minden parancsértelmező fájl csoportosan legyen birtokolva a root, bin, sys vagy system által.	**Hely** /etc/security/pscexpert/dodv2/chowndodfiles **Megfelelési művelet** Biztosítja, hogy a megadott fájlokat a root, bin, sys vagy system csoportosan birtokolja.
GEN002340	Az audioeszközök tulajdonosának root felhasználónak kell lenni.	**Hely** /etc/security/pscexpert/dodv2/chowndodfiles **Megfelelési művelet** Biztosítja, hogy az összes audioeszköz tulajdonosa root felhasználó legyen.
GEN002360	Az audioeszközök csoportosan legyenek birtokolva a root, sys, bin vagy system által.	**Hely** /etc/security/pscexpert/dodv2/chowndodfiles **Megfelelési művelet** Biztosítja, hogy minden audioeszköz csoportosan legyen birtokolva a root, sys, bin vagy system által.
GEN002520	Minden nyilvános könyvtár tulajdonosának root felhasználónak vagy alkalmazásfióknak kell lenni.	**Hely** /etc/security/pscexpert/dodv2/chowndodfiles **Megfelelési művelet** Biztosítja, hogy minden nyilvános könyvtár tulajdonosa root felhasználó vagy alkalmazásfiók legyen.
GEN002540	Minden nyilvános könyvtár csoportosan legyen birtokolva rendszer vagy alkalmazáscsoport által.	**Hely** /etc/security/pscexpert/dodv2/chowndodfiles **Megfelelési művelet** Biztosítja, hogy minden nyilvános könyvtár csoportos tulajdonosa rendszer vagy alkalmazáscsoport legyen.
GEN002680	A rendszer megfigyelési naplói tulajdonosának root felhasználónak kell lenni.	**Hely** /etc/security/pscexpert/dodv2/chowndodfiles **Megfelelési művelet** Biztosítja, hogy a megadott fájlok tulajdonosa root felhasználó legyen.

3. táblázat: DoD tulajdonjog követelmények (Folytatás)

Department of Defense STIG ellenőrzési pont azonosító	**Leírás**	**A parancsfájl helye, ahol a művelet meg van határozva, valamint a művelet eredménye, amely lehetővé teszi a megfelelést**
GEN002690	Minden rendszer megfigyelési napló csoportosan legyen birtokolva a bin, sys vagy system által.	**Hely** /etc/security/pscexpert/dodv2/chowndodfiles **Megfelelési művelet** Biztosítja, hogy a megadott fájlokat a bin, sys vagy system csoportosan birtokolja.
GEN003020	A Cron nem futtathat programokat a bárki számára írható könyvtárakban vagy ezek leszármazottaiban.	**Hely** /etc/security/pscexpert/dodv2/chowndodfiles **Megfelelési művelet** Megakadályozza, hogy a cron programokat futtasson a bárki számára írható könyvtárakban vagy ezek leszármazottaiban.
GEN003040	A Crontabs tulajdonosának root felhasználónak vagy a crontab létrehozójának kell lenni.	**Hely** /etc/security/pscexpert/dodv2/chowndodfiles **Megfelelési művelet** Biztosítja, hogy a crontab tulajdonosa root felhasználó vagy a crontab létrehozó legyen.
GEN003050	A Crontab fájlok csoportosan legyenek birtokolva a system, cron vagy a crontab létrehozójának elsődleges csoportja által.	**Hely** /etc/security/pscexpert/dodv2/chowndodfiles **Megfelelési művelet** Biztosítja, hogy a crontab fájlok csoportosan legyenek birtokolva a system, cron vagy a crontab létrehozójának elsődleges csoportja által.
GEN003110	A Cron és a crontab könyvtárnak nem lehet kiterjesztett hozzáférés-felügyeleti listája.	**Hely** /etc/security/pscexpert/dodv2/chowndodfiles **Megfelelési művelet** Biztosítja, hogy a megadott könyvtáraknak ne legyen kiterjesztett hozzáférés-felügyeleti listája.
GEN003120	A Cron és a crontab könyvtár tulajdonosának root vagy bin felhasználónak kell lenni.	**Hely** /etc/security/pscexpert/dodv2/chowndodfiles **Megfelelési művelet** Biztosítja, hogy a cron és a crontab könyvtára tulajdonosa root vagy bin legyen.
GEN003140	A Cron és a crontab könyvtárat csoportosan birtokolja a system, sys, bin vagy a cron.	**Hely** /etc/security/pscexpert/dodv2/chowndodfiles **Megfelelési művelet** Biztosítja, hogy a megadott könyvtárakat csoportosan birtokolja a system, sys, bin vagy a cron.
GEN003160	A cron naplózást meg kell valósítani.	**Hely** /etc/security/pscexpert/dodv2/chowndodfiles **Megfelelési művelet** Biztosítja a cron naplózás megvalósítását.
GEN003240	A cron.allow fájl tulajdonosának root, bin vagy sys felhasználónak kell lenni.	**Hely** /etc/security/pscexpert/dodv2/chowndodfiles **Megfelelési művelet** Biztosítja, hogy a megadott fájl tulajdonosa root, bin vagy sys legyen.
GEN003250	A cron.allow fájlt csoportosan birtokolja a system, bin, sys vagy cron.	**Hely** /etc/security/pscexpert/dodv2/chowndodfiles **Megfelelési művelet** Biztosítja, hogy a megadott fájlt csoportosan birtokolja asystem, bin, sys vagy a cron.

3. táblázat: DoD tulajdonjog követelmények (Folytatás)

Department of Defense STIG ellenőrzési pont azonosító	**Leírás**	**A parancsfájl helye, ahol a művelet meg van határozva, valamint a művelet eredménye, amely lehetővé teszi a megfelelést**
GEN003260	A cron.deny fájl tulajdonosának root, bin vagy sys felhasználónak kell lenni.	**Hely** /etc/security/pscexpert/dodv2/chowndodfiles **Megfelelési művelet** Biztosítja, hogy a megadott fájl tulajdonosa root, bin vagy sys legyen.
GEN003270	A cron.deny fájlt csoportosan birtokolja a system, bin, sys vagy cron.	**Hely** /etc/security/pscexpert/dodv2/chowndodfiles **Megfelelési művelet** Biztosítja, hogy a megadott fájlt csoportosan birtokolja asystem, bin, sys vagy a cron.
GEN003420	Az at könyvtár tulajdonosának root, bin, sys, daemon vagy cron felhasználónak kell lenni.	**Hely** /etc/security/pscexpert/dodv2/chowndodfiles **Megfelelési művelet** Biztosítja, hogy a megadott könyvtár tulajdonosa root, sys, daemon vagy cron legyen.
GEN003430	Az at könyvtárat csoportosan birtokolja a system, bin, sys vagy cron.	**Hely** /etc/security/pscexpert/dodv2/chowndodfiles **Megfelelési művelet** Biztosítja, hogy a megadott könyvtárat csoportosan birtokolja asystem, bin, sys vagy a cron.
GEN003460	Az at.allow fájl tulajdonosának root, bin vagy sys felhasználónak kell lenni.	**Hely** /etc/security/pscexpert/dodv2/chowndodfiles **Megfelelési művelet** Biztosítja, hogy a megadott fájl tulajdonosa root, bin vagy sys legyen.
GEN003470	Az at.allow fájlt csoportosan birtokolja a system, bin, sys vagy cron.	**Hely** /etc/security/pscexpert/dodv2/chowndodfiles **Megfelelési művelet** Biztosítja, hogy a megadott fájlt csoportosan birtokolja asystem, bin, sys vagy a cron.
GEN003480	Az at.deny fájl tulajdonosának root, bin vagy sys felhasználónak kell lenni.	**Hely** /etc/security/pscexpert/dodv2/chowndodfiles **Megfelelési művelet** Biztosítja, hogy a megadott fájl tulajdonosa root, bin vagy sys legyen.
GEN003490	Az at.deny fájlt csoportosan birtokolja a system, bin, sys vagy cron.	**Hely** /etc/security/pscexpert/dodv2/chowndodfiles **Megfelelési művelet** Biztosítja, hogy a megadott fájlt csoportosan birtokolja asystem, bin, sys vagy a cron.
GEN003720	Az inetd.conf és xinetd.conf fájl, valamint az xinetd.d könyvtár tulajdonosának root vagy bin felhasználónak kell lenni.	**Hely** /etc/security/pscexpert/dodv2/chowndodfiles **Megfelelési művelet** Biztosítja, hogy a megadott fájlok és könyvtár tulajdonosa root vagy bin felhasználó legyen.
GEN003730	Az inetd.conf és xinetd.conf fájl, valamint a xinetd.d könyvtár csoportosan legyen birtokolva a bin, sys vagy system által.	**Hely** /etc/security/pscexpert/dodv2/chowndodfiles **Megfelelési művelet** Biztosítja, hogy a megadott fájlokat és a könyvtárat a bin, sys vagy system csoportosan birtokolja.
GEN003760	A services fájl tulajdonosa root vagy bin legyen.	**Hely** /etc/security/pscexpert/dodv2/chowndodfiles **Megfelelési művelet** Biztosítja, hogy a megadott fájl tulajdonosa root vagy bin felhasználó legyen.

3. táblázat: DoD tulajdonjog követelmények (Folytatás)

Department of Defense STIG ellenőrzési pont azonosító	**Leírás**	**A parancsfájl helye, ahol a művelet meg van határozva, valamint a művelet eredménye, amely lehetővé teszi a megfelelést**
GEN003770	A services fájl csoportosan legyen birtokolva a bin, sys és system által.	**Hely** /etc/security/pscexpert/dodv2/chowndodfiles **Megfelelési művelet** Biztosítja, hogy a megadott fájl csoportosan legyen birtokolva a bin, sys és system által.
GEN003920	A hosts.lpd (vagy egyenértékű) fájl tulajdonosa root, bin, sys vagy lp legyen.	**Hely** /etc/security/pscexpert/dodv2/chowndodfiles **Megfelelési művelet** Biztosítja, hogy a megadott fájl tulajdonosa root, bin, sys vagy lp legyen.
GEN003930	A hosts.lpd (vagy egyenértékű) megfelelőt csoportosan birtokolja a bin, sys vagy system.	**Hely** /etc/security/pscexpert/dodv2/chowndodfiles **Megfelelési művelet** Biztosítja, hogy a megadott fájl csoportosan legyen birtokolva a bin, sys és system által.
GEN003960	A **traceroute** parancs tulajdonosának root felhasználónak kell lenni.	**Hely** /etc/security/pscexpert/dodv2/chowndodfiles **Megfelelési művelet** Biztosítja, hogy a parancs tulajdonosa root legyen.
GEN003980	A **traceroute** parancsot csoportosan birtokolja a sys, bin vagy system.	**Hely** /etc/security/pscexpert/dodv2/chowndodfiles **Megfelelési művelet** Biztosítja, hogy a parancsot csoportosan birtokolja a sys, bin vagy system.
GEN004360	Az alias fájl tulajdonosának root felhasználónak kell lenni.	**Hely** /etc/security/pscexpert/dodv2/chowndodfiles **Megfelelési művelet** Biztosítja, hogy a megadott fájl tulajdonosa root legyen.
GEN004370	Az aliases fájl csoportosan legyen birtokolva a sys, bin vagy system által.	**Hely** /etc/security/pscexpert/dodv2/chowndodfiles **Megfelelési művelet** Biztosítja, hogy a megadott fájlt csoportosan birtokolja a sys, bin vagy system.
GEN004400	A levelezési aliases fájlon keresztül futtatott fájlok tulajdonosának root felhasználónak kell lenni és olyan könyvtárban kell elhelyezkedniük, amelyet csak a root birtokol és csak a root számára írható.	**Hely** /etc/security/pscexpert/dodv2/chowndodfiles **Megfelelési művelet** Biztosítja, hogy a levelezési aliases fájlon keresztül futtatott fájlok tulajdonosa root felhasználó legyen és olyan könyvtárban helyezkedjenek el, amelyet csak a root birtokol és csak a root számára írható.
GEN004410	A levelezési aliases fájlon keresztül futtatott fájlok csoportosan legyenek birtokolva a root, bin, sys vagy más által. Ezen kívül olyan könyvtárban kell elhelyezkedniük, amelyeket csoportosan birtokol a root, bin, sys és mások.	**Hely** /etc/security/pscexpert/dodv2/chowndodfiles **Megfelelési művelet** Biztosítja, hogy a levelezési aliases fájlon keresztül futtatott fájlok csoportosan legyenek birtokolva a root, bin, sys vagy más által. Ezen kívül olyan könyvtárban kell elhelyezkedniük, amelyeket csoportosan birtokol a root, bin, sys és mások.
GEN004480	Az SMTP szolgáltatás naplófájljának tulajdonosa root felhasználó legyen.	**Hely** /etc/security/pscexpert/dodv2/chowndodfiles **Megfelelési művelet** Biztosítja, hogy a megadott fájl tulajdonosa root legyen.

3. táblázat: DoD tulajdonjog követelmények (Folytatás)

Department of Defense STIG ellenőrzési pont azonosító	**Leírás**	**A parancsfájl helye, ahol a művelet meg van határozva, valamint a művelet eredménye, amely lehetővé teszi a megfelelést**
GEN004920	Az ftpusers fájl tulajdonosának root felhasználónak kell lenni.	**Hely** /etc/security/pscexpert/dodv2/chowndodfiles **Megfelelési művelet** Biztosítja, hogy a megadott fájl tulajdonosa root legyen.
GEN004930	Az ftpusers fájl csoportosan legyen birtokolva a bin, sys és system által.	**Hely** /etc/security/pscexpert/dodv2/chowndodfiles **Megfelelési művelet** Biztosítja, hogy a megadott fájl csoportosan legyen birtokolva a bin, sys és system által.
GEN005360	Az snmpd.conf fájl tulajdonosának root felhasználónak kell lenni.	**Hely** /etc/security/pscexpert/dodv2/chowndodfiles **Megfelelési művelet** Biztosítja, hogy a megadott fájl tulajdonosa root legyen.
GEN005365	Az snmpd.conf fájl csoportosan legyen birtokolva a bin, sys és system által.	**Hely** /etc/security/pscexpert/dodv2/chowndodfiles **Megfelelési művelet** Biztosítja, hogy a megadott fájl csoportosan legyen birtokolva a bin, sys és system által.
GEN005400	Az /etc/syslog.conf fájl tulajdonosának root felhasználónak kell lenni.	**Hely** /etc/security/pscexpert/dodv2/chowndodfiles **Megfelelési művelet** Biztosítja, hogy a megadott fájl tulajdonosa root legyen.
GEN005420	Az /etc/syslog.conf fájl csoportosan legyen birtokolva a bin, sys és system által.	**Hely** /etc/security/pscexpert/dodv2/chowndodfiles **Megfelelési művelet** Biztosítja, hogy a megadott fájl csoportosan legyen birtokolva a bin, sys és system által.
GEN005610	A rendszer IP továbbítása az IPv6-hoz nem lehet engedélyezett, hacsak a rendszer nem IPv6 útválasztó.	**Hely** /etc/security/pscexpert/dodv2/chowndodfiles **Megfelelési művelet** Biztosítja, hogy az IP továbbítás az IPv6 protokollhoz ne legyen engedélyezett, hacsak a rendszer nem IPv6 útválasztóként van használatban.
GEN005740	Az NFS exportálás konfigurációs fájl tulajdonosának root felhasználónak kell lenni.	**Hely** /etc/security/pscexpert/dodv2/chowndodfiles **Megfelelési művelet** Biztosítja, hogy a megadott fájl tulajdonosa root legyen.
GEN005750	Az NFS exportálás konfigurációs fájl csoportosan legyen birtokolva a root, bin, sys vagy system által.	**Hely** /etc/security/pscexpert/dodv2/chowndodfiles **Megfelelési művelet** Biztosítja, hogy a megadott fájl csoportosan legyen birtokolva a root, bin, sys és system által.
GEN005800	Minden NFS-exportált rendszerfájl és rendszerkönyvtár tulajdonosának root felhasználónak kell lenni.	**Hely** /etc/security/pscexpert/dodv2/chowndodfiles **Megfelelési művelet** Biztosítja, hogy a megadott fájl tulajdonosa root legyen.

3. táblázat: DoD tulajdonjog követelmények (Folytatás)

Department of Defense STIG ellenőrzési pont azonosító	Leírás	A parancsfájl helye, ahol a művelet meg van határozva, valamint a művelet eredménye, amely lehetővé teszi a megfelelést
GEN005810	Minden NFS-exportált rendszerfájl és rendszerkönyvtár csoportosan legyen birtokolva a root, bin, sys vagy system által.	**Hely** /etc/security/pscexpert/dodv2/chowndodfiles **Megfelelési művelet** Biztosítja, hogy a megadott fájlokat és könyvtárakat a root, bin, sys vagy system csoportosan birtokolja.
GEN006100	Az /usr/lib/smb.conf fájl tulajdonosának root felhasználónak kell lenni.	**Hely** /etc/security/pscexpert/dodv2/chowndodfiles **Megfelelési művelet** Biztosítja, hogy a megadott fájl tulajdonosa root legyen.
GEN006120	Az /usr/lib/smb.conf fájl csoportosan legyen birtokolva a bin, sys és system által.	**Hely** /etc/security/pscexpert/dodv2/chowndodfiles **Megfelelési művelet** Biztosítja, hogy a megadott fájl csoportosan legyen birtokolva a bin, sys és system által.
GEN006160	A /var/private/smbpasswd fájl tulajdonosának root felhasználónak kell lenni.	**Hely** /etc/security/pscexpert/dodv2/chowndodfiles **Megfelelési művelet** Biztosítja, hogy a megadott fájl tulajdonosa root legyen.
GEN006180	A /var/private/smbpasswd fájl csoportosan legyen birtokolva a sys és system által.	**Hely** /etc/security/pscexpert/dodv2/chowndodfiles **Megfelelési művelet** Biztosítja, hogy a megadott fájlt csoportosan birtokolja a sys vagy system.
GEN006340	Az /etc/news könyvtárban található fájlok tulajdonosa root vagy a hírek legyen.	**Hely** /etc/security/pscexpert/dodv2/chowndodfiles **Megfelelési művelet** Biztosítja, hogy a megadott könyvtár tulajdonosa a root vagy a hírek legyen.
GEN006360	Az /etc/news könyvtárban található fájlokat csoportosan birtokolja a rendszer vagy a hírek.	**Hely** /etc/security/pscexpert/dodv2/chowndodfiles **Megfelelési művelet** Biztosítja, hogy a megadott fájlokat csoportosan birtokolja a rendszer vagy a hírek.
GEN008080	Ha a rendszer LDAP protokollt használ a hitelesítéshez vagy a fiókinformációkhoz, akkor az /etc/ldap.conf (vagy egyenértékű) fájl tulajdonosának root felhasználónak kell lenni.	**Hely** /etc/security/pscexpert/dodv2/chowndodfiles **Megfelelési művelet** Biztosítja, hogy a megadott fájl tulajdonosa root legyen.
GEN008100	Ha a rendszer LDAP protokollt használ a hitelesítéshez vagy a fiókinformációkhoz, akkor az /etc/ldap.conf (vagy egyenértékű) fájl csoportosan legyen birtokolva a security, bin, sys vagy system által.	**Hely** /etc/security/pscexpert/dodv2/chowndodfiles **Megfelelési művelet** Biztosítja, hogy a megadott fájl csoportosan legyen birtokolva a bin, sys és system által.
GEN008140	Ha a rendszer LDAP protokollt használ a hitelesítéshez vagy a fiókinformációkhoz, akkor a TLS tanúsítványhatóság fájl vagy könyvtár tulajdonosának root felhasználónak kell lenni.	**Hely** /etc/security/pscexpert/dodv2/chowndodfiles **Megfelelési művelet** Biztosítja, hogy a megadott fájl tulajdonosa root legyen.
GEN008160	Ha a rendszer LDAP protokollt használ a hitelesítéshez vagy a fiókinformációkhoz, akkor a TLS tanúsítványhatóság fájl vagy könyvtár csoportosan legyen birtokolva a root, bin, sys vagy system által.	**Hely** /etc/security/pscexpert/dodv2/chowndodfiles **Megfelelési művelet** Biztosítja, hogy a megadott fájl csoportosan legyen birtokolva a bin, sys és system által.

4. táblázat: Fájlengedélyek DoD szabványai

Department of Defense STIG ellenőrzési pont azonosító	**Leírás**	**A parancsfájl helye, ahol a művelet meg van határozva, valamint a művelet eredménye, amely lehetővé teszi a megfelelést**
AIX00100	Az /etc/netsvc.conf fájlon a 0644-es módnak vagy egy kevésbé megengedő módnak kell beállítva lenni.	**Hely** /etc/security/pscexpert/dodv2/fpmdodfiles **Megfelelési művelet** Biztosítja, hogy a fájl a megadott engedélymódra vagy annál kevésbé megengedő módra legyen beállítva.
AIX00340	Az /etc/ftpaccess.ctl fájlon a 0640-es módnak vagy egy kevésbé megengedő módnak kell beállítva lenni.	**Hely** /etc/security/pscexpert/dodv2/fpmdodfiles **Megfelelési művelet** Biztosítja, hogy a fájl a megadott engedélymódra vagy annál kevésbé megengedő módra legyen beállítva.
GEN000252	Az időszinkronizálási konfigurációs fájlon (például /etc/ntp.conf) a 0640-es módnak vagy egy kevésbé megengedő módnak kell beállítva lenni.	**Hely** /etc/security/pscexpert/dodv2/fpmdodfiles **Megfelelési művelet** Biztosítja, hogy a fájl a megadott engedélymódra vagy annál kevésbé megengedő módra legyen beállítva.
GEN000920	A root fiók saját könyvtárán (amely nem /) a 0700-ás módnak kell beállítva lenni.	**Hely** /etc/security/pscexpert/dodv2/fpmdodfiles **Megfelelési művelet** Biztosítja, hogy a könyvtár a megadott engedélymódra vagy annál kevésbé megengedő módra legyen beállítva.
GEN001140	A rendszerfájloknak és a könyvtáraknak eltérő hozzáférési engedélyekkel kell rendelkezni.	**Hely** /etc/security/pscexpert/dodv2/fpmdodfiles **Megfelelési művelet** Biztosítja, hogy a hozzáférési engedélyek konzisztensek legyenek.
GEN001180	Minden hálózati szolgáltatás démonfájlján a 0755-ös módnak vagy egy kevésbé megengedő módnak kell beállítva lenni.	**Hely** /etc/security/pscexpert/dodv2/fpmdodfiles **Megfelelési művelet** Biztosítja, hogy a fájlok a megadott engedélymódra vagy annál kevésbé megengedő módra legyenek beállítva.
GEN001200	Minden rendszer parancsfájlon a 0755-ös módnak vagy egy kevésbé megengedő módnak kell beállítva lenni.	**Hely** /etc/security/pscexpert/dodv2/fpmdodfiles **Megfelelési művelet** Biztosítja, hogy a fájlok a megadott engedélymódra vagy annál kevésbé megengedő módra legyenek beállítva.
GEN001260	A rendszer naplófájlokon a 0640-es módnak vagy egy kevésbé megengedő módnak kell beállítva lenni.	**Hely** /etc/security/pscexpert/dodv2/fpmdodfiles **Megfelelési művelet** Biztosítja, hogy a fájlok a megadott engedélymódra vagy annál kevésbé megengedő módra legyenek beállítva.
GEN001280	A kézi oldalfájlokon a 0644-es módnak vagy egy kevésbé megengedő módnak kell beállítva lenni.	**Hely** /etc/security/pscexpert/dodv2/fpmdodfiles **Megfelelési művelet** Biztosítja, hogy a fájlok a megadott engedélymódra vagy annál kevésbé megengedő módra legyenek beállítva.

4. táblázat: Fájlengedélyek DoD szabványai (Folytatás)

Department of Defense STIG ellenőrzési pont azonosító	Leírás	A parancsfájl helye, ahol a művelet meg van határozva, valamint a művelet eredménye, amely lehetővé teszi a megfelelést
GEN001300	A könyvtárfájlokon a 0755-ös módnak vagy egy kevésbé megengedő módnak kell beállítva lenni.	**Hely** /etc/security/pscexpert/dodv2/fpmdodfiles **Megfelelési művelet** Biztosítja, hogy a fájlok a megadott engedélymódra vagy annál kevésbé megengedő módra legyenek beállítva.
GEN001360	A NIS/NIS+/yp fájlokon a 0755-ös módnak vagy egy kevésbé megengedő módnak kell beállítva lenni.	**Hely** /etc/security/pscexpert/dodv2/fpmdodfiles **Megfelelési művelet** Biztosítja, hogy a fájlok a megadott engedélymódra vagy annál kevésbé megengedő módra legyenek beállítva.
GEN001364	Az /etc/resolv.conf fájlon a 0644-es módnak vagy egy kevésbé megengedő módnak kell beállítva lenni.	**Hely** /etc/security/pscexpert/dodv2/fpmdodfiles **Megfelelési művelet** Biztosítja, hogy a fájl a megadott engedélymódra vagy annál kevésbé megengedő módra legyen beállítva.
GEN001368	Az /etc/hosts fájlon a 0644-es módnak vagy egy kevésbé megengedő módnak kell beállítva lenni.	**Hely** /etc/security/pscexpert/dodv2/fpmdodfiles **Megfelelési művelet** Biztosítja, hogy a fájl a megadott engedélymódra vagy annál kevésbé megengedő módra legyen beállítva.
GEN001373	Az /etc/nsswitch.conf fájlon a 0644-es módnak vagy egy kevésbé megengedő módnak kell beállítva lenni.	**Hely** /etc/security/pscexpert/dodv2/fpmdodfiles **Megfelelési művelet** Biztosítja, hogy a fájl a megadott engedélymódra vagy annál kevésbé megengedő módra legyen beállítva.
GEN001380	Az /etc/passwd fájlon a 0644-es módnak vagy egy kevésbé megengedő módnak kell beállítva lenni.	**Hely** /etc/security/pscexpert/dodv2/fpmdodfiles **Megfelelési művelet** Biztosítja, hogy a fájl a megadott engedélymódra vagy annál kevésbé megengedő módra legyen beállítva.
GEN001393	Az /etc/group fájlon a 0644-es módnak vagy egy kevésbé megengedő módnak kell beállítva lenni.	**Hely** /etc/security/pscexpert/dodv2/fpmdodfiles **Megfelelési művelet** Biztosítja, hogy a fájl a megadott engedélymódra vagy annál kevésbé megengedő módra legyen beállítva.
GEN001420	Az /etc/security/passwd fájlon a 0400-ás módnak kell beállítva lenni.	**Hely** /etc/security/pscexpert/dodv2/fpmdodfiles **Megfelelési művelet** Biztosítja, hogy a fájl a megadott engedélymódra vagy annál kevésbé megengedő módra legyen beállítva.
GEN001480	Minden felhasználó saját könyvtárán a 0750-es vagy kevésbé megengedő módnak kell beállítva lenni.	**Hely** /etc/security/pscexpert/dodv2/fpmdodfiles **Megfelelési művelet** Biztosítja, hogy a fájl a megadott engedélymódra vagy annál kevésbé megengedő módra legyen beállítva.

4. táblázat: Fájlengedélyek DoD szabványai (Folytatás)

Department of Defense STIG ellenőrzési pont azonosító	**Leírás**	**A parancsfájl helye, ahol a művelet meg van határozva, valamint a művelet eredménye, amely lehetővé teszi a megfelelést**
GEN001560	A felhasználó saját könyvtárában tartalmazott összes fájlon és könyvtáron a 0750-es vagy egy kevésbé megengedő módnak kell beállítva lenni.	**Hely** /etc/security/pscexpert/dodv2/fpmdodfiles **Megfelelési művelet** Biztosítja, hogy a fájlok a megadott engedélymódra vagy annál kevésbé megengedő módra legyenek beállítva.
GEN001580	Minden futtatásvezérlő parancsfájlon a 0755-ös módnak vagy egy kevésbé megengedő módnak kell beállítva lenni.	**Hely** /etc/security/pscexpert/dodv2/fpmdodfiles **Megfelelési művelet** Biztosítja, hogy a fájlok a megadott engedélymódra vagy annál kevésbé megengedő módra legyenek beállítva.
GEN001640	A futtatásvezérlő parancsfájlok nem futtathatnak bárki számára írható programokat és parancsfájlokat.	**Hely** /etc/security/pscexpert/dodv2/fpmdodfiles **Megfelelési művelet** Programok ellenőrzése, mint például a cron, a bárki számára írható programokért és parancsfájlokért.
GEN001720	Minden globális inicializálási fájlon a 0644-es módnak vagy egy kevésbé megengedő módnak kell beállítva lenni.	**Hely** /etc/security/pscexpert/dodv2/fpmdodfiles **Megfelelési művelet** Biztosítja, hogy a fájlok a megadott engedélymódra vagy annál kevésbé megengedő módra legyenek beállítva.
GEN001800	Minden vázfájlon (például az /etc/skel fájljain) a 0644-es módnak vagy egy kevésbé megengedő módnak kell beállítva lenni.	**Hely** /etc/security/pscexpert/dodv2/fpmdodfiles **Megfelelési művelet** Biztosítja, hogy a fájlok a megadott engedélymódra vagy annál kevésbé megengedő módra legyenek beállítva.
GEN001880	Minden helyi inicializálási fájlon a 0740-es módnak vagy egy kevésbé megengedő módnak kell beállítva lenni.	**Hely** /etc/security/pscexpert/dodv2/fpmdodfiles **Megfelelési művelet** Biztosítja, hogy a fájlok a megadott engedélymódra vagy annál kevésbé megengedő módra legyenek beállítva.
GEN002220	Minden parancsértelmező fájlon a 0755-ös módnak vagy egy kevésbé megengedő módnak kell beállítva lenni.	**Hely** /etc/security/pscexpert/dodv2/fpmdodfiles **Megfelelési művelet** Biztosítja, hogy a fájlok a megadott engedélymódra vagy annál kevésbé megengedő módra legyenek beállítva.
GEN002320	Minden audioeszközön a 0660-as módnak vagy egy kevésbé megengedő módnak kell beállítva lenni.	**Hely** /etc/security/pscexpert/dodv2/fpmdodfiles **Megfelelési művelet** Biztosítja, hogy az audioeszközök a megadott engedélymódra vagy annál kevésbé megengedő módra legyenek beállítva,
GEN002560	A rendszer és a felhasználó alapértelmezett **umask** értékének 077-es értéknek kell lenni.	**Hely** /etc/security/pscexpert/dodv2/fpmdodfiles **Megfelelési művelet** Biztosítja, hogy a megadott beállítások értéke *077* legyen.

4. táblázat: Fájlengedélyek DoD szabványai (Folytatás)

Department of Defense STIG ellenőrzési pont azonosító	Leírás	A parancsfájl helye, ahol a művelet meg van határozva, valamint a művelet eredménye, amely lehetővé teszi a megfelelést
GEN002700	A rendszer megfigyelési naplóin a 0640-es módnak vagy egy kevésbé megengedő módnak kell beállítva lenni.	**Hely** /etc/security/pscexpert/dodv2/fpmdodfiles **Megfelelési művelet** Biztosítja, hogy a fájlok a megadott engedélymódra vagy annál kevésbé megengedő módra legyenek beállítva.
GEN002717	A rendszerfigyelő eszköz végrehajtható fájljain a 0750-es módnak vagy egy kevésbé megengedő módnak kell beállítva lenni.	**Hely** /etc/security/pscexpert/dodv2/fpmdodfiles **Megfelelési művelet** Biztosítja, hogy a fájlok a megadott engedélymódra vagy annál kevésbé megengedő módra legyenek beállítva.
GEN002980	A cron.allow fájlon a 0600-ás módnak vagy egy kevésbé megengedő módnak kell beállítva lenni.	**Hely** /etc/security/pscexpert/dodv2/fpmdodfiles **Megfelelési művelet** Biztosítja, hogy a fájl a megadott engedélymódra vagy annál kevésbé megengedő módra legyen beállítva.
GEN003080	A crontab fájlokon a 0600-ás módnak vagy egy kevésbé megengedő módnak kell beállítva lenni.	**Hely** /etc/security/pscexpert/dodv2/fpmdodfiles **Megfelelési művelet** Biztosítja, hogy a fájlok a megadott engedélymódra vagy annál kevésbé megengedő módra legyenek beállítva.
GEN003090	A Crontab fájlok nem rendelkezhetnek kiterjesztett hozzáférés-felügyeleti listákkal (ACL).	**Hely** /etc/security/pscexpert/dodv2/fpmdodfiles **Megfelelési művelet** Biztosítja, hogy a megadott fájlok ne rendelkezzenek kiterjesztett ACL listákkal.
GEN003100	A cron és a crontab könyvtáron a 0755-ös módnak vagy egy kevésbé megengedő módnak kell beállítva lenni.	**Hely** /etc/security/pscexpert/dodv2/fpmdodfiles **Megfelelési művelet** Biztosítja, hogy a megadott könyvtárak a megadott engedélymódra vagy annál kevésbé megengedő módra legyenek beállítva.
GEN003180	A cronlog fájlon a 0600-ás módnak vagy egy kevésbé megengedő módnak kell beállítva lenni.	**Hely** /etc/security/pscexpert/dodv2/fpmdodfiles **Megfelelési művelet** Biztosítja, hogy a fájl a megadott engedélymódra vagy annál kevésbé megengedő módra legyen beállítva.
GEN003200	A cron.deny fájlon a 0600-ás módnak vagy egy kevésbé megengedő módnak kell beállítva lenni.	**Hely** /etc/security/pscexpert/dodv2/fpmdodfiles **Megfelelési művelet** Biztosítja, hogy a fájl a megadott engedélymódra vagy annál kevésbé megengedő módra legyen beállítva.
GEN003252	Az at.deny fájlon a 0640-es módnak vagy egy kevésbé megengedő módnak kell beállítva lenni.	**Hely** /etc/security/pscexpert/dodv2/fpmdodfiles **Megfelelési művelet** Biztosítja, hogy a fájl a megadott engedélymódra vagy annál kevésbé megengedő módra legyen beállítva.

4. táblázat: Fájlengedélyek DoD szabványai (Folytatás)

Department of Defense STIG ellenőrzési pont azonosító	Leírás	A parancsfájl helye, ahol a művelet meg van határozva, valamint a művelet eredménye, amely lehetővé teszi a megfelelést
GEN003340	Az at.allow fájlon a 0600-ás módnak vagy egy kevésbé megengedő módnak kell beállítva lenni.	**Hely** /etc/security/pscexpert/dodv2/fpmdodfiles **Megfelelési művelet** Biztosítja, hogy a fájl a megadott engedélymódra vagy annál kevésbé megengedő módra legyen beállítva.
GEN003400	Az at könyvtáron a 0755-ös módnak vagy egy kevésbé megengedő módnak kell beállítva lenni.	**Hely** /etc/security/pscexpert/dodv2/fpmdodfiles **Megfelelési művelet** Biztosítja, hogy a könyvtár a megadott engedélymódra vagy annál kevésbé megengedő módra legyen beállítva.
GEN003440	Az At feladatok nem állíthatják be az **umask** paramétert a 077-nél kevésbé szigorú értékre.	**Hely** /etc/security/pscexpert/dodv2/fpmdodfiles **Megfelelési művelet** Biztosítja, hogy a paraméter a megadott engedélymódra vagy annál kevésbé megengedő módra legyen beállítva.
GEN003740	Az inetd.conf és a xinetd.conf fájlon a 0440-es módnak vagy egy kevésbé megengedő módnak kell beállítva lenni.	**Hely** /etc/security/pscexpert/dodv2/fpmdodfiles **Megfelelési művelet** Biztosítja, hogy a fájlok a megadott engedélymódra vagy annál kevésbé megengedő módra legyenek beállítva.
GEN003780	A services fájlon a 0444-es módnak vagy egy kevésbé megengedő módnak kell beállítva lenni.	**Hely** /etc/security/pscexpert/dodv2/fpmdodfiles **Megfelelési művelet** Biztosítja, hogy a fájl a megadott engedélymódra vagy annál kevésbé megengedő módra legyen beállítva.
GEN003940	A hosts.lpd fájlon (vagy egyenértékű) a 0644-es módnak vagy egy kevésbé megengedő módnak kell beállítva lenni.	**Hely** /etc/security/pscexpert/dodv2/fpmdodfiles **Megfelelési művelet** Biztosítja, hogy a fájl a megadott engedélymódra vagy annál kevésbé megengedő módra legyen beállítva.
GEN004000	A traceroute fájlon a 0700-ás módnak vagy egy kevésbé megengedő módnak kell beállítva lenni.	**Hely** /etc/security/pscexpert/dodv2/fpmdodfiles **Megfelelési művelet** Biztosítja, hogy a fájl a megadott engedélymódra vagy annál kevésbé megengedő módra legyen beállítva.
GEN004380	Az alias fájlon a 0644-es módnak vagy egy kevésbé megengedő módnak kell beállítva lenni.	**Hely** /etc/security/pscexpert/dodv2/fpmdodfiles **Megfelelési művelet** Biztosítja, hogy a fájl a megadott engedélymódra vagy annál kevésbé megengedő módra legyen beállítva.
GEN004420	A levelezési aliases fájlon keresztül futtatott fájlokon a 0755-ös módnak vagy egy kevésbé megengedő módnak kell beállítva lenni.	**Hely** /etc/security/pscexpert/dodv2/fpmdodfiles **Megfelelési művelet** Biztosítja, hogy a fájlok a megadott engedélymódra vagy annál kevésbé megengedő módra legyenek beállítva.

4. táblázat: Fájlengedélyek DoD szabványai (Folytatás)

Department of Defense STIG ellenőrzési pont azonosító	**Leírás**	**A parancsfájl helye, ahol a művelet meg van határozva, valamint a művelet eredménye, amely lehetővé teszi a megfelelést**
GEN004500	A SMTP szolgáltatás naplófájlján a 0644-es módnak vagy egy kevésbé megengedő módnak kell beállítva lenni.	**Hely** /etc/security/pscexpert/dodv2/fpmdodfiles **Megfelelési művelet** Biztosítja, hogy a fájl a megadott engedélymódra vagy annál kevésbé megengedő módra legyen beállítva.
GEN004940	Az ftpusers fájlon a 0640-es módnak vagy egy kevésbé megengedő módnak kell beállítva lenni.	**Hely** /etc/security/pscexpert/dodv2/fpmdodfiles **Megfelelési művelet** Biztosítja, hogy a fájl a megadott engedélymódra vagy annál kevésbé megengedő módra legyen beállítva.
GEN005040	Minden FTP felhasználónak rendelkezni kell egy alapértelmezett 077-es **umask** beállítással.	**Hely** /etc/security/pscexpert/dodv2/fpmdodfiles **Megfelelési művelet** Biztosítja, hogy a beállítás helyes legyen.
GEN005100	A TFTP démonon a 0755-ös módnak vagy egy kevésbé megengedő módnak kell beállítva lenni.	**Hely** /etc/security/pscexpert/dodv2/fpmdodfiles **Megfelelési művelet** Biztosítja, hogy a démon a megadott engedélymódra vagy annál kevésbé megengedő módra legyen beállítva.
GEN005180	Minden .Xauthority fájlon a 0600-ás módnak vagy egy kevésbé megengedő módnak kell beállítva lenni.	**Hely** /etc/security/pscexpert/dodv2/fpmdodfiles **Megfelelési művelet** Biztosítja, hogy a fájlok a megadott engedélymódra vagy annál kevésbé megengedő módra legyenek beállítva.
GEN005320	Az snmpd.conf fájlon a 0600-ás módnak vagy egy kevésbé megengedő módnak kell beállítva lenni.	**Hely** /etc/security/pscexpert/dodv2/fpmdodfiles **Megfelelési művelet** Biztosítja, hogy a fájl a megadott engedélymódra vagy annál kevésbé megengedő módra legyen beállítva.
GEN005340	A Management Information Base (MIB) fájlokon a 0640-es módnak vagy egy kevésbé megengedő módnak kell beállítva lenni.	**Hely** /etc/security/pscexpert/dodv2/fpmdodfiles **Megfelelési művelet** Biztosítja, hogy a fájlok a megadott engedélymódra vagy annál kevésbé megengedő módra legyenek beállítva.
GEN005390	Az /etc/syslog.conf fájlon a 0640-es módnak vagy egy kevésbé megengedő módnak kell beállítva lenni.	**Hely** /etc/security/pscexpert/dodv2/fpmdodfiles **Megfelelési művelet** Biztosítja, hogy a fájl a megadott engedélymódra vagy annál kevésbé megengedő módra legyen beállítva.
GEN005522	A SSH nyilvános hoszt kulcsfájlokon a 0644-es módnak vagy egy kevésbé megengedő módnak kell beállítva lenni.	**Hely** /etc/security/pscexpert/dodv2/fpmdodfiles **Megfelelési művelet** Biztosítja, hogy a fájlok a megadott engedélymódra vagy annál kevésbé megengedő módra legyenek beállítva.

4. táblázat: Fájlengedélyek DoD szabványai (Folytatás)

Department of Defense STIG ellenőrzési pont azonosító	Leírás	A parancsfájl helye, ahol a művelet meg van határozva, valamint a művelet eredménye, amely lehetővé teszi a megfelelést
GEN005523	A SSH privát hoszt kulcsfájlokon a 0600-ás módnak vagy egy kevésbé megengedő módnak kell beállítva lenni.	**Hely** /etc/security/pscexpert/dodv2/fpmdodfiles **Megfelelési művelet** Biztosítja, hogy a fájlok a megadott engedélymódra vagy annál kevésbé megengedő módra legyenek beállítva.
GEN006140	Az /usr/lib/smb.conf fájlon a 0644-es módnak vagy egy kevésbé megengedő módnak kell beállítva lenni.	**Hely** /etc/security/pscexpert/dodv2/fpmdodfiles **Megfelelési művelet** Biztosítja, hogy a fájl a megadott engedélymódra vagy annál kevésbé megengedő módra legyen beállítva.
GEN006200	A /var/private/smbpasswd fájlon a 0600-ás módnak vagy egy kevésbé megengedő módnak kell beállítva lenni.	**Hely** /etc/security/pscexpert/dodv2/fpmdodfiles **Megfelelési művelet** Biztosítja, hogy a fájl a megadott engedélymódra vagy annál kevésbé megengedő módra legyen beállítva.
GEN006260	Az /etc/news/hosts.nntp fájlon (vagy egyenértékű) a 0600-ás módnak vagy egy kevésbé megengedő módnak kell beállítva lenni.	**Hely** /etc/security/pscexpert/dodv2/fpmdodfiles **Megfelelési művelet** Biztosítja, hogy a fájl a megadott engedélymódra vagy annál kevésbé megengedő módra legyen beállítva.
GEN006280	Az /etc/news/hosts.nntp.nolimit fájlon (vagy egyenértékű) a 0600-ás módnak vagy egy kevésbé megengedő módnak kell beállítva lenni.	**Hely** /etc/security/pscexpert/dodv2/fpmdodfiles **Megfelelési művelet** Biztosítja, hogy a fájl a megadott engedélymódra vagy annál kevésbé megengedő módra legyen beállítva.
GEN006300	Az /etc/news/nnrp.access fájlon (vagy egyenértékű) a 0600-ás módnak vagy egy kevésbé megengedő módnak kell beállítva lenni.	**Hely** /etc/security/pscexpert/dodv2/fpmdodfiles **Megfelelési művelet** Biztosítja, hogy a fájl a megadott engedélymódra vagy annál kevésbé megengedő módra legyen beállítva.
GEN006320	Az /etc/news/passwd.nntp fájlon (vagy egyenértékű) a 0600-ás módnak vagy egy kevésbé megengedő módnak kell beállítva lenni.	**Hely** /etc/security/pscexpert/dodv2/fpmdodfiles **Megfelelési művelet** Biztosítja, hogy a fájl a megadott engedélymódra vagy annál kevésbé megengedő módra legyen beállítva.
GEN008060	Ha a rendszer LDAP protokollt használ a hitelesítéshez vagy a fiókinformációkhoz, akkor az /etc/ldap.conf (vagy egyenértékű) fájlon a 0644-es módnak vagy egy kevésbé megengedő módnak kell beállítva lenni.	**Hely** /etc/security/pscexpert/dodv2/fpmdodfiles **Megfelelési művelet** Biztosítja, hogy a fájl a megadott engedélymódra vagy annál kevésbé megengedő módra legyen beállítva.
GEN008180	Ha a rendszer LDAP protokollt használ a hitelesítéshez vagy a fiókinformációkhoz, akkor a TLS tanúsítványhatóság fájlon, könyvtáron vagy mindkettőn a 0644-es módnak (könyvtárak esetében a 0755-ös módnak) vagy egy kevésbé megengedő módnak kell beállítva lenni.	**Hely** /etc/security/pscexpert/dodv2/fpmdodfiles **Megfelelési művelet** Biztosítja, hogy a megadott fájl, könyvtár vagy mindkettő a megadott engedélymódra vagy egy kevésbé megengedő módra legyen beállítva.

5. táblázat: DoD hozzáférés-felügyeleti lista (ACL) követelményei

Department of Defense STIG ellenőrzési pont azonosító	**Leírás**	**A parancsfájl helye, ahol a művelet meg van határozva, valamint a művelet eredménye, amely lehetővé teszi a megfelelést**
AIX00110	Az /etc/netsvc.conf fájl nem rendelkezhet kiterjesztett hozzáférés-felügyeleti listával (ACL).	**Hely** /etc/security/pscexpert/dodv2/acldodfiles **Megfelelési művelet** Letiltja a megadott kiterjesztett ACL-t. **Megjegyzés:** Ez a beállítás nem módosul automatikusan, ha az irányelv visszaállításra kerül az AIX alapértelmezett irányelvre, a DoDv2_to_ használatával az AIXDefault.xml fájlhoz. Ezt a beállítást kézzel kell módosítani.
AIX00350	Az /etc/ftpaccess.ctl fájl nem rendelkezhet kiterjesztett hozzáférés-felügyeleti listával (ACL).	**Hely** /etc/security/pscexpert/dodv2/acldodfiles **Megfelelési művelet** Letiltja a megadott kiterjesztett ACL-t. **Megjegyzés:** Ez a beállítás nem módosul automatikusan, ha az irányelv visszaállításra kerül az AIX alapértelmezett irányelvre, a DoDv2_to_ használatával az AIXDefault.xml fájlhoz. Ezt a beállítást kézzel kell módosítani.
GEN000253	Az időszinkronizálási konfigurációs fájl (például: /etc/ntp.conf) nem rendelkezhet kiterjesztett hozzáférés-felügyeleti listával (ACL).	**Hely** /etc/security/pscexpert/dodv2/acldodfiles **Megfelelési művelet** Letiltja a megadott kiterjesztett ACL-t. **Megjegyzés:** Ez a beállítás nem módosul automatikusan, ha az irányelv visszaállításra kerül az AIX alapértelmezett irányelvre, a DoDv2_to_ használatával az AIXDefault.xml fájlhoz. Ezt a beállítást kézzel kell módosítani.
GEN000930	A root fiók saját könyvtára nem rendelkezhet kiterjesztett hozzáférés-felügyeleti listával (ACL).	**Hely** /etc/security/pscexpert/dodv2/acldodfiles **Megfelelési művelet** Letiltja a megadott kiterjesztett ACL-t. **Megjegyzés:** Ez a beállítás nem módosul automatikusan, ha az irányelv visszaállításra kerül az AIX alapértelmezett irányelvre, a DoDv2_to_ használatával az AIXDefault.xml fájlhoz. Ezt a beállítást kézzel kell módosítani.
GEN001190	Egy hálózati szolgáltatás démon fájl sem rendelkezhet kiterjesztett hozzáférés-felügyeleti listával (ACL).	**Hely** /etc/security/pscexpert/dodv2/acldodfiles **Megfelelési művelet** Letiltja a megadott kiterjesztett ACL-t. **Megjegyzés:** Ez a beállítás nem módosul automatikusan, ha az irányelv visszaállításra kerül az AIX alapértelmezett irányelvre, a DoDv2_to_ használatával az AIXDefault.xml fájlhoz. Ezt a beállítást kézzel kell módosítani.
GEN001210	Egy rendszer parancsfájl sem rendelkezhet kiterjesztett hozzáférés-felügyeleti listával (ACL).	**Hely** /etc/security/pscexpert/dodv2/acldodfiles **Megfelelési művelet** Letiltja a megadott kiterjesztett ACL-t. **Megjegyzés:** Ez a beállítás nem módosul automatikusan, ha az irányelv visszaállításra kerül az AIX alapértelmezett irányelvre, a DoDv2_to_ használatával az AIXDefault.xml fájlhoz. Ezt a beállítást kézzel kell módosítani.

5. táblázat: DoD hozzáférés-felügyeleti lista (ACL) követelményei (Folytatás)

Department of Defense STIG ellenőrzési pont azonosító	**Leírás**	**A parancsfájl helye, ahol a művelet meg van határozva, valamint a művelet eredménye, amely lehetővé teszi a megfelelést**
GEN001270	A rendszer naplófájljai nem rendelkezhetnek kiterjesztett hozzáférés-felügyeleti listával (ACL) kivéve, ha a hitelesített szoftver támogatásához szükségesek.	**Hely** /etc/security/pscexpert/dodv2/acldodfiles **Megfelelési művelet** Letiltja a megadott kiterjesztett ACL-t. **Megjegyzés:** Ez a beállítás nem módosul automatikusan, ha az irányelv visszaállításra kerül az AIX alapértelmezett irányelvre, a DoDv2_to_ használatával az AIXDefault.xml fájlhoz. Ezt a beállítást kézzel kell módosítani.
GEN001310	Egy könyvtárfájl sem rendelkezhet kiterjesztett hozzáférés-felügyeleti listával (ACL).	**Hely** /etc/security/pscexpert/dodv2/acldodfiles **Megfelelési művelet** Letiltja a megadott kiterjesztett ACL-t. **Megjegyzés:** Ez a beállítás nem módosul automatikusan, ha az irányelv visszaállításra kerül az AIX alapértelmezett irányelvre, a DoDv2_to_ használatával az AIXDefault.xml fájlhoz. Ezt a beállítást kézzel kell módosítani.
GEN001361	A NIS/NIS+/yp parancsfájlok nem rendelkezhetnek kiterjesztett hozzáférés-felügyeleti listával (ACL).	**Hely** /etc/security/pscexpert/dodv2/acldodfiles **Megfelelési művelet** Letiltja a megadott kiterjesztett ACL-t. **Megjegyzés:** Ez a beállítás nem módosul automatikusan, ha az irányelv visszaállításra kerül az AIX alapértelmezett irányelvre, a DoDv2_to_ használatával az AIXDefault.xml fájlhoz. Ezt a beállítást kézzel kell módosítani.
GEN001365	Az /etc/resolv.conf fájl nem rendelkezhet kiterjesztett hozzáférés-felügyeleti listával (ACL).	**Hely** /etc/security/pscexpert/dodv2/acldodfiles **Megfelelési művelet** Letiltja a megadott kiterjesztett ACL-t. **Megjegyzés:** Ez a beállítás nem módosul automatikusan, ha az irányelv visszaállításra kerül az AIX alapértelmezett irányelvre, a DoDv2_to_ használatával az AIXDefault.xml fájlhoz. Ezt a beállítást kézzel kell módosítani.
GEN001369	Az /etc/hosts fájl nem rendelkezhet kiterjesztett hozzáférés-felügyeleti listával (ACL).	**Hely** /etc/security/pscexpert/dodv2/acldodfiles **Megfelelési művelet** Letiltja a megadott kiterjesztett ACL-t. **Megjegyzés:** Ez a beállítás nem módosul automatikusan, ha az irányelv visszaállításra kerül az AIX alapértelmezett irányelvre, a DoDv2_to_ használatával az AIXDefault.xml fájlhoz. Ezt a beállítást kézzel kell módosítani.
GEN001374	Az /etc/nsswitch.conf fájl nem rendelkezhet kiterjesztett hozzáférés-felügyeleti listával (ACL).	**Hely** /etc/security/pscexpert/dodv2/acldodfiles **Megfelelési művelet** Letiltja a megadott kiterjesztett ACL-t. **Megjegyzés:** Ez a beállítás nem módosul automatikusan, ha az irányelv visszaállításra kerül az AIX alapértelmezett irányelvre, a DoDv2_to_ használatával az AIXDefault.xml fájlhoz. Ezt a beállítást kézzel kell módosítani.

5. táblázat: DoD hozzáférés-felügyeleti lista (ACL) követelményei (Folytatás)

Department of Defense STIG ellenőrzési pont azonosító	**Leírás**	**A parancsfájl helye, ahol a művelet meg van határozva, valamint a művelet eredménye, amely lehetővé teszi a megfelelést**
GEN001390	Az /etc/passwd fájl nem rendelkezhet kiterjesztett hozzáférés-felügyeleti listával (ACL).	**Hely** /etc/security/pscexpert/dodv2/acldodfiles **Megfelelési művelet** Letiltja a megadott kiterjesztett ACL-t. **Megjegyzés:** Ez a beállítás nem módosul automatikusan, ha az irányelv visszaállításra kerül az AIX alapértelmezett irányelvre, a DoDv2_to_ használatával az AIXDefault.xml fájlhoz. Ezt a beállítást kézzel kell módosítani.
GEN001394	Az /etc/group fájl nem rendelkezhet kiterjesztett hozzáférés-felügyeleti listával (ACL).	**Hely** /etc/security/pscexpert/dodv2/acldodfiles **Megfelelési művelet** Letiltja a megadott kiterjesztett ACL-t. **Megjegyzés:** Ez a beállítás nem módosul automatikusan, ha az irányelv visszaállításra kerül az AIX alapértelmezett irányelvre, a DoDv2_to_ használatával az AIXDefault.xml fájlhoz. Ezt a beállítást kézzel kell módosítani.
GEN001430	Az /etc/security/passwd fájl nem rendelkezhet kiterjesztett hozzáférés-felügyeleti listával (ACL).	**Hely** /etc/security/pscexpert/dodv2/acldodfiles **Megfelelési művelet** Letiltja a megadott kiterjesztett ACL-t. **Megjegyzés:** Ez a beállítás nem módosul automatikusan, ha az irányelv visszaállításra kerül az AIX alapértelmezett irányelvre, a DoDv2_to_ használatával az AIXDefault.xml fájlhoz. Ezt a beállítást kézzel kell módosítani.
GEN001570	A felhasználói saját könyvtárakban tartalmazott fájlok és könyvtárak nem rendelkezhetnek kiterjesztett hozzáférés-felügyeleti listával (ACL).	**Hely** /etc/security/pscexpert/dodv2/acldodfiles **Megfelelési művelet** Letiltja a megadott kiterjesztett ACL-t. **Megjegyzés:** Ez a beállítás nem módosul automatikusan, ha az irányelv visszaállításra kerül az AIX alapértelmezett irányelvre, a DoDv2_to_ használatával az AIXDefault.xml fájlhoz. Ezt a beállítást kézzel kell módosítani.
GEN001590	A futtatásvezérlő parancsfájlok nem rendelkezhetnek kiterjesztett hozzáférés-felügyeleti listával (ACL).	**Hely** /etc/security/pscexpert/dodv2/acldodfiles **Megfelelési művelet** Letiltja a megadott kiterjesztett ACL-t. **Megjegyzés:** Ez a beállítás nem módosul automatikusan, ha az irányelv visszaállításra kerül az AIX alapértelmezett irányelvre, a DoDv2_to_ használatával az AIXDefault.xml fájlhoz. Ezt a beállítást kézzel kell módosítani.
GEN001730	A globális inicializálási fájlok nem rendelkezhetnek kiterjesztett hozzáférés-felügyeleti listával (ACL).	**Hely** /etc/security/pscexpert/dodv2/acldodfiles **Megfelelési művelet** Letiltja a megadott kiterjesztett ACL-t. **Megjegyzés:** Ez a beállítás nem módosul automatikusan, ha az irányelv visszaállításra kerül az AIX alapértelmezett irányelvre, a DoDv2_to_ használatával az AIXDefault.xml fájlhoz. Ezt a beállítást kézzel kell módosítani.

5. táblázat: DoD hozzáférés-felügyeleti lista (ACL) követelményei (Folytatás)

Department of Defense STIG ellenőrzési pont azonosító	Leírás	A parancsfájl helye, ahol a művelet meg van határozva, valamint a művelet eredménye, amely lehetővé teszi a megfelelést
GEN001810	A vázfájlok nem rendelkezhetnek kiterjesztett hozzáférés-felügyeleti listával (ACL).	**Hely** /etc/security/pscexpert/dodv2/acldodfiles **Megfelelési művelet** Letiltja a megadott kiterjesztett ACL-t. **Megjegyzés:** Ez a beállítás nem módosul automatikusan, ha az irányelv visszaállításra kerül az AIX alapértelmezett irányelvre, a DoDv2_to_ használatával az AIXDefault.xml fájlhoz. Ezt a beállítást kézzel kell módosítani.
GEN001890	A helyi inicializálási fájlok nem rendelkezhetnek kiterjesztett hozzáférés-felügyeleti listával (ACL).	**Hely** /etc/security/pscexpert/dodv2/acldodfiles **Megfelelési művelet** Letiltja a megadott kiterjesztett ACL-t. **Megjegyzés:** Ez a beállítás nem módosul automatikusan, ha az irányelv visszaállításra kerül az AIX alapértelmezett irányelvre, a DoDv2_to_ használatával az AIXDefault.xml fájlhoz. Ezt a beállítást kézzel kell módosítani.
GEN002230	A parancsértelmező fájlok nem rendelkezhetnek kiterjesztett hozzáférés-felügyeleti listával (ACL).	**Hely** /etc/security/pscexpert/dodv2/acldodfiles **Megfelelési művelet** Letiltja a megadott kiterjesztett ACL-t. **Megjegyzés:** Ez a beállítás nem módosul automatikusan, ha az irányelv visszaállításra kerül az AIX alapértelmezett irányelvre, a DoDv2_to_ használatával az AIXDefault.xml fájlhoz. Ezt a beállítást kézzel kell módosítani.
GEN002330	Az audioeszközök nem rendelkezhetnek kiterjesztett hozzáférés-felügyeleti listával (ACL).	**Hely** /etc/security/pscexpert/dodv2/acldodfiles **Megfelelési művelet** Letiltja a megadott kiterjesztett ACL-t. **Megjegyzés:** Ez a beállítás nem módosul automatikusan, ha az irányelv visszaállításra kerül az AIX alapértelmezett irányelvre, a DoDv2_to_ használatával az AIXDefault.xml fájlhoz. Ezt a beállítást kézzel kell módosítani.
GEN002710	A rendszerfigyelő fájlok nem rendelkezhetnek kiterjesztett hozzáférés-felügyeleti listával (ACL).	**Hely** /etc/security/pscexpert/dodv2/acldodfiles **Megfelelési művelet** Letiltja a megadott kiterjesztett ACL-t. **Megjegyzés:** Ez a beállítás nem módosul automatikusan, ha az irányelv visszaállításra kerül az AIX alapértelmezett irányelvre, a DoDv2_to_ használatával az AIXDefault.xml fájlhoz. Ezt a beállítást kézzel kell módosítani.
GEN002990	A kiterjesztett ACL-eket le kell tiltani a cron.allow és a cron.deny fájlhoz.	**Hely** /etc/security/pscexpert/dodv2/acldodfiles **Megfelelési művelet** Letiltja a megadott kiterjesztett ACL-t. **Megjegyzés:** Ez a beállítás nem módosul automatikusan, ha az irányelv visszaállításra kerül az AIX alapértelmezett irányelvre, a DoDv2_to_ használatával az AIXDefault.xml fájlhoz. Ezt a beállítást kézzel kell módosítani.

5. táblázat: DoD hozzáférés-felügyeleti lista (ACL) követelményei (Folytatás)

Department of Defense STIG ellenőrzési pont azonosító	**Leírás**	**A parancsfájl helye, ahol a művelet meg van határozva, valamint a művelet eredménye, amely lehetővé teszi a megfelelést**
GEN003090	A crontab fájlok nem rendelkezhetnek kiterjesztett hozzáférés-felügyeleti listával (ACL).	**Hely** /etc/security/pscexpert/dodv2/acldodfiles **Megfelelési művelet** Letiltja a megadott kiterjesztett ACL-t. **Megjegyzés:** Ez a beállítás nem módosul automatikusan, ha az irányelv visszaállításra kerül az AIX alapértelmezett irányelvre, a DoDv2_to_ használatával az AIXDefault.xml fájlhoz. Ezt a beállítást kézzel kell módosítani.
GEN003110	A cron és a crontab könyvtárak nem rendelkezhetnek kiterjesztett hozzáférés-felügyeleti listával (ACL).	**Hely** /etc/security/pscexpert/dodv2/acldodfiles **Megfelelési művelet** Letiltja a megadott kiterjesztett ACL-t. **Megjegyzés:** Ez a beállítás nem módosul automatikusan, ha az irányelv visszaállításra kerül az AIX alapértelmezett irányelvre, a DoDv2_to_ használatával az AIXDefault.xml fájlhoz. Ezt a beállítást kézzel kell módosítani.
GEN003190	A cron naplófájlok nem rendelkezhetnek kiterjesztett hozzáférés-felügyeleti listával (ACL).	**Hely** /etc/security/pscexpert/dodv2/acldodfiles **Megfelelési művelet** Letiltja a megadott kiterjesztett ACL-t. **Megjegyzés:** Ez a beállítás nem módosul automatikusan, ha az irányelv visszaállításra kerül az AIX alapértelmezett irányelvre, a DoDv2_to_ használatával az AIXDefault.xml fájlhoz. Ezt a beállítást kézzel kell módosítani.
GEN003210	A cron.deny fájl nem rendelkezhet kiterjesztett hozzáférés-felügyeleti listával (ACL).	**Hely** /etc/security/pscexpert/dodv2/acldodfiles **Megfelelési művelet** Letiltja a megadott kiterjesztett ACL-t. **Megjegyzés:** Ez a beállítás nem módosul automatikusan, ha az irányelv visszaállításra kerül az AIX alapértelmezett irányelvre, a DoDv2_to_ használatával az AIXDefault.xml fájlhoz. Ezt a beállítást kézzel kell módosítani.
GEN003245	Az at.allow fájl nem rendelkezhet kiterjesztett hozzáférés-felügyeleti listával (ACL).	**Hely** /etc/security/pscexpert/dodv2/acldodfiles **Megfelelési művelet** Letiltja a megadott kiterjesztett ACL-t. **Megjegyzés:** Ez a beállítás nem módosul automatikusan, ha az irányelv visszaállításra kerül az AIX alapértelmezett irányelvre, a DoDv2_to_ használatával az AIXDefault.xml fájlhoz. Ezt a beállítást kézzel kell módosítani.
GEN003255	Az at.deny fájl nem rendelkezhet kiterjesztett hozzáférés-felügyeleti listával (ACL).	**Hely** /etc/security/pscexpert/dodv2/acldodfiles **Megfelelési művelet** Letiltja a megadott kiterjesztett ACL-t. **Megjegyzés:** Ez a beállítás nem módosul automatikusan, ha az irányelv visszaállításra kerül az AIX alapértelmezett irányelvre, a DoDv2_to_ használatával az AIXDefault.xml fájlhoz. Ezt a beállítást kézzel kell módosítani.

5. táblázat: DoD hozzáférés-felügyeleti lista (ACL) követelményei (Folytatás)

Department of Defense STIG ellenőrzési pont azonosító	**Leírás**	**A parancsfájl helye, ahol a művelet meg van határozva, valamint a művelet eredménye, amely lehetővé teszi a megfelelést**
GEN003410	Az at könyvtár nem rendelkezhet kiterjesztett hozzáférés-felügyeleti listával (ACL).	**Hely** /etc/security/pscexpert/dodv2/acldodfiles **Megfelelési művelet** Letiltja a megadott kiterjesztett ACL-t. **Megjegyzés:** Ez a beállítás nem módosul automatikusan, ha az irányelv visszaállításra kerül az AIX alapértelmezett irányelvre, a DoDv2_to_ használatával az AIXDefault.xml fájlhoz. Ezt a beállítást kézzel kell módosítani.
GEN003745	Az inetd.conf és a xinetd.conf fájl nem rendelkezhet kiterjesztett hozzáférés-felügyeleti listával (ACL).	**Hely** /etc/security/pscexpert/dodv2/acldodfiles **Megfelelési művelet** Letiltja a megadott kiterjesztett ACL-t. **Megjegyzés:** Ez a beállítás nem módosul automatikusan, ha az irányelv visszaállításra kerül az AIX alapértelmezett irányelvre, a DoDv2_to_ használatával az AIXDefault.xml fájlhoz. Ezt a beállítást kézzel kell módosítani.
GEN003790	A szolgáltatásfájl nem rendelkezhet kiterjesztett hozzáférés-felügyeleti listával (ACL).	**Hely** /etc/security/pscexpert/dodv2/acldodfiles **Megfelelési művelet** Letiltja a megadott kiterjesztett ACL-t. **Megjegyzés:** Ez a beállítás nem módosul automatikusan, ha az irányelv visszaállításra kerül az AIX alapértelmezett irányelvre, a DoDv2_to_ használatával az AIXDefault.xml fájlhoz. Ezt a beállítást kézzel kell módosítani.
GEN003950	A hosts.lpd fájl (vagy egyenértékű) nem rendelkezhet kiterjesztett hozzáférés-felügyeleti listával (ACL).	**Hely** /etc/security/pscexpert/dodv2/acldodfiles **Megfelelési művelet** Letiltja a megadott kiterjesztett ACL-t. **Megjegyzés:** Ez a beállítás nem módosul automatikusan, ha az irányelv visszaállításra kerül az AIX alapértelmezett irányelvre, a DoDv2_to_ használatával az AIXDefault.xml fájlhoz. Ezt a beállítást kézzel kell módosítani.
GEN004010	A traceroute fájl nem rendelkezhet kiterjesztett hozzáférés-felügyeleti listával (ACL).	**Hely** /etc/security/pscexpert/dodv2/acldodfiles **Megfelelési művelet** Letiltja a megadott kiterjesztett ACL-t. **Megjegyzés:** Ez a beállítás nem módosul automatikusan, ha az irányelv visszaállításra kerül az AIX alapértelmezett irányelvre, a DoDv2_to_ használatával az AIXDefault.xml fájlhoz. Ezt a beállítást kézzel kell módosítani.
GEN004390	Az alias fájl nem rendelkezhet kiterjesztett hozzáférés-felügyeleti listával (ACL).	**Hely** /etc/security/pscexpert/dodv2/acldodfiles **Megfelelési művelet** Letiltja a megadott kiterjesztett ACL-t. **Megjegyzés:** Ez a beállítás nem módosul automatikusan, ha az irányelv visszaállításra kerül az AIX alapértelmezett irányelvre, a DoDv2_to_ használatával az AIXDefault.xml fájlhoz. Ezt a beállítást kézzel kell módosítani.

5. táblázat: DoD hozzáférés-felügyeleti lista (ACL) követelményei (Folytatás)

Department of Defense STIG ellenőrzési pont azonosító	**Leírás**	**A parancsfájl helye, ahol a művelet meg van határozva, valamint a művelet eredménye, amely lehetővé teszi a megfelelést**
GEN004430	A levelezési aliases fájlon keresztül futtatott fájlok nem rendelkezhetnek kiterjesztett hozzáférés-felügyeleti listával (ACL).	**Hely** /etc/security/pscexpert/dodv2/acldodfiles **Megfelelési művelet** Letiltja a megadott kiterjesztett ACL-t. **Megjegyzés:** Ez a beállítás nem módosul automatikusan, ha az irányelv visszaállításra kerül az AIX alapértelmezett irányelvre, a DoDv2_to_ használatával az AIXDefault.xml fájlhoz. Ezt a beállítást kézzel kell módosítani.
GEN004510	Az SMTP szolgáltatás naplófájl nem rendelkezhet kiterjesztett hozzáférés-felügyeleti listával (ACL).	**Hely** /etc/security/pscexpert/dodv2/acldodfiles **Megfelelési művelet** Letiltja a megadott kiterjesztett ACL-t. **Megjegyzés:** Ez a beállítás nem módosul automatikusan, ha az irányelv visszaállításra kerül az AIX alapértelmezett irányelvre, a DoDv2_to_ használatával az AIXDefault.xml fájlhoz. Ezt a beállítást kézzel kell módosítani.
GEN004950	Az ftpusers fájl nem rendelkezhet kiterjesztett hozzáférés-felügyeleti listával (ACL).	**Hely** /etc/security/pscexpert/dodv2/acldodfiles **Megfelelési művelet** Letiltja a megadott kiterjesztett ACL-t. **Megjegyzés:** Ez a beállítás nem módosul automatikusan, ha az irányelv visszaállításra kerül az AIX alapértelmezett irányelvre, a DoDv2_to_ használatával az AIXDefault.xml fájlhoz. Ezt a beállítást kézzel kell módosítani.
GEN005190	Az .Xauthority fájlok nem rendelkezhetnek kiterjesztett hozzáférés-felügyeleti listával (ACL).	**Hely** /etc/security/pscexpert/dodv2/acldodfiles **Megfelelési művelet** Letiltja a megadott kiterjesztett ACL-t. **Megjegyzés:** Ez a beállítás nem módosul automatikusan, ha az irányelv visszaállításra kerül az AIX alapértelmezett irányelvre, a DoDv2_to_ használatával az AIXDefault.xml fájlhoz. Ezt a beállítást kézzel kell módosítani.
GEN005350	A Management Information Base (MIB) fájlok nem rendelkezhetnek kiterjesztett hozzáférés-felügyeleti listával (ACL).	**Hely** /etc/security/pscexpert/dodv2/acldodfiles **Megfelelési művelet** Letiltja a megadott kiterjesztett ACL-t. **Megjegyzés:** Ez a beállítás nem módosul automatikusan, ha az irányelv visszaállításra kerül az AIX alapértelmezett irányelvre, a DoDv2_to_ használatával az AIXDefault.xml fájlhoz. Ezt a beállítást kézzel kell módosítani.
GEN005375	Az snmpd.conf fájl nem rendelkezhet kiterjesztett hozzáférés-felügyeleti listával (ACL).	**Hely** /etc/security/pscexpert/dodv2/acldodfiles **Megfelelési művelet** Letiltja a megadott kiterjesztett ACL-t. **Megjegyzés:** Ez a beállítás nem módosul automatikusan, ha az irányelv visszaállításra kerül az AIX alapértelmezett irányelvre, a DoDv2_to_ használatával az AIXDefault.xml fájlhoz. Ezt a beállítást kézzel kell módosítani.

5. táblázat: DoD hozzáférés-felügyeleti lista (ACL) követelményei (Folytatás)

Department of Defense STIG ellenőrzési pont azonosító	Leírás	A parancsfájl helye, ahol a művelet meg van határozva, valamint a művelet eredménye, amely lehetővé teszi a megfelelést
GEN005395	Az /etc/syslog.conf fájl nem rendelkezhet kiterjesztett hozzáférés-felügyeleti listával (ACL).	**Hely** /etc/security/pscexpert/dodv2/acldodfiles **Megfelelési művelet** Letiltja a megadott kiterjesztett ACL-t. **Megjegyzés:** Ez a beállítás nem módosul automatikusan, ha az irányelv visszaállításra kerül az AIX alapértelmezett irányelvre, a DoDv2_to_ használatával az AIXDefault.xml fájlhoz. Ezt a beállítást kézzel kell módosítani.
GEN006150	Az /usr/lib/smb.conf fájl nem rendelkezhet kiterjesztett hozzáférés-felügyeleti listával (ACL).	**Hely** /etc/security/pscexpert/dodv2/acldodfiles **Megfelelési művelet** Letiltja a megadott kiterjesztett ACL-t. **Megjegyzés:** Ez a beállítás nem módosul automatikusan, ha az irányelv visszaállításra kerül az AIX alapértelmezett irányelvre, a DoDv2_to_ használatával az AIXDefault.xml fájlhoz. Ezt a beállítást kézzel kell módosítani.
GEN006210	A /var/private/smbpasswd fájl nem rendelkezhet kiterjesztett hozzáférés-felügyeleti listával (ACL).	**Hely** /etc/security/pscexpert/dodv2/acldodfiles **Megfelelési művelet** Letiltja a megadott kiterjesztett ACL-t. **Megjegyzés:** Ez a beállítás nem módosul automatikusan, ha az irányelv visszaállításra kerül az AIX alapértelmezett irányelvre, a DoDv2_to_ használatával az AIXDefault.xml fájlhoz. Ezt a beállítást kézzel kell módosítani.
GEN006270	Az /etc/news/hosts.nntp fájl nem rendelkezhet kiterjesztett hozzáférés-felügyeleti listával (ACL).	**Hely** /etc/security/pscexpert/dodv2/acldodfiles **Megfelelési művelet** Letiltja a megadott kiterjesztett ACL-t. **Megjegyzés:** Ez a beállítás nem módosul automatikusan, ha az irányelv visszaállításra kerül az AIX alapértelmezett irányelvre, a DoDv2_to_ használatával az AIXDefault.xml fájlhoz. Ezt a beállítást kézzel kell módosítani.
GEN006290	Az /etc/news/hosts.nntp.nolimit fájl nem rendelkezhet kiterjesztett hozzáférés-felügyeleti listával (ACL).	**Hely** /etc/security/pscexpert/dodv2/acldodfiles **Megfelelési művelet** Letiltja a megadott kiterjesztett ACL-t. **Megjegyzés:** Ez a beállítás nem módosul automatikusan, ha az irányelv visszaállításra kerül az AIX alapértelmezett irányelvre, a DoDv2_to_ használatával az AIXDefault.xml fájlhoz. Ezt a beállítást kézzel kell módosítani.
GEN006310	Az /etc/news/nnrp.access fájl nem rendelkezhet kiterjesztett hozzáférés-felügyeleti listával (ACL).	**Hely** /etc/security/pscexpert/dodv2/acldodfiles **Megfelelési művelet** Letiltja a megadott kiterjesztett ACL-t. **Megjegyzés:** Ez a beállítás nem módosul automatikusan, ha az irányelv visszaállításra kerül az AIX alapértelmezett irányelvre, a DoDv2_to_ használatával az AIXDefault.xml fájlhoz. Ezt a beállítást kézzel kell módosítani.

5. táblázat: DoD hozzáférés-felügyeleti lista (ACL) követelményei (Folytatás)

Department of Defense STIG ellenőrzési pont azonosító	Leírás	A parancsfájl helye, ahol a művelet meg van határozva, valamint a művelet eredménye, amely lehetővé teszi a megfelelést
GEN006330	Az /etc/news/passwd.nntp fájl nem rendelkezhet kiterjesztett hozzáférés-felügyeleti listával (ACL).	**Hely** /etc/security/pscexpert/dodv2/acldodfiles **Megfelelési művelet** Letiltja a megadott kiterjesztett ACL-t. **Megjegyzés:** Ez a beállítás nem módosul automatikusan, ha az irányelv visszaállításra kerül az AIX alapértelmezett irányelvre, a DoDv2_to_ használatával az AIXDefault.xml fájlhoz. Ezt a beállítást kézzel kell módosítani.
GEN008120	Ha a rendszer LDAP protokollt használ a hitelesítéshez vagy a fiókinformációkhoz akkor az /etc/ldap.conf (vagy egyenértékű) fájl nem rendelkezhet kiterjesztett hozzáférés-felügyeleti listával (ACL).	**Hely** /etc/security/pscexpert/dodv2/acldodfiles **Megfelelési művelet** Biztosítja, hogy a megadott fájlok ne rendelkezzenek kiterjesztett hozzáférés-felügyeleti listával (ACL). **Megjegyzés:** Ez a beállítás nem módosul automatikusan, ha az irányelv visszaállításra kerül az AIX alapértelmezett irányelvre, a DoDv2_to_ használatával az AIXDefault.xml fájlhoz. Ezt a beállítást kézzel kell módosítani.
GEN008200	Ha a rendszer LDAP protokollt használ a hitelesítéshez vagy a fiókinformációkhoz, akkor az LDAP TLS tanúsítványhatóság fájl vagy könyvtár (amelyik megfelelő) nem rendelkezhet kiterjesztett hozzáférés-felügyeleti listával (ACL).	**Hely** /etc/security/pscexpert/dodv2/acldodfiles **Megfelelési művelet** Biztosítja, hogy a megadott könyvtár vagy fájl ne rendelkezzen kiterjesztett hozzáférés-felügyeleti listával (ACL). **Megjegyzés:** Ez a beállítás nem módosul automatikusan, ha az irányelv visszaállításra kerül az AIX alapértelmezett irányelvre, a DoDv2_to_ használatával az AIXDefault.xml fájlhoz. Ezt a beállítást kézzel kell módosítani.

Kapcsolódó tájékoztatás:

Department of Defense STIG megfelelés

Fizetőkártya iparág - Adatbiztonsági szabványnak megfelelés

A Fizetőkártya iparág - Adatbiztonsági szabvány (PCI - DSS) az IT biztonságot 12 kategóriába sorolja, amelynek neve 12 követelmény és biztonság felmérési eljárás.

A PCI - DSS által meghatározott IT biztonság 12 követelmény és biztonság felmérési eljárásai a következő elemeket tartalmazzák:

1. követelmény: Tűzfal konfiguráció telepítése és fenntartása a kártyabirtokos adatainak védelmére.
Az üzletvitelhez szükséges szolgáltatások és portok dokumentált listája. Ennek a követelménynek a teljesítése a szükségtelen és nem biztonságos szolgáltatások letiltásával kerül megvalósításra.

2. követelmény: Ne legyenek használatban a kereskedő által megadott alapértelmezések a rendszerhez tartozó jelszavakhoz és más biztonsági paraméterekhez.
Mielőtt telepít egy rendszert a hálózaton, mindig módosítsa a kereskedő által megadott alapértelmezett értékeket. Ennek a követelménynek a teljesítése az Egyszerű hálózatkezelési protokoll (SNMP) démon letiltásával kerül megvalósításra.

3. követelmény: Kártyabirtokos tárolt adatainak védelme.
Ez a követelmény a Titkosított fájlrendszer (EFS) szolgáltatás engedélyezésével kerül megvalósításra, amelyet az AIX operációs rendszer biztosít.

4. követelmény: Kártyabirtokos adatainak titkosítása az adatok átvitele esetén nyilvános hálózatokon keresztül.

Ennek a követelménynek a teljesítése az IP biztonság (IPSEC) szolgáltatással kerül megvalósításra, amelyet az AIX operációs rendszer biztosít.

5. követelmény: Antivírus programok használata és rendszeres frissítése.

Ennek a követelménynek a teljesítése a Trusted Execution (megbízható végrehajtás) irányelvprogrammal kerül megvalósításra. A Trusted Execution az ajánlott antivírus szoftver, amely be van építve az AIX operációs rendszerbe. A PCI megköveteli, hogy a naplók a Trusted Execution programból kerüljenek lementésre a Biztonsági információk és eseménykezelés (SIEM) engedélyezésével a riasztások figyeléséhez. A Trusted Execution program csak naplózás módban történő futtatása nem állítja le az ellenőrzéseket, ha egy kivonateltérés hibát okoz.

6. követelmény: Biztonságos rendszerek és alkalmazások fejlesztése és karbantartása

A követelmény teljesítéséhez kézzel telepítse a szükséges javításokat a rendszeren. Ha megvásárolta a PowerSC Standard Edition terméket, akkor használhatja a Trusted Network Connect (TNC) szolgáltatást.

7. követelmény: Hozzáférés korlátozása kártyabirtokos adataihoz az üzletvitel számára szükséges információk alapján.

Hatékony hozzáférés-felügyeleti mértékeket valósíthat meg az RBAC szolgáltatás használatával a szabályok és szerepek engedélyezéséhez. Az RBAC nem automatizálható, mivel megköveteli, hogy az adminisztrátor adatbevitele engedélyezett legyen.

Az RbacEnablement ellenőrzi a rendszert és meghatározza, hogy a szerepek isso, so és sa tulajdonsága létezik-e a rendszeren. Ha ezek a tulajdonságok nem léteznek, akkor a parancsfájl létrehozza őket. Ez a parancsfájl a pscexpert ellenőrzések részeként is futtatásra kerül, és az ellenőrzés végrehajtja a parancsok futtatásakor, például a pscxpert -c parancs futtatásakor.

8. követelmény: Egyedi azonosító hozzárendelése minden egyes személyhez, akinek hozzáférése van a számítógéphez.

Ez a követelmény PCI profilok engedélyezésével teljesíthető. A PCI profilra a következő szabályok vonatkoznak:

- Felhasználói jelszavak módosítása legalább 90 naponként.
- Kötelező minimum 7 karakterből álló jelszót megadni.
- Olyan jelszó használata, amely szám és betű karaktereket is tartalmaz.
- Nem engedélyezett az egyén számára olyan új jelszó megadása, amely megegyezik a korábban használt négy előző jelszóval.
- Az ismételt hozzáférési kísérletek korlátozása a felhasználói azonosító kizárásával hat sikertelen kísérlet után.
- A kizárási időtartam beállítása 30 percre, vagy amíg az adminisztrátor újra engedélyezi a felhasználói azonosítót.
- A felhasználónak újra meg kell adni a jelszavát a terminál újraaktiválásához, miután az 15 percig vagy hosszabb ideig tétlen.

9. követelmény: Fizikai hozzáférés korlátozása a kártyabirtokos adataihoz.

Érzékeny kártyabirtokosi adatokat tartalmazó tárolók tárolása korlátozott hozzáférhetőségű helyiségben.

10. követelmény: Összes hozzáférés nyomkövetése és megfigyelése a hálózati erőforrásokhoz és a kártyabirtokos adataihoz.

Ennek a követelménynek a teljesítése a rendszerösszetevőkhöz történő hozzáférés naplózásával kerül megvalósításra, az automatikus naplózás engedélyezésével a rendszer összetevőin.

11. követelmény: A biztonsági rendszerek és folyamatok rendszeres tesztelése.

Ennek a követelménynek a teljesítése a Real-Time Compliance (valós idejű megfelelés) szolgáltatással történik.

12. követelmény: Olyan biztonsági irányelv fenntartása, amely információs biztonságot tartalmaz az alkalmazottak és a vállalkozók számára.

Modemek aktiválása csak olyan kereskedők számára, akik használat után azonnal deaktiválják. Ennek a

követelménynek a teljesítése a távoli root bejelentkezés letiltásával, a rendszeradminisztrátor által szükség esetén történő aktiválással, majd deaktiválással kerül megvalósításra.

A PowerSC Standard Edition csökkenti azt a konfigurációfelügyeletet, amelyre PCI DSS 2.0. változat és a PCI DSS 3.0. változat irányelveinek való megfeleléshez van szükség. Azonban a teljes folyamat nem automatizálható.

Például a kártyabirtokos adataihoz történő hozzáférés korlátozása az üzleti követelmények alapján nem automatizálható. Az AIX operációs rendszer hatékony biztonsági technológiákat biztosít, például a Szerep alapú hozzáférés-felügyeletet (RBAC); azonban a PowerSC Standard Edition nem tudja automatizálni ezt a konfigurációt, mert nem tudja meghatározni azokat az egyéneket, akik hozzáférést igényelnek és azokat, akik nem. Az IBM Compliance Expert képes automatizálni más biztonsági beállítások konfigurációját, amelyek konzisztensek a PCI követelményekkel.

A PCI profil alkalmazásakor az adatbázis-környezethez, a szoftververem által használt több TCP és UDP port is letiltásra kerül a korlátozások által. Az alkalmazás futtatásához és a terhelés kiegyenlítéséhez engedélyezni kell ezeket a portokat és le kell tiltani a Trusted Execution funkciót. A korlátozás eltávolításához a portokon és a Trusted Execution funkció letiltásához futtassa a következő parancsokat:

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

Megjegyzés: Az összes olyan egyéni parancsfájl, amely a PCI - DSS megfelelés fenntartásához lett megadva, az /etc/security/pscexpert/bin könyvtárban található.

A következő táblázatban megtekintheti, hogy a PowerSC Standard Edition hogyan határozza meg a PCI DSS szabvány követelményeit az AIX Security Expert segédprogram funkcióinak használatával:

6. táblázat: PCI DSS megfelelés 2.0. és 3.0. változatú szabványaihoz kapcsolódó beállítások

Az alábbi PCI DSS szabványok megvalósítása	Megvalósítási specifikáció	Az AIX Security Expert megvalósítás	Az értékek módosító parancsfájl helye
2.1	Rendszerek telepítése előtt a hálózaton, mindig módosítsa a kereskedő által megadott alapértelmezett értékeket. Például foglaljon bele jelszavakat, egyszerű hálózatkezelési protokoll közösségi karaktersorozatokat és szüntesse meg a szükségtelen fiókokat.	A hetek minimális számának beállítása 0 hétre, amelynek el kell telnie, mielőtt módosítani lehetne a jelszót, a **minage** paraméter értékének beállításával 0-ra.	/etc/security/pscexpert/bin/chusrattr
PCI 2. változat 8.5.9 **PCI 3. változat** 8.2.4	Felhasználói jelszavak módosítása 90 naponként.	A jelszó érvényességének beállítása 13 hétre, a hetek maximális számára, a **maxage** paraméter értékének beállításával 13-ra.	/etc/security/pscexpert/bin/chusrattr
2.1	Rendszerek telepítése előtt a hálózaton, mindig módosítsa a kereskedő által megadott alapértelmezett értékeket. Például foglaljon bele jelszavakat, egyszerű hálózatkezelési protokoll közösségi karaktersorozatokat és szüntesse meg a szükségtelen fiókokat.	A hetek számának beállítása 8 hétre, ameddig a lejárt jelszót tartalmazó fiók a rendszeren marad, a **maxexpired** paraméter értékének beállításával 8-ra.	/etc/security/pscexpert/bin/chusrattr

6. táblázat: PCI DSS megfelelés 2.0. és 3.0. változatú szabványaihoz kapcsolódó beállítások (Folytatás)

Az alábbi PCI DSS szabványok megvalósítása	Megvalósítási specifikáció	Az AIX Security Expert megvalósítás	Az értékek módosító parancsfájl helye
PCI 2. változat 8.5.10 **PCI 3. változat** 8.2.3	Kötelező legalább 7 karakterből álló jelszót megadni.	A minimális jelszóhossz beállítása 7 karakterre, a **minlen** paraméter értékének beállításával 7-re.	/etc/security/pscexpert/bin/chusrattr
PCI 2. változat 8.5.11 **PCI 3. változat** 8.2.3	Szám és betű karaktert is tartalmazó jelszavak használata.	A kötelezően megadandó betű karakterek minimális számának beállítása 1-re. Ez a beállítás biztosítja, hogy a jelszó tartalmazzon betű karaktert, a **minalpha** paraméter értékének beállításával 1-re.	/etc/security/pscexpert/bin/chusrattr
PCI 2. változat 8.5.11 **PCI 3. változat** 8.2.3	Szám és betű karaktereket is tartalmazó jelszavak használata.	A kötelezően megadandó nem betű karakterek minimális számának beállítása 1-re. Ez a beállítás biztosítja, hogy a jelszó tartalmazzon nem betű karaktert, a **minother** paraméter értékének beállításával 1-re.	/etc/security/pscexpert/bin/chusrattr
PCI 2. változat 2.1 **PCI 3. változat** 8.2.2	Rendszerek telepítése előtt a hálózaton, mindig módosítsa a kereskedő által megadott alapértelmezett értékeket. Például foglaljon bele jelszavakat, egyszerű hálózatkezelési protokoll közösségi karaktersorozatokat és szüntesse meg a szükségtelen fiókokat.	A jelszóban a karakterismétlési alkalmak maximális számának beállítása 8-ra, a **maxrepeats** paraméter értékének beállításával 8-ra. Ez a beállítás azt jelzi, hogy a jelszóban a karakter korlátlanul megismételhető, ha megfelel a többi jelszókorlátozásnak.	/etc/security/pscexpert/bin/chusrattr
PCI 2. változat 8.5.12 **PCI 3. változat** 8.2.5	Nem engedélyezett az egyén számára olyan új jelszó megadása, amely megegyezik az előzőleg használt négy jelszó bármelyikével.	A hetek számának beállítása 52-re, mielőtt a jelszó újrafelhasználható lenne, a **histexpire** paraméter értékének beállításával 52-re.	/etc/security/pscexpert/bin/chusrattr
PCI 2. változat 8.5.12 **PCI 3. változat** 8.2.5	Nem engedélyezett az egyén számára olyan új jelszó megadása, amely megegyezik az előzőleg használt négy jelszó bármelyikével.	Az előző jelszavak számának beállítása 4-re, amelyet nem lehet újrafelhasználni, a **histsize** paraméter értékének beállításával 4-re.	/etc/security/pscexpert/bin/chusrattr
PCI 2. változat 8.5.13 **PCI 3. változat** 8.1.6	Az ismételt hozzáférési kísérletek korlátozása a felhasználói azonosító kizárásával legfeljebb hat kísérlet után.	Az egymást követő sikertelen bejelentkezési kísérletek számának beállítása 6 kísérletre minden egyes nem root fiókhoz, a **loginentries** paraméter értékének beállításával 6-ra.	/etc/security/pscexpert/bin/chusrattr
PCI 2. változat 8.5.13 **PCI 3. változat** 8.1.6	Az ismételt hozzáférési kísérletek korlátozása a felhasználói azonosító kizárásával legfeljebb hat kísérlet után.	Az egymást követő sikertelen bejelentkezési kísérletek számának beállítása 6-ra, amely letiltja a portot, a **logindisable** paraméter értékének beállításával 6-ra.	• /etc/security/pscexpert/bin/chdefstanza • /etc/security/login.cfg
PCI 2. változat 8.5.14 **PCI 3. változat** 8.1.7	A kizárási időtartam beállítása minimum 30 percre, amíg az adminisztrátor engedélyezi a felhasználói azonosítót.	A port zárolási időtartamának beállítása 30 percre, miután a *logindisable* attribútum letiltotta, a **loginreenable** paraméter értékének beállításával 30-ra.	• /etc/security/pscexpert/bin/chdefstanza • /etc/security/login.cfg

6. táblázat: PCI DSS megfelelés 2.0. és 3.0. változatú szabványaihoz kapcsolódó beállítások (Folytatás)

Az alábbi PCI DSS szabványok megvalósítása	Megvalósítási specifikáció	Az AIX Security Expert megvalósítás	Az értékek módosító parancsfájl helye
12.3.9	A távoli hozzáférési technológiák aktiválása a kereskedők és az üzleti partnerek számára kizárólag abban az esetben, ha a szállító vagy az üzleti partner kéri és használat után azonnal deaktiválásra kerül.	A távoli root bejelentkezési funkció letiltása a funkció beállításával false (hamis) értékre. A rendszeradminisztrátor szükség szerint aktiválhatja a távoli bejelentkezési funkció, majd deaktiválhatja, ha a feladat kész.	• /etc/security/pscexpert/bin/chuserstanza • /etc/security/user
8.1.1	Egyedi azonosító hozzárendelése az összes felhasználóhoz, mielőtt hozzáférhetnének a rendszer összetevőkhöz vagy a kártyabirtokosi adatokhoz.	A funkció engedélyezése, amely biztosítja az összes felhasználó számára az egyedi felhasználónevet, mielőtt hozzáférhetnének a rendszerösszetevőkhöz és a kártyabirtokosi adatokhoz, a funkció beállításával true (igaz) értékre.	• /etc/security/pscexpert/bin/chuserstanza • /etc/security/user
10.2	Megfigyelés engedélyezése a rendszeren.	A bináris fájlok megfigyelésének engedélyezése a rendszeren.	/etc/security/pscexpert/bin/pciaudit
PCI 2. változat 1.1.5 2.2.2 **PCI 3. változat** 2.2.2	Szükségtelen és nem biztonságos szolgáltatások letiltása, amely magában foglalja az Egységes munkaasztali környezetet (CDE).	A CDE funkció letiltása, ha a layer four traceroute (LFT) nincs konfigurálva.	/etc/security/pscexpert/bin/comntrows
PCI 2. változat 1.1.5 2.2.2 **PCI 3. változat** 2.2.2	Szükségtelen és nem biztonságos szolgáltatások letiltása, amely magában foglalja a timed démont.	A timed démon leállítása és a vonatkozó bejegyzés kikommentezése az /etc/rc.tcpip fájlban, amely automatikusan indítja a démont.	/etc/security/pscexpert/bin/rctcpip
PCI 2. változat 1.1.5 2.2.2 **PCI 3. változat** 2.2.2	Szükségtelen és nem biztonságos szolgáltatások letiltása, amely magában foglalja az rwhod démont.	Az rwhod démon leállítása és a vonatkozó bejegyzés kikommentezése az /etc/rc.tcpip fájlban, amely automatikusan indítja a démont.	/etc/security/pscexpert/bin/rctcpip
PCI 2. változat 2.1 **PCI 3. változat** 2.1.1	A rendszerek telepítése előtt a hálózaton, módosítsa a gyártó által megadott alapértelmezett értékeket, amely magában foglalja az SNMP démont is.	Az SNMP démon leállítása és a vonatkozó bejegyzés kikommentezése az /etc/rc.tcpip fájlban, amely automatikusan indítja a démont.	/etc/security/pscexpert/bin/rctcpip
PCI 2. változat 2.1 **PCI 3. változat** 2.1.1	A rendszerek telepítése előtt a hálózaton, módosítsa a gyártó által megadott alapértelmezett értékeket, amely magában foglalja az SNMPMIBD démont is.	Az SNMPMIBD démon letiltása a vonatkozó bejegyzés kikommentezésével az /etc/rc.tcpip fájlban, amely automatikusan indítja a démont.	/etc/security/pscexpert/bin/rctcpip
2.1	A rendszerek telepítése előtt a hálózaton, módosítsa a gyártó által megadott alapértelmezett értékeket, amely magában foglalja az AIXMIBD démont is.	Az AIXMIBD démon letiltása a vonatkozó bejegyzés kikommentezésével az /etc/rc.tcpip fájlban, amely automatikusan indítja a démont.	/etc/security/pscexpert/bin/rctcpip

6. táblázat: PCI DSS megfelelés 2.0. és 3.0. változatú szabványaihoz kapcsolódó beállítások (Folytatás)

Az alábbi PCI DSS szabványok megvalósítása	Megvalósítási specifikáció	Az AIX Security Expert megvalósítás	Az értékek módosító parancsfájl helye
2.1	A rendszerek telepítése előtt a hálózaton, módosítsa a gyártó által megadott alapértelmezett értékeket, amely magában foglalja a HOSTMIBD démont is.	A HOSTMIBD démon letiltása a vonatkozó bejegyzés kikommentezésével az /etc/rc.tcpip fájlban, amely automatikusan indítja a démont.	/etc/security/pscexpert/bin/rctcpip
PCI 2. változat 1.1.5 2.2.2 **PCI 3. változat** 2.2.2	Szükségtelen és nem biztonságos szolgáltatások letiltása, amely magában foglalja a DPID2 démont.	A DPID2 démon leállítása és a vonatkozó bejegyzés kikommentezése az /etc/rc.tcpip fájlban, amely automatikusan indítja a démont.	/etc/security/pscexpert/bin/rctcpip
PCI 2. változat 2.1 **PCI 3. változat** 2.2.2	A rendszerek telepítése előtt a hálózaton, módosítsa a gyártó által megadott alapértelmezett értékeket, amely magában foglalja a DHCP szerver leállítását is.	A DHCP szerver letiltása.	/etc/security/pscexpert/bin/rctcpip
PCI 2. változat 1.1.5 2.2.2 **PCI 3. változat** 2.2.2	Szükségtelen és nem biztonságos szolgáltatások letiltása, amely magában foglalja a DHCP ügynököt.	A DHCP továbbító ügynök leállítása és letiltása, valamint a vonatkozó bejegyzés kikommentezése az /etc/rc.tcpip fájlban, amely automatikusan indítja az ügynököt.	/etc/security/pscexpert/bin/rctcpip
PCI 2. változat 1.1.5 2.2.2 **PCI 3. változat** 2.2.2	Szükségtelen és nem biztonságos szolgáltatások letiltása, amely magában foglalja az rshd démont.	Az rshd démon és a parancsértelmező szolgáltatás leállítása és letiltása, valamint a vonatkozó bejegyzések kikommentezése az /etc/inetd.conf fájlban, amely automatikusan indítja a példányokat.	/etc/security/pscexpert/bin/cominetdconf
PCI 2. változat 1.1.5 2.2.2 **PCI 3. változat** 2.2.2	Szükségtelen és nem biztonságos szolgáltatások letiltása, amely magában foglalja az rlogind démont.	Az rlogind démon és az rlogin szolgáltatás leállítása és az összes példányának letiltása. Az AIX Security Expert segédprogram is kikommentezi vonatkozó bejegyzéseket az /etc/inetd.conf fájlban, amely automatikusan indítja a példányokat.	/etc/security/pscexpert/bin/cominetdconf
PCI 2. változat 1.1.5 2.2.2 **PCI 3. változat** 2.2.2	Szükségtelen és nem biztonságos szolgáltatások letiltása, amely magában foglalja a rexecd démont.	A rexecd démon összes példányának leállítása és letiltása. Az AIX Security Expert segédprogram is kikommentezi a vonatkozó bejegyzést az /etc/inetd.conf fájlban, amely automatikusan indítja a démont.	/etc/security/pscexpert/bin/cominetdconf
PCI 2. változat 1.1.5 2.2.2 **PCI 3. változat** 2.2.2	Szükségtelen és nem biztonságos szolgáltatások letiltása, amely magában foglalja a comsat démont.	A comsat démon összes példányának leállítása és letiltása. Az AIX Security Expert segédprogram is kikommentezi a vonatkozó bejegyzést az /etc/inetd.conf fájlban, amely automatikusan indítja a démont.	/etc/security/pscexpert/bin/cominetdconf

6. táblázat: PCI DSS megfelelés 2.0. és 3.0. változatú szabványaihoz kapcsolódó beállítások (Folytatás)

Az alábbi PCI DSS szabványok megvalósítása	Megvalósítási specifikáció	Az AIX Security Expert megvalósítás	Az értékek módosító parancsfájl helye
PCI 2. változat 1.1.5 2.2.2 **PCI 3. változat** 2.2.2	Szükségtelen és nem biztonságos szolgáltatások letiltása, amely magában foglalja a fingerd démont.	A fingerd démon összes példányának leállítása és letiltása. Az AIX Security Expert segédprogram is kikommentezi a vonatkozó bejegyzést az /etc/inetd.conf fájlban, amely automatikusan indítja a démont.	/etc/security/pscexpert/bin/cominetdconf
PCI 2. változat 1.1.5 2.2.2 **PCI 3. változat** 2.2.2	Szükségtelen és nem biztonságos szolgáltatások letiltása, amely magában foglalja a systat démont.	A systat démon összes példányának leállítása és letiltása. Az AIX Security Expert segédprogram is kikommentezi a vonatkozó bejegyzést az /etc/inetd.conf fájlban, amely automatikusan indítja a démont.	/etc/security/pscexpert/bin/cominetdconf
2.1	A rendszerek telepítése előtt a hálózaton, módosítsa a gyártó által megadott alapértelmezett értékeket, amely magában foglalja a netstat parancsot.	A netstat parancs letiltása a vonatkozó bejegyzés kikommentezésével az /etc/inetd.conf fájlban.	/etc/security/pscexpert/bin/cominetdconf
PCI 2. változat 1.1.5 2.2.2 **PCI 3. változat** 2.2.3	Szükségtelen és nem biztonságos szolgáltatások letiltása, amely magában foglalja a tftp démont.	A tftp démon összes példányának leállítása és letiltása. Az AIX Security Expert segédprogram is kikommentezi a vonatkozó bejegyzést az /etc/inetd.conf fájlban, amely automatikusan indítja a démont.	/etc/security/pscexpert/bin/cominetdconf
PCI 2. változat 1.1.5 2.2.2 **PCI 3. változat** 2.2.2	Szükségtelen és nem biztonságos szolgáltatások letiltása, amely magában foglalja a talkd démont.	A talkd démon összes példányának leállítása és letiltása. Az AIX Security Expert segédprogram is kikommentezi a vonatkozó bejegyzést az /etc/inetd.conf fájlban, amely automatikusan indítja a démont.	/etc/security/pscexpert/bin/cominetdconf
PCI 2. változat 1.1.5 2.2.2 **PCI 3. változat** 2.2.2	Szükségtelen és nem biztonságos szolgáltatások letiltása, amely magában foglalja a rquotad démont.	A rquotad démon összes példányának leállítása és letiltása. Az AIX Security Expert segédprogram is kikommentezi a vonatkozó bejegyzést az /etc/inetd.conf fájlban, amely automatikusan indítja a démont.	/etc/security/pscexpert/bin/cominetdconf
PCI 2. változat 1.1.5 2.2.2 **PCI 3. változat** 2.2.2	Szükségtelen és nem biztonságos szolgáltatások letiltása, amely magában foglalja az rstatd démont.	Az rstatd démon összes példányának leállítása és letiltása. Az AIX Security Expert segédprogram is kikommentezi a vonatkozó bejegyzést az /etc/inetd.conf fájlban, amely automatikusan indítja a démont.	/etc/security/pscexpert/bin/cominetdconf
PCI 2. változat 1.1.5 2.2.2 **PCI 3. változat** 2.2.2	Szükségtelen és nem biztonságos szolgáltatások letiltása, amely magában foglalja az rusersd démont.	Az rusersd démon összes példányának leállítása és letiltása. Az AIX Security Expert segédprogram is kikommentezi a vonatkozó bejegyzést az /etc/inetd.conf fájlban, amely automatikusan indítja a démont.	/etc/security/pscexpert/bin/cominetdconf

6. táblázat: PCI DSS megfelelés 2.0. és 3.0. változatú szabványaihoz kapcsolódó beállítások (Folytatás)

Az alábbi PCI DSS szabványok megvalósítása	Megvalósítási specifikáció	Az AIX Security Expert megvalósítás	Az értékek módosító parancsfájl helye
PCI 2. változat 1.1.5 2.2.2 **PCI 3. változat** 2.2.2	Szükségtelen és nem biztonságos szolgáltatások letiltása, amely magában foglalja az rwalld démont.	Az rwalld démon összes példányának leállítása és letiltása. Az AIX Security Expert segédprogram is kikommentezi a vonatkozó bejegyzést az /etc/inetd.conf fájlban, amely automatikusan indítja a démont.	/etc/security/pscexpert/bin/cominetdconf
PCI 2. változat 1.1.5 2.2.2 **PCI 3. változat** 2.2.2	Szükségtelen és nem biztonságos szolgáltatások letiltása, amely magában foglalja a sprayd démont.	A sprayd démon összes példányának leállítása és letiltása. Az AIX Security Expert segédprogram is kikommentezi a vonatkozó bejegyzést az /etc/inetd.conf fájlban, amely automatikusan indítja a démont.	/etc/security/pscexpert/bin/cominetdconf
PCI 2. változat 1.1.5 2.2.2 **PCI 3. változat** 2.2.2	Szükségtelen és nem biztonságos szolgáltatások letiltása, amely magában foglalja a pcnfsd démont.	A pcnfsd démon összes példányának leállítása és letiltása. Az AIX Security Expert segédprogram is kikommentezi a vonatkozó bejegyzést az /etc/inetd.conf fájlban, amely automatikusan indítja a démont.	/etc/security/pscexpert/bin/cominetdconf
PCI 2. változat 1.1.5 2.2.2 **PCI 3. változat** 2.2.2	Szükségtelen és nem biztonságos szolgáltatások letiltása, amely magában foglalja a TCP echo szolgáltatást.	Az echo(tcp) szolgáltatás összes példányának leállítása és letiltása. Az AIX Security Expert segédprogram is kikommentezi a vonatkozó bejegyzést az /etc/inetd.conf fájlban, amely automatikusan indítja a szolgáltatást.	/etc/security/pscexpert/bin/cominetdconf
PCI 2. változat 1.1.5 2.2.2 **PCI 3. változat** 2.2.2	Szükségtelen és nem biztonságos szolgáltatások letiltása, amely magában foglalja a TCP discard szolgáltatást.	A discard(tcp) szolgáltatás összes példányának leállítása és letiltása. Az AIX Security Expert segédprogram is kikommentezi a vonatkozó bejegyzést az /etc/inetd.conf fájlban, amely automatikusan indítja a szolgáltatást.	/etc/security/pscexpert/bin/cominetdconf
PCI 2. változat 1.1.5 2.2.2 **PCI 3. változat** 2.2.2	Szükségtelen és nem biztonságos szolgáltatások letiltása, amely magában foglalja a TCP chargen szolgáltatást.	A chargen(tcp) szolgáltatás összes példányának leállítása és letiltása. Az AIX Security Expert segédprogram is kikommentezi a vonatkozó bejegyzést az /etc/inetd.conf fájlban, amely automatikusan indítja a szolgáltatást.	/etc/security/pscexpert/bin/cominetdconf
PCI 2. változat 1.1.5 2.2.2 **PCI 3. változat** 2.2.2	Szükségtelen és nem biztonságos szolgáltatások letiltása, amely magában foglalja a TCP daytime szolgáltatást.	A daytime(tcp) szolgáltatás összes példányának leállítása és letiltása. Az AIX Security Expert segédprogram is kikommentezi a vonatkozó bejegyzést az /etc/inetd.conf fájlban, amely automatikusan indítja a szolgáltatást.	/etc/security/pscexpert/bin/cominetdconf

6. táblázat: PCI DSS megfelelés 2.0. és 3.0. változatú szabványaihoz kapcsolódó beállítások (Folytatás)

Az alábbi PCI DSS szabványok megvalósítása	Megvalósítási specifikáció	Az AIX Security Expert megvalósítás	Az értékek módosító parancsfájl helye
PCI 2. változat 1.1.5 2.2.2 **PCI 3. változat** 2.2.2	Szükségtelen és nem biztonságos szolgáltatások letiltása, amely magában foglalja a TCP time szolgáltatást.	A timed(tcp) szolgáltatás összes példányának leállítása és letiltása. Az AIX Security Expert segédprogram is kikommentezi a vonatkozó bejegyzést az /etc/inetd.conf fájlban, amely automatikusan indítja a szolgáltatást.	/etc/security/pscexpert/bin/cominetdconf
PCI 2. változat 1.1.5 2.2.2 **PCI 3. változat** 2.2.2	Szükségtelen és nem biztonságos szolgáltatások letiltása, amely magában foglalja az UDP echo szolgáltatást.	Az echo(udp) szolgáltatás összes példányának leállítása és letiltása. Az AIX Security Expert segédprogram is kikommentezi a vonatkozó bejegyzést az /etc/inetd.conf fájlban, amely automatikusan indítja a szolgáltatást.	/etc/security/pscexpert/bin/cominetdconf
PCI 2. változat 1.1.5 2.2.2 **PCI 3. változat** 2.2.2	Szükségtelen és nem biztonságos szolgáltatások letiltása, amely magában foglalja az UDP discard szolgáltatást.	Az discard(udp) szolgáltatás összes példányának leállítása és letiltása. Az AIX Security Expert segédprogram is kikommentezi a vonatkozó bejegyzést az /etc/inetd.conf fájlban, amely automatikusan indítja a szolgáltatást.	/etc/security/pscexpert/bin/cominetdconf
PCI 2. változat 1.1.5 2.2.2 **PCI 3. változat** 2.2.2	Szükségtelen és nem biztonságos szolgáltatások letiltása, amely magában foglalja az UDP chargen szolgáltatást.	A chargen(udp) szolgáltatás összes példányának leállítása és letiltása. Az AIX Security Expert segédprogram is kikommentezi a vonatkozó bejegyzést az /etc/inetd.conf fájlban, amely automatikusan indítja a szolgáltatást.	/etc/security/pscexpert/bin/cominetdconf
PCI 2. változat 1.1.5 2.2.2 **PCI 3. változat** 2.2.2	Szükségtelen és nem biztonságos szolgáltatások letiltása, amely magában foglalja az UDP daytime szolgáltatást.	A daytime(udp) szolgáltatás összes példányának leállítása és letiltása. Az AIX Security Expert segédprogram is kikommentezi a vonatkozó bejegyzést az /etc/inetd.conf fájlban, amely automatikusan indítja a szolgáltatást.	/etc/security/pscexpert/bin/cominetdconf
PCI 2. változat 1.1.5 2.2.2 **PCI 3. változat** 2.2.2	Szükségtelen és nem biztonságos szolgáltatások letiltása, amely magában foglalja az UDP time szolgáltatást.	A timed(udp) szolgáltatás összes példányának leállítása és letiltása. Az AIX Security Expert segédprogram is kikommentezi a vonatkozó bejegyzést az /etc/inetd.conf fájlban, amely automatikusan indítja a szolgáltatást.	/etc/security/pscexpert/bin/cominetdconf
PCI 2. változat 1.1.5 2.2.2 **PCI 3. változat** 2.2.3	Szükségtelen és nem biztonságos szolgáltatások letiltása, amely magában foglalja az FTP szolgáltatást.	Az ftpd démon összes példányának leállítása és letiltása. Az AIX Security Expert segédprogram is kikommentezi a vonatkozó bejegyzést az /etc/inetd.conf fájlban, amely automatikusan indítja a démont.	/etc/security/pscexpert/bin/cominetdconf

6. táblázat: PCI DSS megfelelés 2.0. és 3.0. változatú szabványaihoz kapcsolódó beállítások (Folytatás)

Az alábbi PCI DSS szabványok megvalósítása	Megvalósítási specifikáció	Az AIX Security Expert megvalósítás	Az értékek módosító parancsfájl helye
PCI 2. változat 1.1.5 2.2.2 **PCI 3. változat** 2.2.3	Szükségtelen és nem biztonságos szolgáltatások letiltása, amely magában foglalja a telnet szolgáltatást.	A telnetd démon összes példányának leállítása és letiltása. Az AIX Security Expert segédprogram is kikommentezi a vonatkozó bejegyzést az /etc/inetd.conf fájlban, amely automatikusan indítja a démont.	/etc/security/pscexpert/bin/cominetdconf
PCI 2. változat 1.1.5 2.2.2 **PCI 3. változat** 2.2.2	Szükségtelen és nem biztonságos szolgáltatások letiltása, amely magában foglalja a dtspc szolgáltatást.	A dtspc démon összes példányának leállítása és letiltása. Az AIX Security Expert is kikommentezi a vonatkozó bejegyzést az /etc/inittab fájlban, amely automatikusan elindítja a démont, ha az LFT nincs beállítva és a CDE tiltott az /etc/inittab fájlban.	/etc/security/pscexpert/bin/cominetdconf
PCI 2. változat 1.1.5 2.2.2 **PCI 3. változat** 2.2.2	Szükségtelen és nem biztonságos szolgáltatások letiltása, amely magában foglalja a ttdbserver szolgáltatást.	A ttdbserver szolgáltatás összes példányának leállítása és letiltása. Az AIX Security Expert segédprogram is kikommentezi a vonatkozó bejegyzést az /etc/inetd.conf fájlban, amely automatikusan indítja a szolgáltatást.	/etc/security/pscexpert/bin/cominetdconf
PCI 2. változat 1.1.5 2.2.2 **PCI 3. változat** 2.2.2	Szükségtelen és nem biztonságos szolgáltatások letiltása, amely magában foglalja a cmsd szolgáltatást.	A cmsd szolgáltatás összes példányának leállítása és letiltása. Az AIX Security Expert segédprogram is kikommentezi a vonatkozó bejegyzést az /etc/inetd.conf fájlban, amely automatikusan indítja a szolgáltatást.	/etc/security/pscexpert/bin/cominetdconf
PCI 2. változat 2.2.3 **PCI 3. változat** 2.2.4	Rendszer biztonsági paramétereinek beállítása a hibás használat megakadályozása érdekében.	A Set User ID (SUID) (felhasználói azonosító beállítása) parancsok eltávolítása a vonatkozó bejegyzés kikommentezésével az /etc/inetd.conf fájlban, amely automatikusan engedélyezi a parancsokat.	/etc/security/pscexpert/bin/rmsuidfrmrcmds
PCI 2. változat 2.2.3 **PCI 3. változat** 2.2.4	Rendszer biztonsági paramétereinek beállítása a hibás használat megakadályozása érdekében.	A legalacsonyabb biztonsági szint engedélyezése a fájlengedély-kezelőhöz.	/etc/security/pscexpert/bin/filepermgr
PCI 2. változat 2.2.3 **PCI 3. változat** 2.2.4	Rendszer biztonsági paramétereinek beállítása a hibás használat megakadályozása érdekében.	A Hálózati fájlrendszer protokoll módosítása korlátozó beállításokkal, amelyek megfelelnek a PCI biztonsági követelményeknek. Ezek a korlátozó beállítások magukban foglalják a távoli root hozzáférés, valamint az anonim UID és GID hozzáférés letiltását.	/etc/security/pscexpert/bin/nfsconfig

6. táblázat: PCI DSS megfelelés 2.0. és 3.0. változatú szabványaihoz kapcsolódó beállítások (Folytatás)

Az alábbi PCI DSS szabványok megvalósítása	Megvalósítási specifikáció	Az AIX Security Expert megvalósítás	Az értékek módosító parancsfájl helye
PCI 2. változat 2.2.2 **PCI 3. változat** 2.2.3	Csak a szükséges és biztonságos szolgáltatások, protokollok, démonok stb. engedélyezése, ahogy a rendszer megfelelő működéséhez szükséges. Biztonsági szolgáltatások megvalósítása minden szükséges szolgáltatáshoz, protokollhoz és démonhoz, amely nem tekinthető biztonságosnak.	Az rlogind, rshd és tftpd démon letiltása, amely nem biztonságos.	/etc/security/pscexpert/bin/disrmtdmns
PCI 2. változat 2.2.2 **PCI 3. változat** 2.2.3	Csak a szükséges és biztonságos szolgáltatások, protokollok, démonok stb. engedélyezése, ahogy a rendszer megfelelő működéséhez szükséges. Biztonsági szolgáltatások megvalósítása minden szükséges szolgáltatáshoz, protokollhoz és démonhoz, amely nem tekinthető biztonságosnak.	Az rlogind, rshd és tftpd démon letiltása, amely nem biztonságos.	/etc/security/pscexpert/bin/rmrhostsnetrc
PCI 2. változat 2.2.2 **PCI 3. változat** 2.2.3	Csak a szükséges és biztonságos szolgáltatások, protokollok, démonok stb. engedélyezése, ahogy a rendszer megfelelő működéséhez szükséges. Biztonsági szolgáltatások megvalósítása minden szükséges szolgáltatáshoz, protokollhoz és démonhoz, amely nem tekinthető biztonságosnak.	A logind, rshd és tftpdpci_rmetchostsequiv démon letiltása, amely nem biztonságos.	/etc/security/pscexpert/bin/rmetchostsequiv
PCI 2. változat 1.3.6 **PCI 3. változat** 2.2.3	Részletes vizsgálat vagy csomagszűrés megvalósítása, amelyben csak a létrejött kapcsolatok engedélyezettek a hálózaton.	A hálózati **clean_partial_conns** beállítás engedélyezése az értékének beállításával 1-re.	/etc/security/pscexpert/bin/ntwkopts
PCI 2. változat 2.2.2 **PCI 3. változat** 2.2.3	Részletes vizsgálat vagy csomagszűrés megvalósítása, amelyben csak a létrejött kapcsolatok engedélyezettek a hálózaton.	A TCP biztonság engedélyezése a hálózati **tcp_tcpsecure** opció beállításával 7 értékre. Ez a beállítás biztosít védelmet az adat, visszaállítási (RST) és a TCP kapcsolatkérés (SYN) támadások ellen.	/etc/security/pscexpert/bin/ntwkopts
1.2	Védelem a jogosulatlan hozzáféréssel szemben a használaton kívüli portokhoz.	A rendszer beállítása a hosztok kikerülésére 5 percre, annak megakadályozása érdekében, hogy már rendszerek hozzáférjenek a nem használt portokhoz.	/etc/security/pscexpert/bin/ipsecshunhosthls **Megjegyzés:** További szűrőszabályokat is megadhat az /etc/security/aixpert/bin/filter.txt fájlban. Ezeket a szabályokat az ipsecshunhosthls.sh parancsfájl integrálja a profil alkalmazásakor. A bejegyzéseknek a következő formátumban kell lenni: *portszám*:*ip_cím*: *művelet* Ahol a *művelet* lehetséges értékei az Allow és a Deny.

6. táblázat: PCI DSS megfelelés 2.0. és 3.0. változatú szabványaihoz kapcsolódó beállítások (Folytatás)

Az alábbi PCI DSS szabványok megvalósítása	Megvalósítási specifikáció	Az AIX Security Expert megvalósítás	Az értékek módosító parancsfájl helye
1.2	Hoszt megvédése a portelemzésektől.	A rendszer beállítása a támadható portok elkerülésére 5 percig, amely megakadályozza a portelemzéseket.	/etc/security/pscexpert/bin/ipsecshunports **Megjegyzés:** További szűrőszabályokat is megadhat az /etc/security/aixpert/bin/filter.txt fájlban. Ezeket a szabályokat az ipsecshunhosthls.sh parancsfájl integrálja a profil alkalmazásakor. A bejegyzéseknek a következő formátumban kell lenni: *portszám*:*ip_cím*: *művelet* Ahol a *művelet* lehetséges értékei az Allow és a Deny.
7.1.1	Objektumlétrehozási engedélyek korlátozása.	Az alapértelmezett objektumlétrehozási engedélyek beállítása 22-re, a **umask** paraméter értékének beállításával 22-re.	/etc/security/pscexpert/bin/chusrattr
7.1.1	Rendszerhozzáférés korlátozása.	Biztosítja, hogy a root azonosító legyen az egyetlen, amely felsorolásra kerül a cron.allow fájlban, és eltávolítja a cron.deny fájlt a rendszerről.	/etc/security/pscexpert/bin/limitsysacc
6.5.8	Pont eltávolítása az útvonal gyökeréből.	A pontok eltávolítása a PATH környezeti változóból az alábbi fájlokban, amelyek a gyökér alapkönyvtárban találhatók: • .cshrc • .kshrc • .login • .profile	/etc/security/pscexpert/bin/rmdotfrmpathroot
6.5.8	Pont eltávolítása a nem root útvonalról:	A pontok eltávolítása a *PATH* környezeti változóból az alábbi fájlokban, amelyek a felhasználó saját könyvtárában találhatók: • .cshrc • .kshrc • .login • .profile	/etc/security/pscexpert/bin/rmdotfrmpathnroot
2.2.3	Rendszerhozzáférés korlátozása.	Root felhasználói képesség és a felhasználónév felvétele az /etc/ftpusers fájlban.	/etc/security/pscexpert/bin/chetcftpusers
2.1	Vendég fiók eltávolítása.	Vendég fiók és fájljainak az eltávolítása.	/etc/security/pscexpert/bin/execmds
6.5.2	Programok indításának megakadályozása a tartalomterületen.	A veremvégrehajtás letiltása (SED) szolgáltatás engedélyezése.	/etc/security/pscexpert/bin/sedconfig
8.2	Meggyőződés a root felhasználó jelszavának biztonságosságáról.	A root jelszó integritási ellenőrzésének elindítása a root jelszóhoz, ezáltal biztosítva a biztonságos root jelszót.	/etc/security/pscexpert/bin/chuserstanza
PCI 2. változat 8.5.15 **PCI 3. változat** 8.1.8	Hozzáférés korlátozása a rendszerhez a munkamenet tétlen idejének beállításával.	Tétlenségi várakozik beállítása 15 percre. Ha a munkamenet 15 percnél hosszabb ideig tétlen, akkor újra meg kell adni a jelszót.	/etc/security/pscexpert/bin/autologoff

6. táblázat: PCI DSS megfelelés 2.0. és 3.0. változatú szabványaihoz kapcsolódó beállítások (Folytatás)

Az alábbi PCI DSS szabványok megvalósítása	Megvalósítási specifikáció	Az AIX Security Expert megvalósítás	Az értékek módosító parancsfájl helye
1.3.5	Forgalom hozzáférés korlátozása a kártyabirtokos információihoz.	A TCP forgalom szabályozás beállítása magas értékre, amely kikényszeríti a szolgáltatás megbénítását a portokon.	/etc/security/pscexpert/bin/tcptr_pscexpert
1.3.5	Biztonságos kapcsolat fenntartása az adatok áttelepítésekor.	Automatikus IP biztonsági (IPSec) alagút létrehozás engedélyezése a Virtual I/O Server szerverek között az élő partíció átállítás során.	/etc/security/pscexpert/bin/cfgsecmig
1.3.5	Ismeretlen forrásokból származó csomagok korlátozása.	Engedélyezi a csomagokat a hardverkezelő konzolról.	/etc/security/pscexpert/bin/ipsecpermithostorport
5.1.1	Antivírus szoftver karbantartása.	Fenntartja a rendszerintegritást a rosszindulatú szoftvertípusok észlelésével, eltávolításával.	/etc/security/pscexpert/bin/manageITsecurity
PCI 2. változat 7. szakasz **PCI 3. változat** 7. szakasz	Hozzáférés karbantartása igény szerinti alapon.	A szerep alapú hozzáférés-felügyelet (RBAC) engedélyezése, ehhez létrehozásra kerül a rendszeroperátor, rendszeradminisztrátor és az információs rendszer adatvédelmi megbízott felhasználói szerep a szükséges engedélyekkel.	/etc/security/pscexpert/bin/EnableRbac
PCI 2. változat Nincs benne a 2. változatú profilban, a 3. változatban lett hozzáadva. **PCI 3. változat** 2.3	További biztonsági szolgáltatások megvalósítása minden szükséges szolgáltatáshoz, protokollhoz és démonhoz, amely nem tekinthető biztonságosnak.	Biztonságos technológiákat használ, mint például a Biztonságos parancsértelmező (SSH), SSH Fájlátviteli protokoll (S-FTP), Védett socket réteg (SSL) vagy az Internet Protocol Security Virtual Private Network (IPsec VPN) a nem biztonságos szolgáltatások védelmére, mint például a NetBIOS, fájlmegosztás, Telnet és FTP. Ezenkívül beállítja az SSH démont kizárólag az SSHv2 protokoll használatára.	/etc/security/pscexpert/bin/sshPCIconfig
PCI 2. változat Nincs benne a 2. változatú profilban, a 3. változatban lett hozzáadva. **PCI 3. változat** 2.3	Az SSH ügyfelet úgy kell beállítani, hogy csak az SSHv2 protokollt használja.	Az SSH ügyfelet csak az SSHv2 protokoll használatára állítja be.	/etc/security/pscexpert/bin/sshPCIconfig
PCI 2. változat Nincs benne a 2. változatú profilban, a 3. változatban lett hozzáadva. **PCI 3. változat** 2.3	Az SSH démon csak felügyeleti hálózati címeken figyelhet, hacsak nem jogosult más használatra is a felügyeleten kívül.	Biztosítja, hogy az SSH démon csak figyelésre legyen beállítva.	/etc/security/pscexpert/bin/sshPCIconfig

6. táblázat: PCI DSS megfelelés 2.0. és 3.0. változatú szabványaihoz kapcsolódó beállítások (Folytatás)

Az alábbi PCI DSS szabványok megvalósítása	Megvalósítási specifikáció	Az AIX Security Expert megvalósítás	Az értékek módosító parancsfájl helye
PCI 2. változat Nincs benne a 2. változatú profilban, a 3. változatban lett hozzáadva. **PCI 3. változat** 2.3	Az SSH démon csak FIPS 140-2-es jóváhagyott rejtjelek használatára állítható be	Biztosítja, hogy az SSH démon csak FIPS 140-2-es rejtjeleket használjon.	/etc/security/pscexpert/bin/sshPCIconfig
PCI 2. változat Nincs benne a 2. változatú profilban, a 3. változatban lett hozzáadva. **PCI 3. változat** 2.3	Az SSH démont úgy kell beállítani, hogy csak azokat az üzenethitelesítési kódokat (MAC) használja, amelyek FIPS 140-2-es jóváhagyott kriptográfiai kivonat algoritmusokat alkalmaznak.	Biztosítja, hogy a MAC-ek a jóváhagyott algoritmusokat futtassák.	/etc/security/pscexpert/bin/sshPCIconfig
PCI 2. változat Nincs benne a 2. változatú profilban, a 3. változatban lett hozzáadva. **PCI 3. változat** 2.3	Az SSH démonnak korlátozni kell a bejelentkezési képességet specifikus felhasználókra vagy csoportokra.	Korlátozza a bejelentkezést specifikus felhasználókra és csoportokra a rendszeren.	/etc/security/pscexpert/bin/sshPCIconfig
PCI 2. változat Nincs benne a 2. változatú profilban, a 3. változatban lett hozzáadva. **PCI 3. változat** 2.3	A rendszernek bejelentkezéskor meg kell jeleníteni az utolsó sikeres fiókba történő bejelentkezés dátumát és időpontját.	Fenntartja az információkat a legutóbbi sikeres bejelentkezésről és megjeleníti a következő sikeres bejelentkezés után.	/etc/security/pscexpert/bin/sshPCIconfig
PCI 2. változat Nincs benne a 2. változatú profilban, a 3. változatban lett hozzáadva. **PCI 3. változat** 2.3	Az SSH démonnak az alapkönyvtár konfigurációs fájljainak szigorú ellenőrzését kell végrehajtani.	Biztosítja, hogy az alapkönyvtár konfigurációs fájljai a helyes módokra legyenek beállítva.	/etc/security/pscexpert/bin/sshPCIconfig
PCI 2. változat Nincs benne a 2. változatú profilban, a 3. változatban lett hozzáadva. **PCI 3. változat** 2.3	Az SSH démonnak jogosultság elkülönítést kell használni.	Biztosítja, hogy az SSH démon a jogosultságainak megfelelő mennyiségű elkülönítésével rendelkezzen.	/etc/security/pscexpert/bin/sshPCIconfig

6. táblázat: PCI DSS megfelelés 2.0. és 3.0. változatú szabványaihoz kapcsolódó beállítások (Folytatás)

Az alábbi PCI DSS szabványok megvalósítása	Megvalósítási specifikáció	Az AIX Security Expert megvalósítás	Az értékek módosító parancsfájl helye
PCI 2. változat Nincs benne a 2. változatú profilban, a 3. változatban lett hozzáadva. **PCI 3. változat** 2.3	Az SSH démon nem engedélyezheti az rhosts számára az RSA hitelesítést.	Letiltja az RSA hitelesítést az rhosts számára az SSH démon használatakor.	/etc/security/pscexpert/bin/sshPCIconfig
PCI 2. változat 1.1.5 2.2.2 **PCI 3. változat** 10.4	Konfigurációs szabványok és folyamatok vizsgálata annak ellenőrzése érdekében, hogy az időszinkronizációs technológia megvalósításra kerül-e és aktuális marad-e PCI DSS 6.1-es és 6.2-es követelményekként.	Engedélyezi az ntp démont.	/etc/security/pscexpert/bin/rctcpip
PCI 2. változat Nincs benne a 2. változatú profilban, a 3. változatban lett hozzáadva. **PCI 3. változat** 8.1.5	Felhasználói fiók letiltása, ha nincs használatban.	Letiltja a felhasználói fiókokat 35 nap inaktivitást követően.	/etc/security/pscexpert/bin/disableacctpci
PCI 3. változat 2.2.3	Védett socket réteg (SSL) v3 és Szállítási réteg biztonság (TLS) v1.0 letiltása az alkalmazásokban.	SSLv3 és TLS v1.0 változat letiltása a Courier POP3 szerver (Pop3d) konfigurációjában.	/etc/security/pscexpert/bin/disableSSL
PCI 3. változat 2.2.3	SSL v3 és TLS v1.0 letiltása az alkalmazásokban.	SSLV3 és TLS v1.0 letiltása a Courier IMAP szerveren (imapd).	/etc/security/pscexpert/bin/disableSSL
PCI 3. változat 8.2.1	SSL v3 és TLS v1.0 letiltása az alkalmazásokban.	Hálózati időprotokoll (NTP) konfigurációs fájl ellenőrzése a TLS 1.1. vagy újabb biztonsági megvalósításhoz.	/etc/security/pscexpert/bin/checkNTP
PCI 3. változat 2.2.3	SSL v3 és TLS v1.0 letiltása az alkalmazásokban.	Fájlátviteli protokoll démon (FTPD) konfigurációs fájl ellenőrzése a TLS 1.1. vagy újabb biztonsági megvalósításhoz.	/etc/security/pscexpert/bin/secureFTP
PCI 3. változat 2.2.3	SSL v3 és TLS v1.0 letiltása az alkalmazásokban.	Fájlátviteli protokoll (FTP) konfigurációs fájl ellenőrzése a TLS 1.1. vagy újabb biztonsági megvalósításhoz.	/etc/security/pscexpert/bin/secureFTP
PCI 3. változat 2.2.3	SSL v3 és TLS v1.0 letiltása az alkalmazásokban.	SSLv3 és TLS v1.0 letiltása a levélküldési konfigurációban.	/etc/security/pscexpert/bin/sendmailPCIConfig
PCI 3. változat 2.2.3	SSL v3 és TLS v1.0 letiltása az alkalmazásokban.	Annak ellenőrzése, hogy az AIX rendszeren az SSL változat újabb-e, mint 1.0.2.	/etc/security/pscexpert/bin/sslversion
PCI 3. változat 8.2.1	Kétfaktoros hitelesítés kikényszerítése.	Kétfaktoros hitelesítés kikényszerítése, mint például az SHA-256 és az SHA-512.	/etc/security/pscexpert/bin/pwdalgchk

Kapcsolódó tájékoztatás:

Fizetőkártya iparág - Adatbiztonsági szabványnak megfelelés

Sarbanes-Oxley törvény és COBIT megfelelés

A 2002-es Sarbanes-Oxley (SOX) törvény, amelyet az Amerikai Egyesült Államok 107. kongresszusán hoztak, a befektetők védelme érdekében szabályozza azon nyilvános vállalatok auditálását, amelyek értékpapírokkal és a kapcsolódó anyagokkal foglalkoznak.

A SOX 404-es paragrafusa kötelezővé teszi a felügyelet felmérését a belső szabályozások felett. A legtöbb szervezet esetében a belső szabályozások kiterjednek az információtechnológia rendszerekre, amely a vállalat pénzügyi adatait dolgozzák fel és jelentést készítenek róluk. A SOX törvény specifikus részleteket tartalmaz az IT-ra és az IT biztonságra vonatkozóan. A legtöbb SOX auditor olyan szabványokra támaszkodik, mint például a COBIT, amely alapján kimutatja és auditálja a megfelelő IT irányítást és szabályozást. A PowerSC Standard Edition SOX/COBIT XML konfigurációs beállítás biztosítja az AIX és Virtual I/O Server (VIOS rendszerek biztonsági konfigurációját, amelyre a COBIT megfelelési irányelveknek való megfeleléshez van szükség.

Az IBM Compliance Expert Express Edition az AIX operációs rendszer alábbi változatain fut:

- AIX 6.1
- AIX 7.1
- AIX 7.2

A külső szabványoknak való megfelelés az AIX rendszeradminisztrátor felelőssége. Az IBM Compliance Expert Express Edition úgy lett tervezve, hogy leegyszerűsítse az operációs rendszer beállítások és jelentések kezelését, amelyek a szabványoknak való megfeleléshez szükségesek.

Az IBM Compliance Expert Express Edition termékkel együtt szállított előre meghatározott megfelelési profilok csökkentik a megfelelési dokumentáció értelmezésének adminisztrációs terhelését, valamint a szabványok megvalósítását specifikus rendszerkonfigurációs paraméterekként.

Az IBM Compliance Expert Express Edition képességei úgy lettek kialakítva, hogy segítsenek az ügyfeleknek hatékonyan kezelni a külső szabványnak való megfeleléshez tartozó rendszerkövetelményeket, ami jelentősen csökkenti a költségeket, miközben növeli a megfelelést. Minden külső biztonsági szabvány tartalmaz aspektusokat a nem rendszerkonfigurációs beállításokra is. Az IBM Compliance Expert Express Edition használata nem tudja biztosítani a szabványoknak való megfelelést. A Compliance Expert úgy lett tervezve, hogy leegyszerűsítse a rendszerkonfigurációs beállítások kezelését, így segítve az adminisztrátorokat a szabványoknak való megfelelés más szempontjaira fókuszálni.

Kapcsolódó tájékoztatás:

COBIT megfelelés

Az egészségbiztosítás hordozhatóságát és elszámoltathatóságát előíró törvény (HIPAA)

A Health Insurance Portability and Accountability Act (HIPAA) egy olyan biztonsági profil, amely az Electronically Protected Health Information (EPHI) (Elektronikusan védett egészséginformációk) védelmére szolgál.

A HIPAA biztonsági szabály specifikusan az EPHI védelmére fókuszál, és a HIPAA biztonsági szabály tárgyát csak az ügynökségek egy része képezi, a funkciójuk és EPHI használatuk alapján.

Minden HIPAA lefedettségű entitásnak, néhány szövetségi ügynökséghez hasonlóan, meg kell felelni a HIPAA biztonsági szabálynak.

A HIPAA biztonsági szabály az EPHI bizalmasságának, integritásának és elérhetőségének a védelmére szolgál, a biztonsági szabályban meghatározottak szerint.

A lefedett entitás által létrehozott, fogadott, fenntartott és átadott EPHI-t meg kell védeni a valószínűsíthető támadásokkal és veszélyekkel szemben, valamint az engedély nélküli felhasználások és közzétételek ellen.

A HIPAA biztonsági szabály követelményei, szabványai és megvalósítási specifikációi az alábbi lefedett entitásokhoz kerülnek alkalmazásra:

- Egészségügyi szolgáltatók
- Egészségügyi tervek
- Egészségügyi klíringintézetek
- Állami egészségbiztosítók és gyógyszerkártya szponzorok

Az alábbi táblázat részletezi a HIPAA biztonsági szabály több részét, és minden egyes szakasz számos szabványt és megvalósítási specifikációt tartalmaz.

Megjegyzés: A HIPAA megfelelés fenntartásának biztosításához szükséges összes egyéni parancsfájl az /etc/security/pscexpert/bin könyvtárban található.

7. táblázat: HIPAA szabályok és megvalósítási részletek

HIPAA biztonsági szabály szakaszai	Megvalósítási specifikáció	Az aixpert megvalósítás	Parancsok és visszatérési értékek
164.308 (a) (1) (ii) (D) 164.308 (a) (5) (ii) (C) 164.312 (b)	Eljárások megvalósítása az információs rendszertevékenység rekordjainak rendszeres áttekintéséhez, például a megfigyelési naplók, hozzáférési jelentések és biztonsági incidens jelentések áttekintéséhez.	Megállapítja. hogy a megfigyelés engedélyezett-e a rendszeren.	**Parancs**: **#audit query**. **Visszatérési érték**: Ha sikeres, akkor ez a parancs a 0 értékkel lép ki. Ha sikertelen, akkor a parancs az 1-es értékkel lép ki.
164.308 (a) (1) (ii) (D) 164.308 (a) (5) (ii) (C) 166.312 (b)	Eljárások megvalósítása az információs rendszertevékenység rekordjainak rendszeres áttekintéséhez, például a megfigyelési naplók, hozzáférési jelentések és biztonsági incidens jelentések áttekintéséhez.	Engedélyezi a megfigyelést a rendszeren. Ezenkívül beállítja a lementendő eseményeket.	**Parancs**: **# audit start >/dev/null 2>&1**. **Visszatérési érték**: Ha sikeres, akkor ez a parancs a 0 értékkel lép ki. Ha sikertelen, akkor a parancs az 1-es értékkel lép ki. A rendszer az alábbi eseményeket figyeli: **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)	Titkosítás és visszafejtés (A):Az EPHI titkosítás és visszafejtés mechanizmusának megvalósítása.	Megállapítja, hogy a titkosított fájlrendszer (EFS) engedélyezett-e a rendszeren.	**Parancs**: **# efskeymgr -V >/dev/null 2>&1**. **Visszatérési érték**: Ha az EFS már engedélyezett, akkor ez a parancs a 0 értékkel lép ki. Ha az EFS nem engedélyezett, akkor a parancs az 1-es értékkel lép ki.

7. táblázat: HIPAA szabályok és megvalósítási részletek (Folytatás)

HIPAA biztonsági szabály szakaszai	Megvalósítási specifikáció	Az aixpert megvalósítás	Parancsok és visszatérési értékek
164.312 (a) (2) (iii)	Automatikus kijelentkezés (A): Az elektronikus munkamenet leállításához szükséges elektronikus eljárás megvalósítása, egy előre meghatározott inaktivitási időtartam elteltével.	Beállítja, hogy a rendszer jelentkezzen ki az interaktív folyamatokból 15 perces inaktivitás elteltével.	**Parancs**: **grep TMOUT= /etc/security /.profile > /dev/null 2>&1** **echo "TMOUT=900 ; TIMEOUT=900; export TMOUT TIMEOUT**. **Visszatérési érték**: Ha a parancs nem találja a **TMOUT=15** értéket, akkor a parancsfájl kilép az 1-es értékkel. Ellenkező esetben a parancs a 0 értékkel lép ki.
164.308 (a) (5) (ii) (D) 164.312 (a) (2) (i)	Jelszókezelés (A):Jelszó létrehozási, módosítási és védelmi eljárásainak megvalósítása.	Meggyőződik róla, hogy minden jelszó minimum 14 karaktert tartalmaz.	**Parancs**: **chsec -f /etc/security/user -s user -a minlen=8**. **Visszatérési érték**: Ha sikeres, akkor a parancsfájl a 0 értékkel lép ki. Ha sikertelen, akkor a parancsfájl az 1-es hibakóddal lép ki.
164.308 (a) (5) (ii) (D) 164.312 (a) (2) (i)	Jelszókezelés (A):Jelszó létrehozási, módosítási és védelmi eljárásainak megvalósítása.	Meggyőződik róla, hogy minden jelszó tartalmaz legalább két alfabetikus karaktert, amelyek egyike nagybetűs.	**Parancs**: **chsec -f /etc/security/user -s user –a minalpha=4**. **Visszatérési érték**: Ha sikeres, akkor a parancsfájl a 0 értékkel lép ki. Ha sikertelen, akkor a parancs az 1-es hibakóddal lép ki.
164.308 (a) (5) (ii) (D) 164.312 (a) (2) (i)	Jelszókezelés (A):Jelszó létrehozási, módosítási és védelmi eljárásainak megvalósítása.	Megadja, hogy a nem alfabetikus karakterek minimális száma a jelszóban 2.	**Parancs**: **#chsec –f /etc/security/user –s user –a minother=2**. **Visszatérési érték**: Ha sikeres, akkor a parancsfájl a 0 értékkel lép ki. Ha sikertelen, akkor a parancs az 1-es hibakóddal lép ki.
164.308 (a) (5) (ii) (D) 164.312 (a) (2) (i)	Jelszókezelés (A):Jelszó létrehozási, módosítási és védelmi eljárásainak megvalósítása.	Meggyőződik róla, hogy egy jelszó sem tartalmaz ismétlődő karaktereket.	**Parancs**: **#chsec –f /etc/security/user –s user –a maxrepeats=1**. **Visszatérési érték**: Ha sikeres, akkor a parancsfájl a 0 értékkel lép ki. Ha sikertelen, akkor a parancs az 1-es hibakóddal lép ki.
164.308 (a) (5) (ii) (D) 164.312 (a) (2) (i)	Jelszókezelés (A):Jelszó létrehozási, módosítási és védelmi eljárásainak megvalósítása.	Meggyőződik róla, hogy a jelszó nincs újrafelhasználva a legutóbbi öt módosításban.	**Parancs**: **#chsec –f /etc/security/user –s user –a histsize=5**. **Visszatérési érték**: Ha sikeres, akkor a parancsfájl a 0 értékkel lép ki. Ha sikertelen, akkor a parancs az 1-es hibakóddal lép ki.
164.308 (a) (5) (ii) (D) 164.312 (a) (2) (i)	Jelszókezelés (A):Jelszó létrehozási, módosítási és védelmi eljárásainak megvalósítása.	Megadja a hetek maximális számát 13 hétben, amíg a jelszó érvényes marad.	**Parancs**: **#chsec –f /etc/security/user –s user –a maxage=8**. **Visszatérési érték**: Ha sikeres, akkor a parancsfájl a 0 értékkel lép ki. Ha sikertelen, akkor a parancs az 1-es hibakóddal lép ki.

7. táblázat: HIPAA szabályok és megvalósítási részletek (Folytatás)

HIPAA biztonsági szabály szakaszai	Megvalósítási specifikáció	Az aixpert megvalósítás	Parancsok és visszatérési értékek
164.308 (a) (5) (ii) (D) 164.312 (a) (2) (i)	Jelszókezelés (A):Jelszó létrehozási, módosítási és védelmi eljárásainak megvalósítása.	Eltávolít minden hetek minimális száma követelményt, mielőtt a jelszót módosítani lehetne.	**Parancs**: **#chsec –f /etc/security/user –s user –a minage=2**. **Visszatérési érték**: Ha sikeres, akkor a parancsfájl a 0 értékkel lép ki. Ha sikertelen, akkor a parancs az 1-es hibakóddal lép ki.
164.308 (a) (5) (ii) (D) 164.312 (a) (2) (i)	Jelszókezelés (A):Jelszó létrehozási, módosítási és védelmi eljárásainak megvalósítása.	Megadja a hetek maximális számát 4 hétben, a lejárt jelszó módosításához, miután a felhasználó által beállított **maxage** paraméter értéke lejár.	**Parancs**: **#chsec –f /etc/security/user –s user –a maxexpired=4**. **Visszatérési érték**: Ha sikeres, akkor a parancsfájl a 0 értékkel lép ki. Ha sikertelen, akkor a parancs az 1-es hibakóddal lép ki.
164.308 (a) (5) (ii) (D) 164.312 (a) (2) (i)	Jelszókezelés (A):Jelszó létrehozási, módosítási és védelmi eljárásainak megvalósítása.	Megadja a karakterek minimális számát 4 karakterben, amely nem ismétlődhet a régi jelszóból.	**Parancs**: **#chsec –f /etc/security/user –s user –a mindiff=4**. **Visszatérési érték**: Ha sikeres, akkor a parancsfájl a 0 értékkel lép ki. Ha sikertelen, akkor a parancs az 1-es hibakóddal lép ki.
164.308 (a) (5) (ii) (D) 164.312 (a) (2) (i)	Jelszókezelés (A):Jelszó létrehozási, módosítási és védelmi eljárásainak megvalósítása.	Megadja a várakozási napok számát 5 napban, mielőtt a rendszer figyelmeztetést ad ki, hogy jelszómódosítás szükséges.	**Parancs**: **#chsec –f /etc/security/user –s user –a pwdwarntime = 5**. **Visszatérési érték**: Ha sikeres, akkor a parancsfájl a 0 értékkel lép ki. Ha sikertelen, akkor a parancs az 1-es hibakóddal lép ki.
164.308 (a) (5) (ii) (D) 164.312 (a) (2) (i)	Jelszókezelés (A):Jelszó létrehozási, módosítási és védelmi eljárásainak megvalósítása.	Ellenőrzi a felhasználói meghatározások helyességét és kijavítja a hibákat.	**Parancs**: **/usr/bin/usrck -y ALL** **/usr/bin/usrck –n ALL**. **Visszatérési érték**: A parancs nem ad vissza értéket. A parancs ellenőrzi és javítja a hibát, ha van.
164.308 (a) (5) (ii) (D) 164.312 (a) (2) (i)	Jelszókezelés (A):Jelszó létrehozási, módosítási és védelmi eljárásainak megvalósítása.	Zárolja a fiókot három egymást követő sikertelen bejelentkezési kísérlet után.	**Parancs**: **#chsec –f /etc/security/user –s user –a loginretries=3**. **Visszatérési érték**: Ha sikeres, akkor a parancsfájl a 0 értékkel lép ki. Ha sikertelen, akkor a parancs az 1-es hibakóddal lép ki.
164.308 (a) (5) (ii) (D) 164.312 (a) (2) (i)	Jelszókezelés (A):Jelszó létrehozási, módosítási és védelmi eljárásainak megvalósítása.	Megadja a késleltetést egy sikertelen bejelentkezés és a következő között 5 másodpercben.	**Parancs**: **chsec -f /etc/security/login.cfg -s default -a logindelay=5**. **Visszatérési érték**: Ha sikeres, akkor a parancsfájl a 0 értékkel lép ki. Ha sikertelen, akkor a parancs az 1-es hibakóddal lép ki.

7. táblázat: HIPAA szabályok és megvalósítási részletek (Folytatás)

HIPAA biztonsági szabály szakaszai	Megvalósítási specifikáció	Az aixpert megvalósítás	Parancsok és visszatérési értékek
164.308 (a) (5) (ii) (D) 164.312 (a) (2) (i)	Jelszókezelés (A):Jelszó létrehozási, módosítási és védelmi eljárásainak megvalósítása.	Megadja a sikertelen bejelentkezési kísérletek számát a porton 10-es értékben, mielőtt a port zárolásra kerül.	**Parancs**: **chsec -f /etc/security/lastlog -s username -a \ unsuccessful_login_count=10**. **Visszatérési érték**: Ha sikeres, akkor a parancsfájl a 0 értékkel lép ki. Ha sikertelen, akkor a parancs az 1-es hibakóddal lép ki.
164.308 (a) (5) (ii) (D) 164.312 (a) (2) (i)	Jelszókezelés (A):Jelszó létrehozási, módosítási és védelmi eljárásainak megvalósítása.	Megadja a porton a sikertelen bejelentkezési kísérletekhez az időtartamot 60 másodpercben, mielőtt a port letiltásra kerül.	**Parancs**: **#chsec -f /etc/security/lastlog -s user –a time_last_unsuccessful_ login=60**. **Visszatérési érték**: Ha sikeres, akkor a parancsfájl a 0 értékkel lép ki. Ha sikertelen, akkor a parancs az 1-es hibakóddal lép ki.
164.308 (a) (5) (ii) (D) 164.312 (a) (2) (i)	Jelszókezelés (A):Jelszó létrehozási, módosítási és védelmi eljárásainak megvalósítása.	Meghatározza az időtartamot 30 percben, miután a port letiltása után a zárolás feloldása kerül.	**Parancs**: **#chsec -f /etc/security/login.cfg -s default -a loginreenable = 30**. **Visszatérési érték**: Ha sikeres, akkor a parancsfájl a 0 értékkel lép ki. Ha sikertelen, akkor a parancs az 1-es hibakóddal lép ki.
164.308 (a) (5) (ii) (D) 164.312 (a) (2) (i)	Jelszókezelés (A):Jelszó létrehozási, módosítási és védelmi eljárásainak megvalósítása.	Meghatározza az időtartamot a jelszó beírásához 30 másodpercben.	**Parancs**: **chsec -f /etc/security/login.cfg -s usw -a logintimeout=30**. **Visszatérési érték**: Ha sikeres, akkor a parancsfájl a 0 értékkel lép ki. Ha sikertelen, akkor a parancs az 1-es hibakóddal lép ki.
164.308 (a) (5) (ii) (D) 164.312 (a) (2) (i)	Jelszókezelés (A):Jelszó létrehozási, módosítási és védelmi eljárásainak megvalósítása.	Biztosítja, hogy a fiókok 35 napos inaktivitást követően zárolásra kerüljenek.	**Parancs**: **grep TMOUT= /etc/security /.profile > /dev/null 2>&1if TMOUT = (35x24x60x60){#chsec -f /etc/security/user -s user -aaccount_locked = true}**. **Visszatérési érték**: Ha a kilépési pontnak nem sikerül beállítani az **account_locked** értékét **true** értékre, akkor a parancsfájl az 1-es értékkel lép ki. Ellenkező esetben a parancs a 0 értékkel lép ki.
164.312 (c) (1)	Az irányelvek és eljárások megvalósítása az EPHI megvédése érdekében a hibás módosításokkal és megsemmisítésekkel szemben.	A megbízható végrehajtás (TE) irányelveinek beállítása ON (BE) értékre.	**Parancs**: **CHKEXEC, CHKSHLIB, CHKSCRIPT, CHKKERNEXT, STOP_ON_CHKFAIL,TE=ON bekapcsolása, például: trustchk –p TE=ON CHKEXEC = ON, CHKSHLIB,=ON, CHKSCRIPT=ON, CHKKERNEXT = ON**. **Visszatérési érték**: Hiba esetén a parancsfájl az 1-es értékkel lép ki.

7. táblázat: HIPAA szabályok és megvalósítási részletek (Folytatás)

HIPAA biztonsági szabály szakaszai	Megvalósítási specifikáció	Az aixpert megvalósítás	Parancsok és visszatérési értékek
164.312 (e) (1)	Technikai biztonsági intézkedések megvalósítása a jogosulatlan hozzáférés megakadályozása érdekében az elektronikus kommunikációs hálózaton keresztül átadott EPHI információkhoz.	Megállapítja, hogy az **ssh** fájlkészletek telepítve vannak-e. Ha nem ,akkor megjelenít egy hibaüzenetet.	**Parancs**: **# lslpp –l | grep openssh > /dev/null 2>&1**. **Visszatérési érték**: Ha a parancs visszatérési kódja a 0, akkor a parancsfájl a 0 értékkel lép ki. Ha nincs telepítve ssh fájlkészlet, akkor a parancsfájl az 1-es értékkel lép ki és megjeleníti az alábbi hibaüzenetet: Telepítse az ssh fájlkészleteket a biztonságos átvitelhez.

Az alábbi táblázat részletezi a HIPAA biztonsági szabály több funkcióját, és minden egyes funkció számos szabványt és megvalósítási specifikációt tartalmaz.

8. táblázat: HIPAA funkciók és megvalósítási részletek

HIPAA funkciók	Megvalósítási specifikáció	Az aixpert megvalósítás	Parancsok és visszatérési értékek
Hibanaplózás	Összevonja a hibákat a különböző naplókból és e-mailt küld az adminisztrátornak.	Megállapítja, hogy van-e hardverhiba. Megállapítja, hogy van-e helyreállíthatatlan hiba a **trcfile** fájlban, amely a /var/adm/ras/trcfile fájlban található. Elküldi a hibákat a **root@<hostname>** címre.	**Parancs**: **errpt -d H**. **Visszatérési érték**: Ha sikeres, akkor ez a parancs a 0 értékkel lép ki. Ha sikertelen, akkor a parancs az 1-es értékkel lép ki.
FPM engedélyezés	Fájlengedélyek módosítása.	Módosítja a fájlok engedélyeit az engedélyek és fájlok listájáról az **fpm** paranccsal.	**Parancs**: **# fpm -1 <level> -f <commands file>**. **Visszatérési érték**: Ha sikeres, akkor ez a parancs a 0 értékkel lép ki. Ha sikertelen, akkor a parancs az 1-es értékkel lép ki.
RBAC engedélyezés	Létrehozza az **isso**, **so** és **sa** felhasználót, majd hozzárendeli a megfelelő szerepeket a felhasználókhoz.	Javasolja, hogy hozza létre az **isso**, **so** és **sa** felhasználót. Hozzárendeli a megfelelő szerepeket a felhasználókhoz.	**Parancs**: **/etc/security/pscexpert/bin/RbacEnablement**.

Kapcsolódó tájékoztatás:

Az egészségbiztosítás hordozhatóságát és elszámoltathatóságát előíró törvény (HIPAA)

North American Electric Reliability Corporation megfelelés

A North American Electric Reliability Corporation (NERC) egy nonprofit vállalat, amely szabványokat fejleszt az elektromos áramellátó rendszerekhez. A PowerSC Standard Edition tartalmaz egy előre beállított NERC profilt, amely olyan biztonsági szabványokat biztosít, amelyek felhasználásával megvédheti a kritikus elektromos áramellátó rendszereket.

A NERC profil a Critical Infrastructure Protection (CIP) szabványokat követi.

A NERC profil az /etc/security/aixpert/custom/NERC.xml fájlban található. A NERC profilhoz alkalmazott CIP követelményeket visszaállíthatja az alapértelmezett állapotra a NERC_to_AIXDefault.xml profil alkalmazásával, amely az /etc/security/aixpert/custom könyvtárban található. Ez a folyamat nem egyezik meg a NERC profil visszavonási műveletével.

A következő táblázat azokról a CIP szabványokról nyújt információkat, amelyek az AIX operációs rendszerhez lettek alkalmazva, valamint arról, hogy a PowerSC Standard Edition hogyan kezeli a CIP szabványokat:

9. táblázat: PowerSC Standard Edition CIP szabványai

CIP szabvány	AIX Security Expert megvalósítás	Az értékek módosító parancsfájl helye
CIP-003-3 R5.1	Beállítja a rendszer biztonsági paramétereit a problémák megakadályozása érdekében, ehhez eltávolítja a felhasználó azonosítás beállítása (SUID) és a csoport azonosítás beállítása (SGID) attribútumokat a bináris fájlokból.	• /etc/security/pscexpert/bin/filepermgr • /etc/security/pscexpert/bin/rmsuidfrmrcmds
CIP-003-3 R5.1.1	Engedélyezi a szerep alapú hozzáférés-felügyeletet (RBAC), ehhez létrehozza a rendszeroperátor, rendszeradminisztrátor és az információs rendszer adatvédelmi megbízott felhasználói szerepet a szükséges engedélyekkel.	/etc/security/pscexpert/bin/EnableRbac
CIP-005-3a R2.1-R2.4	Engedélyezi a biztonságos parancsértelmezőt (SSH) a biztonságos hozzáféréshez.	/etc/security/pscexpert/bin/sshstart
CIP-005-3a R2.5 CIP-007-5 R1.1	Letiltja az alábbi szükségtelen és nem biztonságos szolgáltatásokat: • **lpd** démon • Egységes munkaasztali környezet (CDE)	/etc/security/pscexpert/bin/comntrows
CIP-005-3a R2.5 CIP-007-5 R1.1	Letiltja az alábbi szükségtelen és nem biztonságos szolgáltatásokat: • **timed** démon • **NTP** démon • **rwhod** démon • **DPID2** démon • DHCP ügynök	/etc/security/pscexpert/bin/rctcpip

9. táblázat: PowerSC Standard Edition CIP szabványai (Folytatás)

CIP szabvány	AIX Security Expert megvalósítás	Az értékek módosító parancsfájl helye
CIP-005-3a R2.5 CIP-007-5 R1.1	Letiltja az alábbi szükségtelen és nem biztonságos szolgáltatásokat: • **comsat** démon • **dtspcd** démon • **fingerd** démon • **ftpd** démon • **rshd** démon • **rlogind** démon • **rexecd** démon • **systat** démon • **tfptd** démon • **talkd** démon • **rquotad** démon • **rstatd** démon • **rusersd** démon • **rwalld** démon • **sprayd** démon • **pcnfsd** démon • **telnet** démon • cmsd szolgáltatás • ttdbserver szolgáltatás • TCP visszhang szolgáltatás • TCP megszüntetési szolgáltatás • TCP terhelési szolgáltatás • TCP napi időpont szolgáltatás • TCP idő szolgáltatás • UDP visszhang szolgáltatás • UDP megszüntetési szolgáltatás • UDP terhelési szolgáltatás • UDP napi időpont szolgáltatás • UDP idő szolgáltatás	/etc/security/pscexpert/bin/cominetdconf
CIP-005-3a R2.5 CIP-007-5 R1.1	Kikényszeríti a szolgáltatás megbénítása kérést a portok enyhítéséért.	/etc/security/pscexpert/bin/tcptr_aixpert
CIP-005-3a R3 CIP-007-3a R5, R6.5 CIP-007-5 R4.4	Engedélyezi a bináris fájlok megfigyelését a rendszeren.	/etc/security/pscexpert/bin/pciaudit
CIP-007-3a R3 CIP-007-5 R2.1	Megjeleníti az üzenetet a Megbízható hálózati kapcsolat (TNC) engedélyezésére.	/etc/security/pscexpert/bin/GeneralMsg
CIP-007-3a R4 CIP-007-5 R3.3	Fenntartja a rendszerintegritást a rosszindulatú szoftvertípusok észlelésével, eltávolításával.	/etc/security/pscexpert/bin/manageITsecurity
CIP-007-3a R5.2.1	Engedélyezi a jelszó módosítását első bejelentkezéskor az összes nem zárolt, alapértelmezett felhasználói fiók számára.	/etc/security/pscexpert/bin/pwdchg
CIP-007-3a R5.2.2-R5.2.3	Zárolja az összes alapértelmezett felhasználói fiókot.	/etc/security/pscexpert/dodv2/lockacc_rlogin
CIP-007-3a R5.3.1	Beállít minden egyes jelszót minimum 6 karakterre.	/etc/security/pscexpert/bin/chusrattr

9. táblázat: PowerSC Standard Edition CIP szabványai (Folytatás)

CIP szabvány	AIX Security Expert megvalósítás	Az értékek módosító parancsfájl helye
CIP-007-5 R5.5.1	Beállít minden egyes jelszót minimum 8 karakterre.	/etc/security/pscexpert/bin/chusrattr
CIP-007-3a R5.3.2 CIP-007-5 R5.5.2	Beállít minden egyes jelszót betű, numerikus és speciális karakterek kombinációjára.	/etc/security/pscexpert/bin/chusrattr
CIP-007-3a R5.3.3 CIP-007-5 R5.6	Minden egyes jelszót megváltoztat évenként.	/etc/security/pscexpert/bin/chusrattr
CIP-007-3a R7	Megjelenít egy üzenetet a Titkosított fájlrendszer (EFS) engedélyezésére.	/etc/security/pscexpert/bin/GeneralMsg
CIP-007-5 R5.7	Korlátozza a sikertelen hitelesítési kísérletek számát.	/etc/security/pscexpert/bin/chusrattr
CIP-010-1 CIP-010-2 R2.1	Megjelenít egy üzenetet a Valós idejű megfelelés (RTC) engedélyezésére.	/etc/security/pscexpert/bin/GeneralMsg

Kapcsolódó tájékoztatás:

North American Electric Reliability Corporation megfelelés

Biztonsági és megfelelési automatizálás kezelése

Megismerheti a PowerSC biztonsági és megfelelési automatizálási profilok tervezési és bevezetési folyamatát egy adott rendszercsoporton, az elfogadott IT irányítási és megfelelési eljárások szerint.

A megfelelés és az IT irányítás részeként a rendszerek hasonló terheléssel futnak, és az adatok biztonsági osztályait következetesen kell kezelni és konfigurálni. A rendszeren tervezéséhez ls telepítéséhez a rendszereken, tegye a következőket:

Rendszer munkacsoportjainak azonosítása

A megfelelés és az IT irányítás irányelvei szerint a rendszerek hasonló terhelésen futnak és az adatok biztonsági osztályait konzisztensen kell kezelni és konfigurálni. Ezért minden rendszert hasonló munkacsoportban kell azonosítani.

Nem éles tesztrendszer használata a kezdeti telepítéshez

Alkalmazza a megfelelő PowerSC megfelelési profilt a tesztrendszerhez.

Vegye figyelembe az szem előtt tart példákat a megfelelési profilok alkalmazásához az AIX operációs rendszeren.

1. példa: DoD.xml alkalmazása

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

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

Ebben a példában nincs meghiúsult szabály, azaz a Failedrules=0. Ez azt jelenti, hogy minden szabály sikeresen alkalmazásra került és a tesztelési fázis elkezdhető. Ha hiba történt, akkor a rendszer részletes kimenetel állít elő.

2. példa: PCI.xml alkalmazása hibával

```
# 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

A pci_grpck szabály meghibásodását meg kell oldani. A hiba lehetséges okai:

- A szabály nem alkalmazható a környezethez és el kell távolítani.
- Olyan probléma van a rendszeren, amelyet meg kell oldani.

Sikertelen szabály kivizsgálása

A legtöbb esetben nincs meghibásodás a PowerSC biztonsági és megfelelési profil alkalmazásakor. Azonban a rendszeren lehetnek olyan telepítéshez kapcsolódó előfeltételek, amelyek hiányoznak vagy egyéb problémák, amelyek az adminisztrátor figyelmét igénylik.

A hiba oka kivizsgálható az alábbi példa felhasználásával:

Jelenítse meg az /etc/security/aixpert/custom/PCI.xml fájlt és keresse meg a sikertelen szabályt. Ebben a példában a szabály a pci_grpck. Futtassa az **fgrep** parancsot, keresse meg a pci_grpck sikertelen szabályt, majd tekintse meg a társított XML szabályt.

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

A pci_grpck szabályból a /usr/sbin/grpck parancs látható.

Sikertelen szabály frissítése

A PowerSC biztonsági és megfelelési profil alkalmazásakor hibákba ütközhet.

A rendszeren lehetnek hiányzó telepítési előfeltételek vagy egyéb problémák, amelyek az adminisztrátor figyelmét igénylik. A sikertelen szabály alapul szolgáló parancsának meghatározása után vizsgálja meg a rendszert és keresse meg a sikertelen konfigurációs parancsot. A rendszernek lehet biztonsági problémája. Ez is lehet az oka annak, hogy egy adott szabály nem alkalmazható a rendszerkörnyezethez. Ezután létre kell hozni egy egyéni biztonsági profilt.

Egyéni biztonsági konfigurációs profil létrehozása

Ha egy szabály nem alkalmazható egy adott rendszerkörnyezethez, a legtöbb megfelelési szervezet engedélyezi a dokumentált kivételeket.

Szabály eltávolításához és egyéni biztonsági irányelv és konfigurációs fájl létrehozásához tegye a következőket:

1. Másolja a következő fájlok tartalmát egyetlen /etc/security/aixpert/custom/<*my_security_policy*>.xml nevű fájlja:

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

2. Módosítsa a <*my_security_policy*>.xml fájlt a nem alkalmazható szabály eltávolításával a nyitási XML címkéből <AIXPertEntry name... a lezáró XML címkébe </AIXPertEntry.

A biztonság érdekében további konfigurációs szabályokat is beszúrhat. A további szabályokat az XML AIXPertSecurityHardening sémába szúrja be. A PowerSC profilok nem módosíthatók közvetlenül, de személyre lehet szabni őket.

A legtöbb környezetben létre kell hozni egy egyéni XML irányelvet. Az ügyfélprofil továbbításához más rendszerekre, biztonságosan másolja az egyéni XML irányelvet arra a rendszerre, amely ugyanazt a konfigurációt igényli. Biztonságos protokoll, például a biztonságos fájlátviteli protokoll (SFTP) kerül felhasználásra az egyéni XML irányelv továbbításához más rendszerekre, és a profil a biztonságos /etc/security/aixpert/custom/<*my_security_policy.xml*>/ etc/security/aixpert/custom/ helyen kerül tárolásra.

Jelentkezzen be abba a rendszerbe, ahol az egyéni profilt létre kell hozni, majd futtassa a következő parancsot:

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

Alkalmazások tesztelése az AIX Profile Manager használatával

A biztonsági konfigurációk befolyásolhatják az alkalmazásokat, illetve a rendszer elérésének és kezelésének a módját. Fontos tesztelni az alkalmazásokat és a rendszer elvárt kezelési módszereit, mielőtt a rendszer éles környezetbe kerül telepítésre.

A szabályozó megfelelési szabványok előírják a biztonsági konfiguráció, amely szigorúbb, mint a csomagban kapható konfiguráció. A rendszer teszteléséhez tegye a következőket:

1. Az AIX Profile Manager üdvözlő oldal jobb oldali panelén válassza ki a **Profilok megjelenítése és kezelése** elemet.
2. Válassza ki a profilt, amelyet a sablon használt a megfigyelendő rendszerekre való telepítéshez.
3. Kattintson az **Összehasonlítás** elemre.
4. Válassza ki a felügyelni kívánt csoportot vagy válasszon ki egyedi rendszereket a csoportban, majd kattintson a **Hozzáadás** elemre a hozzáadáshoz a kiválasztottakhoz.
5. Kattintson az **OK** gombra.

Elkezdődik az összehasonlítási művelet.

Rendszerfigyelés az AIX Profile Manager segítségével a folyamatos megfelelés érdekében

A biztonsági konfigurációk befolyásolhatják az alkalmazásokat, illetve a rendszer elérésének és kezelésének a módját. Fontos figyelni az alkalmazásokat és a rendszer elvárt kezelési módszereit, amikor a rendszer éles környezetbe kerül telepítésre.

Az AIX Profile Manager használatához az AIX rendszer figyelésére, tegye a következőket:

1. Az AIX Profile Manager üdvözlő oldal jobb oldali panelén válassza ki a **Profilok megjelenítése és kezelése** elemet.
2. Válassza ki a profilt, amelyet a sablon használt a megfigyelendő rendszerekre való telepítéshez.
3. Kattintson az **Összehasonlítás** elemre.
4. Válassza ki a felügyelt csoportot vagy válasszon ki egyéni rendszereket a csoportban, majd adja hozzá őket a kiválasztott mezőhöz.
5. Kattintson az **OK** gombra.

Elkezdődik az összehasonlítási művelet.

PowerSC biztonság és megfelelés automatizálása szolgáltatás konfigurálása

Megismerheti a PowerSC konfigurálási eljárását a Biztonság és megfelelés automatizálása szolgáltatáshoz, az AIX Profile Manager használatával a parancssorból.

PowerSC megfelelési opciók beállításainak konfigurálása

Megismerheti a PowerSC biztonság és megfelelés automatizálása szolgáltatását, tesztelheti a konfigurációt nem éles tesztrendszereken, valamint megtervezheti és telepítheti a beállításokat. A megfelelési konfiguráció alkalmazásakor a beállítások számos konfigurációs beállítást módosítanak az operációs rendszeren.

Megjegyzés: Néhány megfelelési szabvány és profil letiltja a Telnet-et, mert a Telnet sima szöveges jelszavakat használ. Ezért a rendszeren telepítve kell lenni egy beállított, működő nyitott SSH-nak. Ezenkívül más kommunikációs eszközt is használhat a konfigurálás alatt álló rendszerhez. Ezek a megfelelési szabványok megkövetelik, hogy a root bejelentkezés tiltott legyen. Állítson be legalább egy nem root felhasználót, mielőtt folytatja a konfigurációs módosítások alkalmazását. Ez a konfiguráció nem tiltja le a root felhasználót, és bejelentkezhet nem root felhasználóként és futtathatja a **su** parancsot a root felhasználóhoz. Tesztelje, hogy létre tudja-e hozni az SSH kapcsolatot a rendszerrel, jelentkezzen be nem root felhasználóként, majd futtassa parancsot a root felhasználóhoz.

A DoD, PCI, SOX és COBIT konfigurációs profilok eléréséhez használja az alábbi könyvtárat:

- AIX operációs rendszeren a profilok az /etc/security/aixpert/custom könyvtárban találhatók.
- Virtual I/O Server (VIOS) rendszeren a profilok az /etc/security/aixpert/core könyvtárban találhatók.

PowerSC megfelelés konfigurálása a parancssorból

A megfelelési profilt a **pscxpert** paranccsal valósíthatja meg és ellenőrizheti AIX rendszeren, Virtual I/O Server (VIOS) rendszeren pedig a **viosecure** paranccsal.

A PowerSC megfelelési profilok alkalmazásához AIX rendszeren, adja ki a következő parancsok egyikét, ami az alkalmazni kívánt megfelelés szintjétől függ:

10. táblázat: PowerSC parancsok AIX rendszerhez

Parancs	Megfelelési szabvány
% pscxpert -f /etc/security/aixpert/custom/DoD.xml	*USA Department of Defense UNIX biztonságtechnikai megvalósítási kézikönyv*
% pscxpert -f /etc/security/aixpert/custom/Hipaa.xml	*Heath Insurance Portability and Accountability Act*
% pscxpert -f /etc/security/aixpert/custom/PCI.xml	*Fizetőkártya iparág - Adatbiztonsági szabvány*
% pscxpert -f /etc/security/aixpert/custom/SOX-COBIT.xml	*Sarbanes-Oxley Act of 2002 – COBIT IT Governance*

A PowerSC megfelelési profilok alkalmazásához VIOS rendszeren, adja ki az alábbi parancsok egyikét az alkalmazni kívánt biztonsági megfelelési szinthez:

11. táblázat: PowerSC parancsok Virtual I/O Server rendszerhez

Parancs	Megfelelési szabvány
% viosecure -file /etc/security/aixpert/custom/DoD.xml	*USA Department of Defense UNIX biztonságtechnikai megvalósítási kézikönyv*
% viosecure -file /etc/security/aixpert/custom/Hipaa.xml	*Heath Insurance Portability and Accountability Act*
% viosecure -file /etc/security/aixpert/custom/PCI.xml	*Fizetőkártya iparág - Adatbiztonsági szabvány*
% viosecure -file /etc/security/aixpert/custom/SOX-COBIT.xml	*Sarbanes-Oxley Act of 2002 – COBIT IT Governance*

A **pscxpert** parancs futtatása AIX rendszeren és a **viosecure** parancs futtatása VIOS rendszeren hosszú időt vehet igénybe, mert a parancsok a teljes rendszert ellenőrzik és beállítják, valamint elvégzik a biztonsággal kapcsolatos konfigurációs módosításokat. A kimenet hasonló a következő példához:

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

Azonban néhány szabály az AIX környezettől, a telepítőkészlettől és az előző konfigurációtól függően meghiúsulhat.

Például az egyik előfeltétel szabály meghiúsulhat, ha a rendszer nem rendelkezik a szükséges telepítési fájlkészlettel. Meg kell érteni minden meghibásodást és meg kell oldani, mielőtt a megfelelési profilok az egész adatközponton telepítésre kerülnek.

Kapcsolódó fogalmak:

“Biztonsági és megfelelési automatizálás kezelése” oldalszám: 85
Megismerheti a PowerSC biztonsági és megfelelési automatizálási profilok tervezési és bevezetési folyamatát egy adott rendszercsoporton, az elfogadott IT irányítási és megfelelési eljárások szerint.

PowerSC megfelelés beállítása az AIX Profile Manager használatával

Megismerheti a PowerSC biztonsági és megfelelési profilok beállítását, valamint a konfiguráció rendszerbe állítását az AIX felügyelt rendszeren az AIX Profile Manager használatával.

A PowerSC biztonsági és megfelelési profilok beállításához az AIX Profile Manager használatával, tegye a következőket:

1. Jelentkezzen be az IBM Systems Director rendszerbe, majd válassza ki az AIX Profile Manager alkalmazást.
2. Hozzon létre egy sablont az egyik PowerSC biztonsági és megfelelési profil alapján, a következő lépésekkel:
   a. Az AIX Profile Manager üdvözlőoldalának jobb oldali panelén kattintson a **Sablonok megjelenítése és kezelése** elemre.
   b. Kattintson a **Létrehozás** gombra.
   c. Kattintson az **Operációs rendszer** elemre a **Sablon típusa** listán.
   d. Adja meg a sablon nevét a **Konfigurációs sablon neve** mezőben.
   e. Kattintson a **Folytatás > Mentés** elemre.
3. Válassza ki a sablonnal használandó profilt a **Tallózás** elemre kattintva a **Válassza ki az adott sablonhoz használni kívánt profilt** beállítás alatt. A profilok megjelenítik a következő elemeket:
   - Az ice_DLS.xml az AIX operációs rendszer alapértelmezés biztonsági szintje.
   - Az ice_DoD.xml a Department of Defense biztonsági és megvalósítási kézikönyv a UNIX beállításokhoz.
   - Az ice_HLS.xml egy általános magas szintű biztonság az AIX beállításokhoz.
   - Az ice_LLS.xml egy alacsony szintű biztonság az AIX beállításokhoz.
   - Az ice_MLS.xml a közepes szintű biztonság az AIX beállításokhoz.
   - Az ice_PCI.xml a fizetőkártya iparág beállítása az AIX operációs rendszerhez.
   - Az ice_SOX.xml a SOX vagy COBIT beállítás az AIX operációs rendszerhez.
4. Távolítsa el bármelyik profilt a kiválasztott listáról.
5. A kívánt profil áthelyezéséhez a kiválasztott listára, kattintson a **Hozzáadás** gombra.
6. Kattintson a **Mentés** gombra.

A konfiguráció rendszerbe állításához az AIX felügyelt rendszeren, tegye a következőket:

1. Az AIX Profile Manager üdvözlő oldal jobb oldali panelén válassza ki a **Sablonok megjelenítése és kezelése** elemet.
2. Válassza ki a kívánt telepítendő sablont.
3. Kattintson a **Telepítés** elemre.
4. Válassza ki a rendszereket a profil telepítéséhez, majd kattintson a **Hozzáadás** gombra a kívánt profil áthelyezéséhez a kiválasztott listára.
5. A konfigurációs sablon telepítéséhez kattintson az **OK** gombra. A rendszer beállításra kerül a profil kiválasztott sablonja szerint.

Ahhoz, hogy a telepítés sikeres legyen a DoD, PCI vagy SOX követelményekhez, a PowerSC Standard Editiont az AIX rendszer végpontján kell telepíteni. Ha a rendszeren, amelyen a telepítés folyamatban van, nincs telepítve a PowerSC, akkor a telepítés meghiúsul. Az IBM Systems Director telepíti a konfigurációs sablont a kiválasztott AIX rendszer végpontjaira, majd beállítja őket a megfelelési követelmények szerint.

Kapcsolódó tájékoztatás:
AIX Profile Manager
IBM Systems Director

PowerSC Real Time Compliance

A PowerSC Real Time Compliance szolgáltatás folyamatosan figyeli a támogatással rendelkező AIX rendszereket és biztosítja, hogy konzisztensen és biztonságosan legyenek beállítva.

A PowerSC Real Time Compliance szolgáltatás a PowerSC megfelelés automatizálása és az AIX biztonsági szakértő irányelveinek kezelésével küld értesítést, ha megfelelési sértés történik, vagy ha a megfigyelt fájl módosul. Ha a rendszer biztonsági konfigurációs irányelve sérül, akkor a PowerSC Real Time Compliance szolgáltatás e-mailt vagy szöveges üzenetet küld és riasztja a rendszeradminisztrátort.

A PowerSC Real Time Compliance szolgáltatás egy passzív biztonsági szolgáltatás, amely támogatja az előre meghatározott és a módosított megfelelési profilokat, amelyek magukban foglalják a Department of Defense biztonságtechnikai megvalósítási kézikönyvet, a Fizetőkártya iparág adatbiztonsági szabványát, a Sarbanes-Oxley törvényt és a COBIT megfelelést. A szolgáltatás biztosítja a módosításokat figyelő fájlok alapértelmezett listáját, de a felhasználó is hozzáadhat fájlokat a listához.

PowerSC Real Time Compliance telepítése

A PowerSC Real Time Compliance szolgáltatás a PowerSC Standard Edition 1.1.4. vagy újabb változattal kerül telepítésre és nem része az alap AIX operációs rendszernek.

A PowerSC Standard Edition telepítéséhez tegye a következőket:

1. Győződjön meg róla, hogy az alábbi AIX operációs rendszerek egyikét futtatja azon a rendszeren, amelyen a PowerSC Standard Edition összetevőt telepíti:
   - IBM AIX 6 with Technology Level 7 vagy újabb a következővel: AIX Event Infrastructure for AIX és AIX Clusters (bos.ahafs 6.1.7.0) vagy újabb
   - IBM AIX 7 with Technology Level 1 vagy újabb a következővel: AIX Event Infrastructure for AIX és AIX Clusters (bos.ahafs 7.1.1.0) vagy újabb
   - AIX 7.2. változat vagy újabb a következővel: AIX Event Infrastructure for AIX és AIX Clusters (bos.ahafs 7.2.0.0) vagy újabb
2. A PowerSC Standard Edition összetevő fájlkészletének frissítéséhez vagy telepítéséhez telepítse a powerscStd.rtc fájlkészletet a telepítőcsomagból a PowerSC Standard Edition 1.1.4. vagy újabb változathoz.

PowerSC Real Time Compliance konfigurálása

A PowerSC Real Time Compliance beállítható riasztások küldésére, ha a megfelelési profilt megsértik, vagy ha a megfigyelt fájlban változás történik. A profilokra néhány példa többek között a Department of Defense biztonságtechnikai megvalósítási kézikönyv, a Fizetőkártya iparág adatbiztonsági szabványa, a Sarbanes-Oxley törvény és a COBIT.

A PowerSC Real Time Compliance az alábbi módszerek egyikével állítható be:

- Adja ki az **mkrtc** parancsot.
- Futtassa a SMIT eszközt a következő paranccsal:

  ```
  smit RTC
  ```

PowerSC Real Time Compliance összetevő által figyelt fájlok azonosítása

A PowerSC Real Time Compliance összetevő figyeli a fájlok alapértelmezett listájának változásait a magas szintű biztonsági beállításokból, ami személyre szabható a fájlok hozzáadásával a listához vagy az eltávolításukkal a listáról az /etc/security/rtc/rtcd_policy.conf fájlban.

A rendszeren alkalmazott megfelelési sablon azonosításának két módja van. Az egyik módszer a **pscxpert** parancs használata, a másik pedig az AIX Profile Manager és az IBM Systems Director együttes használata.

A megfelelési profil azonosításakor további fájlok adhatók hozzá a megfigyelendő fájlok listájához, további fájlok belefoglalásával az /etc/security/rtc/rtcd_policy.conf fájlba. A fájl mentése után az új lista azonnal felhasználásra kerül és elkezdődik a változások figyelése a rendszer újraindítása nélkül.

Riasztások beállítása a PowerSC Real Time Compliance összetevőhöz

Be kell állítani a PowerSC Real Time Compliance összetevő értesítését a riasztások típusának és címzettjének megadásával.

Az rtcd démon, amely a PowerSC Real Time Compliance szolgáltatás fő összetevője, lekérdezi az információkat a riasztások típusáról és a címzettjéről az /etc/security/rtc/rtcd.conf konfigurációs fájlból. Ez a fájl módosítható az információk frissítésével egy szövegszerkesztő segítségével.

Kapcsolódó tájékoztatás:

/etc/security/rtc/rtcd.conf fájlformátum a valós idejű megfeleléshez

Megbízható rendszerbetöltés

A Megbízható rendszerbetöltési szolgáltatás a Virtuális megbízható platform modult (VTPM) használja, amely a Trusted Computing Group TPM megoldásának egy virtuális példánya. A VTPM arra szolgál, hogy biztonságosa tárolja a rendszerbetöltés mérőszámait a későbbi ellenőrzéshez.

Megbízható rendszerbetöltés - alapelvek

Fontos megérteni a rendszerbetöltési folyamat integritását, valamint azt, hogy a rendszerbetöltés minek alapján minősül megbízható vagy megbízhatatlan rendszerbetöltésnek.

Legfeljebb 60 VTPM használatára felkészített logikai partíció (LPAR) konfigurálható az egyes fizikai rendszerekhez, a Hardverkezelő konzol (HMC) használatával. A konfiguráláskor a VTPM minden LPAR esetén egyedi. Az AIX Megbízható végrehajtás technológiával használva a VTPM biztonságot és garanciát biztosít a következő partíciókhoz:

- A lemezen lévő rendszerbetöltési képfájl
- A teljes operációs rendszer
- Az alkalmazás rétegek

Egy adminisztrátor egy központi konzolról tekintheti meg a megbízható és megbízhatatlan rendszereket, amely az AIX kiterjesztéscsomagban elérhető **openpts** ellenőrzővel van telepítve. Az **openpts** konzol kezeli a Power Systems szervereket, és megfigyeli vagy hitelesíti az adatközpontban lévő AIX Profile Manager rendszerek megbízható állapotát. A hitelesítés az a folyamat, melynek során az ellenőrző megállapítja (vagy hitelesíti), hogy egy adatgyűjtő megbízható rendszerbetöltést hajtott-e végre.

Megbízható rendszerbetöltés állapota

Egy partíció akkor mondható megbízhatónak, ha az ellenőrző sikeresen hitelesíti az adatgyűjtő integritását. Az ellenőrző a távoli partíció, amely megállapítja, hogy az adatgyűjtő egy megbízható rendszerbetöltést hajtott-e végre. Az adatgyűjtő az az AIX partíció, amelyhez csatolva van egy Virtuális megbízható platform modul (VTPM), és amelyen a Megbízható szoftver verem (TSS) telepítve van. Jelzi, hogy a VTPM modulon belül rögzített mérőszámok megfelelnek-e egy ellenőrző által fenntartott referenciakészletnek. Egy megbízható rendszerbetöltési állapot azt jelzi, hogy a partíció megbízható módon lett-e betöltve. Ez az állítás a rendszerbetöltési folyamat integrációjára vonatkozik, és nem jelzi a rendszer biztonságának aktuális vagy folyamatban lévő szintjét.

Nem megbízható rendszerbetöltési állapot

Egy partíció akkor lesz megbízhatatlan állapotú, ha az ellenőrző nem tudta sikeresen hitelesíteni a rendszerbetöltési folyamat integritását. A megbízhatatlan állapot azt jelzi, hogy a rendszerbetöltési folyamat néhány aspektusa nem konzisztens az ellenőrző által fenntartott referencia információkkal. Egy sikertelen hitelesítés lehetséges okai közé tartozik a rendszerbetöltés egy eltérő rendszerbetöltési eszközről, egy eltérő kernel képfájlból, illetve a meglévő rendszerbetöltési képfájl módosítása.

Kapcsolódó fogalmak:

“Megbízható rendszerbetöltés hibaelhárítása” oldalszám: 97
A Megbízható rendszerbetöltés használatakor van néhány általános forgatókönyv és kiigazító lépés, amelyek segítenek a hitelesítési hiba okának azonosításában.

Megbízható rendszerbetöltés tervezése

A Megbízható rendszerbetöltés telepítéséhez szükséges hardver- és szoftverkonfigurációval kapcsolatos információk.

Megbízható rendszerbetöltés - előfeltételek

A Megbízható rendszerbetöltés telepítése az adatgyűjtő és az ellenőrző konfigurálását foglalja magában.

Amikor egy olyan rendszeren készíti elő az AIX operációs rendszer újratelepítését, amelyen már telepítve van a Megbízható rendszerbetöltés, át kell másolnia a /var/tss/lib/tpm/system.data fájlt, és az újratelepítés befejeződése után felül kell írnia ezzel az azonos helyen található fájlt. Ha nem másolja ezt a fájlt, akkor a virtualizált Megbízható platform modult el kell távolítania a felügyeleti konzolból, és újra kell telepítenie a partíción.

Adatgyűjtő

Egy adatgyűjtő telepítésének konfigurációs követelményei a következő előfeltételeket jelentik:

- 740-es firmware kiadáson futó POWER7 hardver.
- IBM AIX 6 with Technology Level 7 vagy IBM AIX 7 with Technology Level 1 telepítése.
- Hardverkezelő konzol (HMC) 7.4 vagy újabb változat telepítése.
- A partíció konfigurálása a VTPM használatával, és legalább 1 GB memória.
- Secure Shell (SSH), különösen az OpenSSH vagy ezzel egyenértékű telepítése.

Ellenőrző

Az **openpts** ellenőrző a parancssori felületről és többféle platformon való futtatásra tervezett grafikus felhasználói felületről érhető el. Az OpenTPS ellenőrző AIX változata az AIX kiterjesztéscsomagban érhető el. Az OpenPTS ellenőrző Linux és egyéb platformokra készült változatai webes letöltéssel szerezhetők be. A konfigurációs követelmények a következő előfeltételeket tartalmazzák:

- SSH, különösen az OpenSSH vagy ezzel egyenértékű telepítése.
- Hálózati kapcsolat létesítése (SSH használatával) az adatgyűjtővel.
- Java™ 1.6 vagy újabb változat telepítése az **openpts** konzol eléréséhez a grafikus felületről.

Felkészülés a kiigazításra

Az itt leírt Megbízható rendszerbetöltési információk iránymutatásként szolgálnak azon helyzetek azonosításához, amelyek kiigazítást igényelhetnek. Ez nincs hatással a rendszerbetöltési folyamatra.

Számos olyan körülmény lehet, amely a hitelesítés sikertelenségét okozhatja, és nehéz előre megmondani, hogy milyen körülményekkel találkozhat. A megfelelő műveletet a körülményektől függően kell kiválasztania. Azonban jó gyakorlat felkészülni néhány súlyos forgatókönyvre, és kialakítani egy irányelvet vagy munkafolyamatot, amely segítséget nyújt az ilyen incidensek kezelésében. A kiigazítás az a javító művelet, amelyet akkor kell elvégezni, amikor a hitelesítés azt jelenti, hogy néhány adatgyűjtő nem megbízható.

Például, ha egy hitelesítési hiba történt, mert a rendszerbetöltési képfájl eltér az ellenőrző referenciájától, gondolja át, hogy milyen válaszokat adna a következő kérdésekre:

- Hogyan ellenőrizheti, hogy a fenyegetettség hitelt érdemlő?
- Történt bármilyen tervezett karbantartás, AIX frissítés, vagy volt telepítve nemrégiben új hardver?
- Kapcsolatba tud lépni az adminisztrátorral, akinek van hozzáférése ezekhez az információkhoz?
- Mikor volt a rendszer legutóbb betöltve megbízható állapotban?
- Ha a biztonsági fenyegetettség szabályszerűnek tűnik, akkor mit kell tennie? (A javaslatok közé tartozik a megfigyelési naplók összegyűjtése, a rendszer leválasztása a hálózatról, a rendszer kikapcsolása, illetve a felhasználók figyelmeztetése).
- Más rendszerek is veszélyeztetve voltak, amelyeket ellenőrizni kell?

Kapcsolódó fogalmak:

“Megbízható rendszerbetöltés hibaelhárítása” oldalszám: 97
A Megbízható rendszerbetöltés használatakor van néhány általános forgatókönyv és kiigazító lépés, amelyek segítenek a hitelesítési hiba okának azonosításában.

Áttérési szempontok

Fontolja meg a következő előfeltételeket, mielőtt átállítana egy Virtuális megbízható platform modul (VTPM) támogatással rendelkező partíciót.

A VTPM előnye egy fizikai TPM modullal szemben az, hogy lehetővé teszi a partíció rendszerek közötti áthelyezését a VTPM megtartásával. A logikai partíció biztonságos átállításához a firmware átvitel előtt titkosítja a VTPM adatokat. A biztonságos átállítás biztosítása érdekében a következő biztonsági intézkedéseket kell megvalósítani az átállítás előtt:

- IPSEC engedélyezése az átállítást végrehajtó Virtual I/O Server (VIOS) rendszeren.
- A megbízható rendszer kulcs beállítása a Hardverkezelő konzolon (HMC) keresztül a VTPM adatok átállítás utáni visszafejtésére képes felügyelt rendszerek vezérléséhez. Az adatok sikeres átállításához az áttérés célrendszerének rendelkeznie kell a forrásrendszeren lévő kulcsnak megfelelő kulccsal.

Kapcsolódó tájékoztatás:

HMC használata

VIOS átállítás

Megbízható rendszerbetöltés telepítése

A Megbízható rendszerbetöltés telepítéséhez szükségesek bizonyos hardver- és szoftverkonfigurációk.

Kapcsolódó tájékoztatás:

“PowerSC Standard Edition telepítése” oldalszám: 7
A PowerSC Standard Edition minden egyes adott funkciójához telepítenie kell egy fájlkészletet.

Az adatgyűjtő telepítése

Az adatgyűjtőt az AIX alap CD lemezen található fájlkészlet használatával kell telepítenie.

Az adatgyűjtő telepítéshez telepítse az alap CD-n található powerscStd.vtpm és openpts.collector csomagokat az **smit** vagy az **installp** parancs használatával.

Az ellenőrző telepítése

Az OpenPTS ellenőrző összetevő AIX operációs rendszeren és más platformokon is fut.

Az ellenőrző AIX változata a fájlkészletből telepíthető, az AIX kiterjesztéscsomag használatával. Az ellenőrző telepítéséhez AIX operációs rendszeren, telepítse az openpts.verifier csomagot az AIX kiterjesztéscsomagból az **smit** vagy **installp** parancs futtatásával. Ez egyaránt telepíti az ellenőrző parancssori és grafikus felülettel rendelkező változatát.

A más operációs rendszereken használható OpenPTS ellenőrző a Linux OpenPTS ellenőrző letöltése az AIX Megbízható rendszerbetöltési összetevőhöz útvonalról tölthető le.

Kapcsolódó tájékoztatás:

Linux OpenPTS ellenőrző letöltése az AIX Megbízható rendszerbetöltéssel való használathoz

---

Megbízható rendszerbetöltés konfigurálása

Egy rendszer Megbízható rendszerindítás összetevőbe történő bejegyzéséhez és hitelesítéséhez szükséges eljárás bemutatása.

Rendszer bejegyzése

Megismerheti az eljárást, amellyel bejegyezhet egy rendszert az ellenőrzőhöz.

Egy rendszer bejegyzése az a folyamat, amikor megadja a mérőszámok kezdeti készletét az ellenőrző számára, ami a soron következő hitelesítési kérések alapjául szolgál. Egy rendszer bejegyzéséhez a parancssorból, használja a következő parancsot az ellenőrzőből:

```
openpts -i <hosztnév>
```

A bejegyzett partícióval kapcsolatos információk a $HOME/.openpts könyvtárban találhatók. A bejegyzési folyamat során minden egyes új partícióhoz hozzá van rendelve egy egyedi azonosító, és a bejegyzett partíciókkal kapcsolatos információk az egyedi azonosítónak megfelelő könyvtárban vannak tárolva.

Egy rendszer bejegyzéséhez a grafikus felületről, tegye a következőket:

1. Indítsa el a grafikus felületet az **/opt/ibm/openpts_gui/openpts_GUI.sh** parancs segítségével.
2. A navigációs menüből válassza ki a **Bejegyzés** menüpontot.
3. Adja meg a rendszer hosztnevét és SSH hitelesítő adatait.
4. Kattintson a **Bejegyzés** lehetőségre.

Kapcsolódó fogalmak:

“Rendszer hitelesítése”
Megismerheti az eljárást, amellyel egy rendszert a parancssorból vagy a grafikus felület használatával hitelesíthet.

Rendszer hitelesítése

Megismerheti az eljárást, amellyel egy rendszert a parancssorból vagy a grafikus felület használatával hitelesíthet.

Egy rendszerbetöltés integritásának lekérdezéséhez használja a következő parancsot az ellenőrzőből:

```
openpts <hosztnév>
```

Egy rendszer hitelesítéséhez a grafikus felületről, tegye a következőket:

1. Válasszon ki egy kategóriát a navigációs menüből.
2. Válassza ki a hitelesítendő rendszer(eke)t.
3. Kattintson a **Hitelesítés** lehetőségre.

Rendszer bejegyzése és hitelesítése jelszó nélkül

A hitelesítési kérés elküldése Secure Shell (SSH) protokollon keresztül történik. Telepítse az ellenőrző tanúsítványát az adatgyűjtőn, hogy engedélyezze az SSH kapcsolatok jelszó nélküli használatát.

Az ellenőrző tanúsítványának beállításához az adatgyűjtő rendszerén tegye a következőket:

- Az ellenőrzőn futtassa a következő parancsokat:

  ```
  ssh-keygen    # Nincs jelmondat
  scp ~/.ssh/id_rsa.pub <adatgyűjtő>:/tmp
  ```

- Az adatgyűjtőn futtassa a következő parancsot:

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

Megbízható rendszerbetöltés kezelése

A Megbízható rendszerbetöltés hitelesítési eredményeinek kezeléséhez szükséges eljárás bemutatása.

Hitelesítési eredmények értelmezése

A hitelesítési eredmények megtekintéséhez és megértéséhez szükséges eljárás bemutatása.

A hitelesítés eredménye a következő állapotok egyike lehet:

1. A hitelesítési kérés meghiúsult: A hitelesítési kérés nem fejeződött be sikeresen. A hiba lehetséges okainak megértéséhez tekintse meg a Hibaelhárítás szakaszt.

2. A rendszerintegritás érvényes: A hitelesítés sikeresen befejeződött, és a rendszerbetöltés megfelel az ellenőrző által fenntartott referencia információknak. Ez egy sikeres Megbízható rendszerbetöltést jelez.
3. A rendszerintegritás érvénytelen: A hitelesítési kérés befejeződött, azonban ellentmondás található a rendszerindítás során gyűjtött információk és az ellenőrző által fenntartott referencia információk között. Ez egy nem megbízható rendszerbetöltés jelez.

A hitelesítés a következő üzenettel jelenti azt is, hogy az adatgyűjtőre lett-e alkalmazva frissítés:

Rendszerfrissítés elérhető: Ez az üzenet azt jelzi, hogy az adatgyűjtőre alkalmazva lett egy frissítés, és elérhető a frissített referencia információk halmaza, amely a következő rendszerbetöltésnél lesz hatályos. A felhasználó az ellenőrzőn felszólítást kap a frissítések elfogadására vagy visszautasítására. Például a felhasználó dönthet úgy, hogy elfogadja ezeket a frissítéseket, ha tud az adatgyűjtőn történő karbantartásról.

Egy hitelesítési hiba kivizsgálásához a grafikus felületről, tegye a következőket:

1. Válasszon ki egy kategóriát a navigációs menüből.
2. Válassza ki a kivizsgálni kívánt rendszert.
3. Kattintson duplán a rendszernek megfelelő bejegyzésre. Megjelenik egy tulajdonság ablak. Ez az ablak tartalmazza a meghiúsult hitelesítés naplóinformációit.

Rendszerek törlése

Megismerheti az eljárást, amellyel törölhet egy rendszert az ellenőrző adatbázisából.

Egy rendszer eltávolításához az ellenőrző adatbázisából, futtassa a következő parancsot:

```
openpts -r <hosztnév>
```

Megbízható rendszerbetöltés hibaelhárítása

A Megbízható rendszerbetöltés használatakor van néhány általános forgatókönyv és kiigazító lépés, amelyek segítenek a hitelesítési hiba okának azonosításában.

Az **openpts** parancs akkor határoz meg érvénytelenként egy rendszert, ha a rendszer aktuális rendszerbetöltési állapota nem felel meg az ellenőrzőn fenntartott referencia információknak. Az **openpts** parancs megállapítja a lehetséges okot, ami miatt az integritás érvénytelen lehet. Egy teljes AIX rendszerbetöltés során számos változó létezik, és egy sikertelen hitelesítés esetén a hiba okának megállapításához elemzés szükséges.

A következő táblázat felsorolja a hiba okának azonosításához szükséges általános forgatókönyveket és kiigazító lépéseket:

12. táblázat: Néhány hiba forgatókönyv hibaelhárítása

Hiba jellege	Hiba lehetséges okai	Javasolt kiigazítás

A hitelesítés nem fejeződött be.	• Helytelen hosztnév.
	• Nincs hálózati útvonal a forrás és a cél között.
	• Helytelen biztonsági hitelesítő adatok.
		Ellenőrizze a Secure Shell (SSH) kapcsolatot a következő parancs használatával:
		`ssh ptsc@hosztnév`
		
		Ha az SSH kapcsolat sikeres, akkor ellenőrizze a hitelesítési hiba következő okait:
		• A hitelesítendő rendszeren nem fut a **tcsd** démon.
		• A hitelesítendő rendszer nem lett inicializálva a **ptsc** paranccsal. Ez a folyamat elvileg automatikusan megtörténik a rendszerindítás során, azonban ellenőrizze, hogy létezik-e egy /var/ptsc/ könyvtár az adatgyűjtőn. Ha a /var/ptsc/ könyvtár nem létezik, akkor futtassa az adatgyűjtőn a következő parancsot:
		`ptsc -i`

12. táblázat: Néhány hiba forgatókönyv hibaelhárítása (Folytatás)

Hiba jellege	Hiba lehetséges okai	Javasolt kiigazítás
A CEC firmware megváltozott.	• Alkalmazva lett egy firmware frissítés. • Az LPAR át lett állítva egy olyan rendszerre, amely a firmware egy eltérő változatát futtatta.	Ellenőrizze a logikai partíciót (LPAR) tartalmazó rendszer firmware szintjét.
Az LPAR számára lefoglalt erőforrások megváltoztak.	Az LPAR számára lefoglalt CPU vagy memória megváltozott.	Ellenőrizze a partíció profilt a HMC konzolban.
A logikai partícióban elérhető adapterekhez tartozó firmware megváltozott.	A logikai partícióhoz hozzá lett adva vagy onnan el lett távolítva egy hardver eszköz.	Ellenőrizze a partíció profilt a HMC konzolban.
A logikai partícióhoz csatlakoztatott eszközök listája megváltozott.	A logikai partícióhoz hozzá lett adva vagy onnan el lett távolítva egy hardver eszköz.	Ellenőrizze a partíció profilt a HMC konzolban.
Az operációs rendszer kernelt tartalmazó rendszerbetöltési képfájl megváltozott.	• Egy AIX frissítés lett alkalmazva, és az ellenőrző nem tudott a frissítésről. • Lefutott a **bosboot** parancs.	• Ellenőrizze az adatgyűjtő adminisztrátorával, hogy történt-e bármilyen karbantartási tevékenység a legutóbbi újrabetöltési művelet előtt. • Keressen az adatgyűjtő naplóiban karbantartásra utaló tevékenységet.
A logikai partíció egy másik eszközről lett betöltve.	• Közvetlenül a hálózat telepítése után bejegyzés lett végrehajtva. • A rendszer egy karbantartó eszközről van betöltve.	A rendszerbetöltő eszköz és kapcsolók a **bootinfo** parancs használatával ellenőrizhetők. Ha közvetlenül a Hálózati telepítéskezelő (NIM) telepítése után és az újrabetöltési művelet előtt bejegyzés történt, akkor a bejegyzett részletek a hálózati telepítéshez tartoznak, nem pedig a következő lemezbetöltéshez. Ez a bejegyzés a bejegyzés eltávolításával és a logikai partíció ismételt bejegyzésével javítható.
Az Interaktív rendszerfelügyeleti szolgáltatások (SMS) rendszerbetöltési menü meghívásra került.		A rendszerbetöltési folyamatnak megszakítás és felhasználói interakció nélkül kell lefutnia ahhoz, hogy egy rendszer megbízható legyen. Az SMS rendszerbetöltési menü érvénytelenné teszi a rendszerbetöltést.
A Megbízható végrehajtás (TE) adatbázis módosítva lett.	• Bináris fájlok lettek hozzáadva vagy eltávolítva a TE adatbázisból. • Az adatbázisban lévő bináris fájlok frissítve lettek.	Futtassa a **trustchk** parancsot az adatbázis ellenőrzéséhez.

Kapcsolódó fogalmak:

“Felkészülés a kiigazításra” oldalszám: 94
Az itt leírt Megbízható rendszerbetöltési információk iránymutatásként szolgálnak azon helyzetek azonosításához, amelyek kiigazítást igényelhetnek. Ez nincs hatással a rendszerbetöltési folyamatra.

“Megbízható rendszerbetöltés - alapelvek” oldalszám: 93
Fontos megérteni a rendszerbetöltési folyamat integritását, valamint azt, hogy a rendszerbetöltés minek alapján minősül megbízható vagy megbízhatatlan rendszerbetöltésnek.

Kapcsolódó tájékoztatás:

HMC használata

Megbízható tűzfal

A Megbízható tűzfal szolgáltatás virtualizációs réteg biztonságot nyújt, ami javítja a teljesítményt és az erőforrások hatékonyságát azonos Power Systems szerveren lévő két különböző virtuális LAN (VLAN) biztonsági zónák kommunikációja során. A Megbízható tűzfal csökkenti a külső hálózat terhelését azáltal, hogy adott szabályoknak megfelelő tűzfalcsomagok szűrésének képességét áthelyezi a virtualizációs rétegbe. Ezt a szűrési képességet könnyen meghatározható hálózati szűrőszabályok vezérlik, amelyek a virtuális környezet elhagyása nélkül teszik lehetővé a megbízható hálózati forgalom kereszteződését a VLAN biztonsági zónák között. A Megbízható tűzfal védi és továbbítja az AIX, IBM i és Linux operációs rendszerek közötti belső hálózati forgalmat.

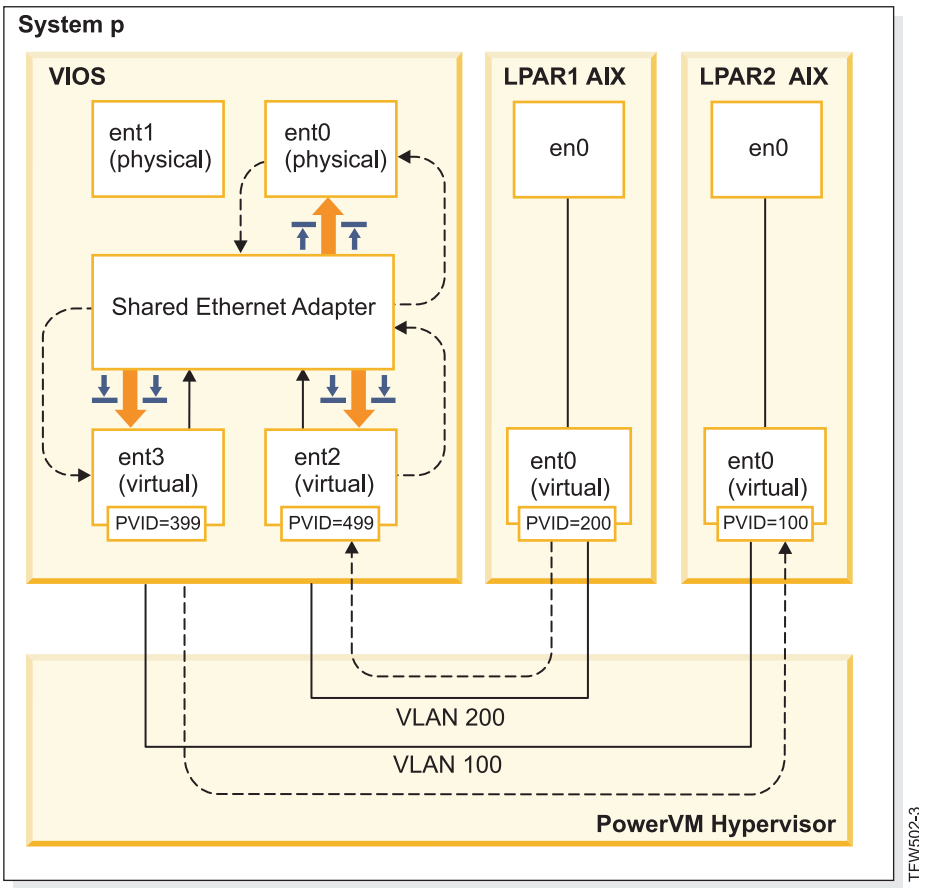
Megbízható tűzfal - alapelvek

A Megbízható tűzfal használatakor van néhány alapelv, amit fontos megérteni.

A Power Systems hardver több virtuális LAN (VLAN) biztonsági zónával konfigurálható. Egy felhasználó által konfigurált, Megbízható tűzfal szűrőszabályként létrehozott irányelv engedélyezi a megbízható hálózati forgalom számára, hogy keresztezzen VLAN biztonsági zónákat, és közben a virtualizációs rétegen belül maradjon. Ez hasonló egy hálózatra csatlakozó fizikai tűzfal bevezetéséhez a virtuális környezetben, ami teljesítmény tekintetében hatékonyabb módszert biztosít tűzfal képességek megvalósítására virtualizált adatközpontok esetén.

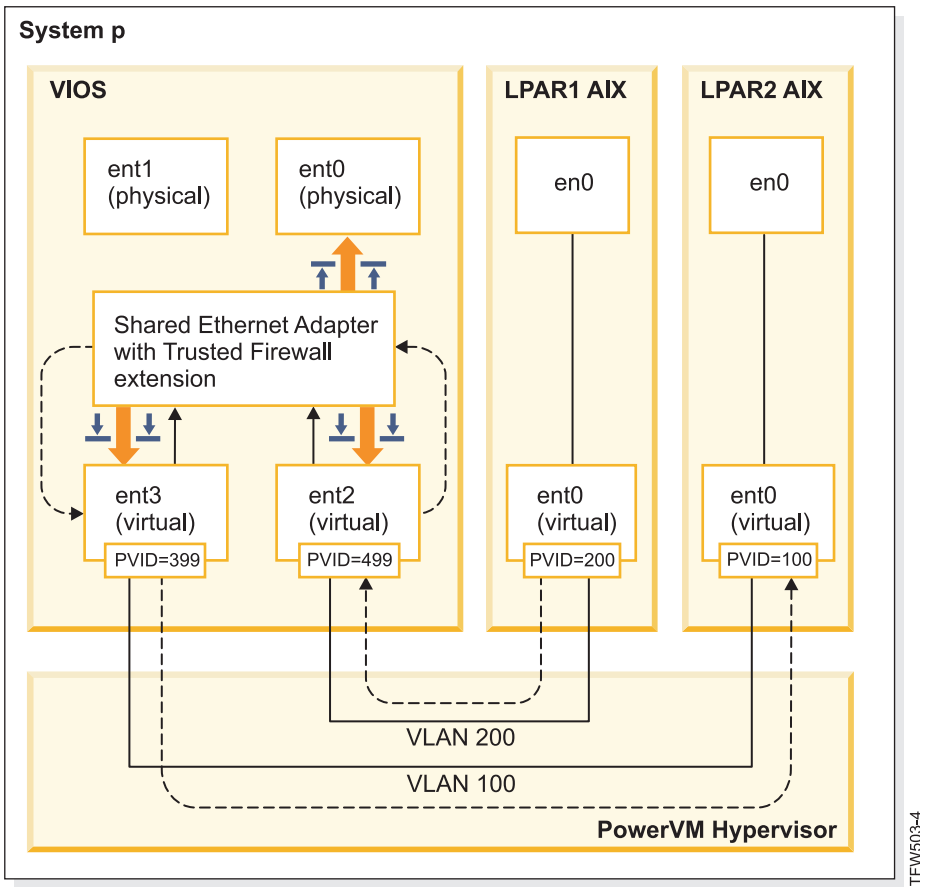
A Megbízható tűzfal lehetővé teszi szabályok konfigurálását, hogy bizonyos típusú forgalom közvetlenül átvitele engedélyezve legyen a Virtual I/O Serveren (VIOS) lévő egyik VLAN hálózatról egy azonos VIOS szerveren lévő másik VLAN hálózatba, miközben más típusú forgalom korlátozásával továbbra is fenntartható a magas szintű biztonság. Ez egy konfigurálható tűzfal a Power Systems szerverek virtualizációs rétegén belül.

Az alábbi ábrán (1. ábra: oldalszám: 100) bemutatott példa használatával, a cél az, hogy az információk átvitele biztonságosan és hatékonyan történjen a VLAN 200 hálózaton lévő LPAR1 egy és a VLAN 100 hálózaton lévő LPAR2 között. A Megbízható tűzfal nélkül az LPAR1 partícióról az LPAR2 partícióra irányuló információk a belső hálózatról az útválasztónak vannak kiküldve, amely továbbítja az információkat vissza az LPAR2 partícióra.



1. ábra: Példa a VLAN hálózatok közötti információk átvitelére a Megbízható tűzfal nélkül

A Megbízható tűzfal használatával konfigurálhat szabályokat, hogy az információk az LPAR1 partícióról az LPAR2 partícióra a belső hálózat elhagyása nélkül mehessenek át. Ez az útvonal látható a következő helyen is: 2. ábra: oldalszám: 101.



2. ábra: Példa a VLAN hálózatok közötti információk átvitelére a Megbízható tűzfalon keresztül

A konfigurációs szabályok, amelyek lehetővé teszik bizonyos információk biztonságos átvitelét a VLAN hálózatok között, lerövidítik az információk céljához vezető útvonalat. A Megbízható tűzfal a Megosztott Ethernet adapter (SEA) és a Biztonságos virtuális gép (SVM) kernel kiterjesztéseket használja a kommunikáció megvalósításához.

Megosztott Ethernet Adapter
A SEA az a hely, ahol az útválasztás kezdődik és végződik. Az SVM regisztrálásakor a SEA fogadja a csomagokat, és továbbítja azokat az SVM felé. Ha az SVM azt állapítja meg, hogy a csomag egy azonos Power Systems szerveren lévő LPAR partícióra irányul, akkor frissíti a csomag 2-es réteghez tartozó fejlécét. A csomagot visszaküldi a SEA számára, hogy továbbítsa azt a végső célnak a rendszeren belül vagy a külső hálózatba.

Biztonságos virtuális gép
Az SVM az a hely, ahol a szűrőszabályok alkalmazásra kerülnek. A szűrőszabályok a belső hálózat biztonságának fenntartásához szükségesek. Miután az SVM regisztrálva lett a SEA adapterrel, a csomagok az SVM számára lesznek továbbítva, mielőtt elküldésre kerülnének a külső hálózatra. Az SVM az aktív szűrőszabályok alapján megállapítja, hogy egy csomag a belső hálózaton marad-e, vagy pedig a külső hálózatra kell továbbítani.

Megbízható tűzfal telepítése

A PowerSC Megbízható tűzfal telepítése hasonló a többi PowerSC szolgáltatás telepítéséhez.

Előfeltételek:

- A PowerSC 1.1.1.0 változatnál korábbi kiadásai nem rendelkeznek a Megbízható tűzfal telepítéséhez szükséges fájlkészlettel. Győződjön meg róla, hogy a PowerSC telepítő CD az 1.1.1.0 vagy újabb változathoz tartozik.

- A Megbízható tűzfal előnyeinek kihasználásához már használnia kellett a Hardverkezelő konzolt (HMC) vagy a Virtual I/O Servert (VIOS) a Virtuális LAN (VLAN) hálózatok konfigurálásához.

A Megbízható tűzfal egy kiegészítő fájlkészletként szerepel a PowerSC Standard Edition telepítő CD-n. A fájl neve powerscStd.svm.rte. A Megbízható tűzfal hozzáadható a PowerSC 1.1.0.0 vagy újabb változat egy meglévő példányához, vagy telepítheti a PowerSC 1.1.1.0 vagy újabb változat új telepítésének részeként.

A Megbízható tűzfal funkció hozzáadásához egy meglévő PowerSC példányhoz:

1. Győződjön meg róla, hogy VIOS 2.2.1.4 vagy újabb változatot futtat.
2. Helyezze be a PowerSC 1.1.1.0 változathoz tartozó telepítő CD-t, vagy töltse le a telepítő CD képfájlját.
3. Root hozzáféréshez használja az **oem_setup_env** parancsot.
4. Az **installp** parancs vagy az SMIT eszköz használatával telepítse a PowerscStd.svm.rte fájlkészletet.

Kapcsolódó tájékoztatás:

“PowerSC Standard Edition telepítése” oldalszám: 7
A PowerSC Standard Edition minden egyes adott funkciójához telepítenie kell egy fájlkészletet.

Megbízható tűzfal konfigurálása

A Megbízható tűzfal szolgáltatás a telepítése után további konfigurációs beállítások megadását igényli.

Megbízható tűzfal tanácsadó

A Megbízható tűzfal tanácsadó elemzi a rendszeren a különböző logikai partíciókról (LPAR) kiinduló forgalmat, hogy információkat biztosítson annak megállapításához, hogy a Megbízható tűzfal futtatása javítja-e a rendszer teljesítményét.

Ha a Megbízható tűzfal tanácsadó funkció jelentős mennyiségű forgalmat rögzít azonos központi elektronikus komplexumon belül lévő különböző virtuális LAN (VLAN) hálózatokról, akkor a Megbízható tűzfal engedélyezése jó hatással lehet a rendszerre.

A Megbízható tűzfal tanácsadó engedélyezéséhez adja ki a következő parancsot:

```
vlantfw -m
```

A Megbízható tűzfal tanácsadó eredményeinek megtekintéséhez írja be a következő parancsot:

```
vlantfw -D
```

A Megbízható tűzfal tanácsadó letiltásához adja ki a következő parancsot:

```
vlantfw -M
```

Megbízható tűzfal naplózás

A Megbízható tűzfal naplózás összegyűjti a központi elektronikus komplexumon belüli hálózati forgalom útvonalainak listáját. A lista megjeleníti a szűrőket, amelyeket a Megbízható tűzfal a forgalom továbbításához használ.

Amikor a Megbízható tűzfal tanácsadó megállapítja, hogy a forgalom belső továbbítása növeli a hatékonyságot, a Megbízható tűzfal naplózás karbantartja az útvonalak listáját az svm.log fájlban. Az svm.log fájl mérete legfeljebb 16 MB lehet. Ha a bejegyzések meghaladják a 16 MB-os korlátot, akkor a legrégebbi bejegyzések eltávolításra kerülnek a naplófájlból.

A Megbízható tűzfal naplózás elindításához adja ki a következő parancsot:

```
vlantfw -l
```

A Megbízható tűzfal naplózás leállításához adja ki a következő parancsot:

```
vlantfw -L
```

A naplófájlt a következő helyen tekintheti meg: /home/padmin/svm/svm.log.

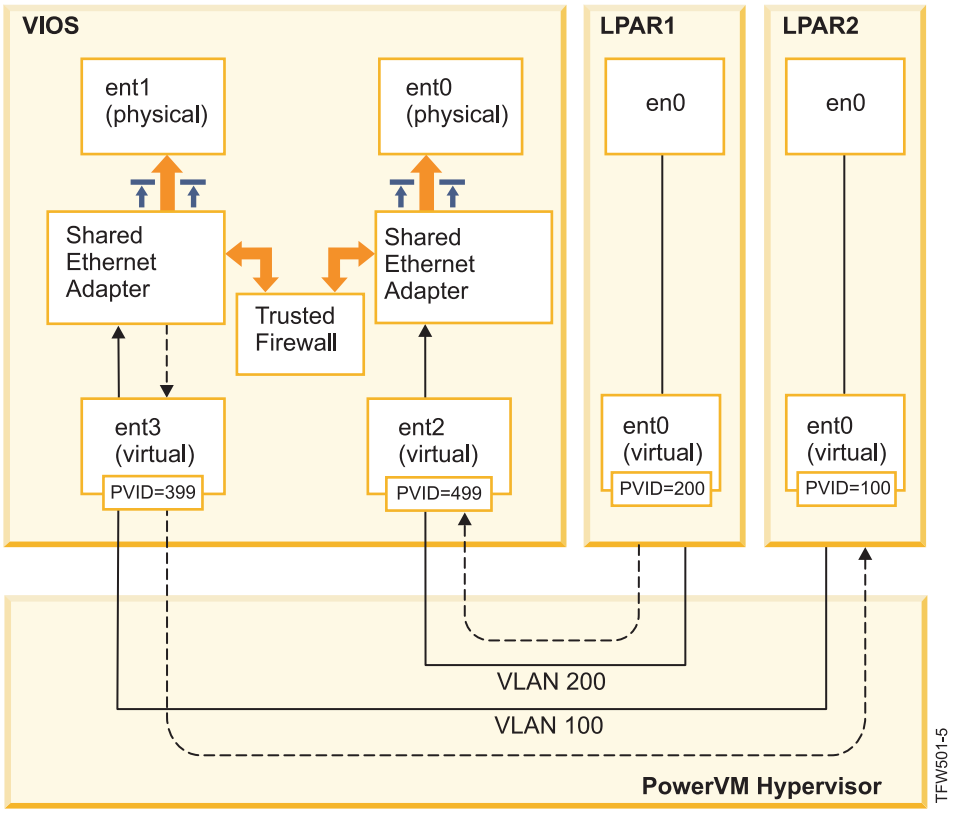
Megjegyzés: Csak abban az esetben futtathat parancsokat a megbízható tűzfal naplózás indítására és leállítására, ha root felhasználóként hitelesített a rendszerre.

Több Megosztott Ethernet adapter

A Megbízható tűzfal konfigurálható több Megosztott Ethernet adaptert használó rendszereken.

Bizonyos konfigurációk több Megosztott Ethernet adaptert (SEA) használnak egyazon Virtual I/O Serveren (VIOS). Több SEA használata biztosítja az átállási védelem és az erőforrás szintek beállításának előnyeit. A Megbízható tűzfal támogatja az útválasztást több SEA között, feltéve, hogy ezek mind egyazon VIOS szerveren vannak.

A következő ábrán egy több SEA adaptert használó környezet látható: 3. ábra:.



3. ábra: Egyetlen VIOS szerveren több Megosztott Ethernet adaptert használó konfiguráció

A következő példák a Megbízható tűzfal által támogatott több SEA konfigurációt mutatják be:

- A SEA adapterek csonk adapterekkel vannak konfigurálva egyazon Power hypervisor virtuális kapcsolón. Ez a konfiguráció azért támogatott, mert minden egyes SEA eltérő VLAN azonosítókkal fogadja a hálózati forgalmat.
- A SEA adaptere eltérő Power hypervisor virtuális kapcsolókon lévő csonk adapterekkel vannak konfigurálva, és minden csonk adapter egy eltérő VLAN azonosítójú VLAN hálózaton található. Ebben a konfigurációban minden egyes SEA továbbra is eltérő VLAN azonosítókkal fogadja a hálózati forgalmat.
- A SEA adaptere eltérő Power hypervisor virtuális kapcsolókon lévő csonk adapterekkel vannak konfigurálva, és ugyanazok a VLAN azonosítók kerülnek újrafelhasználásra a virtuális kapcsolókon. Ebben az esetben a forgalomnak mindkét SEA esetén ugyanaz a VLAN azonosítója.

Egy ilyen konfigurációra példa lehet a VLAN200 hálózaton lévő LPAR2 a 10-es azonosítójú virtuális kapcsolóval, és a VLAN 200 hálózaton lévő LPAR3 a 20-as azonosítójú virtuális kapcsolóval. Mivel mindkét LPAR és a megfelelő SEA adapterek ugyanazt a VLAN azonosítót használják (VLAN200), mindkét SEA hozzáfér az ilyen VLAN azonosítójú csomagokhoz.

A híd használata nem engedélyezhető több VIOS szerveren. Ezért a következő, több SEA adaptert használó konfigurációkat a Megbízható tűzfal:

- Több VIOS és több SEA illesztőprogram.
- Redundáns SEA terhelésmegosztás: A VLAN hálózatok közötti továbbításhoz konfigurált csonk adapterek nem oszthatók fel két VIOS szerver között.

Megosztott Ethernet adapterek eltávolítása

A Megosztott Ethernet adapter eszközök eltávolítását a rendszerről egy adott sorrendben kell elvégezni.

Egy megosztott Ethernet adapter (SEA) eltávolításához a rendszerről, tegye a következőket:

1. Távolítsa el a megosztott Ethernet adapterrel társított Megbízható virtuális gépet a következő parancs kiadásával:
   ```
   rmdev -dev svm
   ```
2. Távolítsa el a megosztott Ethernet adaptert a következő parancs kiadásával:
   ```
   rmdev -dev megosztott_ethernet_adapter_azonosítója
   ```

Megjegyzés: A SEA eltávolítása az SVM eltávolítása előtt rendszerhibát eredményezhet.

Szabályok létrehozása

Létrehozhat szabályokat a Megbízható tűzfal VLAN hálózatok közötti útválasztásához.

A Megbízható tűzfal útválasztási szolgáltatásainak engedélyezéséhez létre kell hoznia az engedélyezett kommunikációkat megadó szabályokat. Kibővített biztonság esetén nincs olyan egyetlen szabály, amely engedélyezné a kommunikációt a rendszeren lévő VLAN hálózatok mindegyike között. Minden engedélyezett kapcsolatnak saját szabállyal kell rendelkeznie, habár az egyes aktivált szabályok mindkét irányban engedélyezik a kommunikációt a megadott végpontok között.

Mivel a szabályok létrehozása a Virtual I/O Server (VIOS) felületen történik, a parancsokkal kapcsolatos további információk a VIOS témakör gyűjteményben érhetők el, a Power Systems hardver információs központban.

Egy szabály létrehozásához tegye a következőket:

1. Nyissa meg a VIOS parancssori felületet.
2. Inicializálja az SVM illesztőprogramot a következő parancs kiadásával:
   ```
   mksvm
   ```
3. Indítsa el a Megbízható tűzfal szolgáltatást az indító parancs kiadásával:
   ```
   vlantfw -s
   ```
4. Az összes ismert LPAR IP és MAC cím megjelenítéséhez adja ki a következő parancsot:
   ```
   vlantfw -d
   ```

   Azoknak a logikai partícióknak (LPAR) az IP és MAC címére lesz szüksége, amelyekhez szabályokat szeretne létrehozni.
5. Hozza létre a szűrőszabályt a két LPAR (LPAR1 és LPAR2) közötti kommunikáció engedélyezéséhez a következő parancsok egyikének kiadásával (a parancsokat egy sorban kell megadni):
   ```
   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
   ```

Megjegyzés: Az egyik szűrőszabály alapértelmezés szerint mindkét irányban engedélyezi a kommunikációt, a port és protokoll bejegyzésektől függően. Például a Telnet kommunikációt az LPAR1 partícióról az LPAR2 partíció irányában a következő parancs futtatásával engedélyezheti:

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

6. A kernelben lévő összes szűrőszabály aktiválásához a következő parancsot adja ki:

```
mkvfilt -u
```

Megjegyzés: Ez az eljárás aktiválja ezt a szabályt, valamint bármely más, a rendszerben létező szűrőszabályt.

További példák

A következő példák bemutatnak néhány más szűrőszabályt, amelyet a Megbízható tűzfal használatával hozhat létre.

- A Secure Shell kommunikáció engedélyezéséhez a VLAN 100 hálózaton található LPAR partícióról a VLAN 200 hálózaton található LPAR partícióra, adja ki a következő parancsot:

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

- A 0 - 499 tartományba eső összes port közötti forgalom engedélyezéséhez adja ki a következő parancsot:

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

- A logikai partíciók közötti összes TCP forgalom engedélyezéséhez adja ki a következő parancsot:

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

  Ha nem ad meg portokat vagy portműveleteke, akkor a forgalom minden portot használhat.

- Az Internet vezérlőüzenet protokoll (ICMP) üzenetek engedélyezéséhez a logikai partíciók között, adja ki a következő parancsot:

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

Kapcsolódó fogalmak:

“Szabályok deaktiválása”
A Megbízható tűzfal szolgáltatásban a VLAN hálózatok közötti továbbítást engedélyező szabályok deaktiválhatók.

Kapcsolódó hivatkozás:

“genvfilt parancs” oldalszám: 148

“mkvfilt parancs” oldalszám: 150

“vlantfw parancs” oldalszám: 169

Kapcsolódó tájékoztatás:

Virtuális I/O szerver

Szabályok deaktiválása

A Megbízható tűzfal szolgáltatásban a VLAN hálózatok közötti továbbítást engedélyező szabályok deaktiválhatók.

Mivel a szabályok deaktiválás a Virtual I/O Server (VIOS) felületen végezhető el, a parancsokkal és a folyamattal kapcsolatos további információk a VIOS témakör gyűjteményben érhetők el, a Power Systems hardver információs központban.

Egy szabály deaktiválásához tegye a következőket:

1. Nyissa meg a VIOS parancssori felületet.
2. Az összes aktív szűrőszabály megjelenítéséhez írja be a következő parancsot:

   ```
   lsvfilt -a
   ```

   Az **-a** kapcsoló elhagyásával az Objektumadat-kezelőben tárolt összes szabályt jelenítheti meg.
3. Jegyezze fel a deaktiválni kívánt szűrőszabály azonosítószámát. Ebben a példában a szűrőszabály azonosítószáma 23.

4. A kernelben aktív 23-as azonosítószámú szűrőszabály deaktiválásához adja ki a következő parancsot:
   ```
   rmvfilt -n 23
   ```

   A kernelben lévő összes szűrőszabály deaktiválásához adja ki a következő parancsot:
   ```
   rmvfilt -n all
   ```

Kapcsolódó fogalmak:

“Szabályok létrehozása” oldalszám: 104
Létrehozhat szabályokat a Megbízható tűzfal VLAN hálózatok közötti útválasztásához.

Kapcsolódó hivatkozás:

“lsvfilt parancs” oldalszám: 149
“rmvfilt parancs” oldalszám: 168

Megbízható naplózás

A PowerVM Megbízható naplózás lehetővé teszi, hogy az AIX logikai partíciók egy csatolt Virtual I/O Serveren (VIOS) lévő naplófájlokba írjanak. Az adatok a hypervisoron keresztül közvetlenül a VIOS szerverre vannak továbbítva, és nem szükséges hálózati csatlakozás a kliens LPAR és a VIOS között.

Virtuális naplók

A naplófájlokat a Virtual I/O Server (VIOS) adminisztrátor hozza létre és kezeli, és ezek az AIX operációs rendszer számára virtuális naplóeszközökként jelennek meg a /dev könyvtárban, a virtuális lemezekhez vagy virtuális optikai adathordozókhoz hasonlóan.

A naplófájlok tárolása virtuális naplóként növeli a rekordok megbízhatósági szintjét, mivel ezeket a kliens LPAR partíción (ahol elő lettek állítva) egy root jogosultságokkal rendelkező felhasználó sem módosíthatja. Egyazon kliens LPAR partícióhoz több virtuális naplóeszköz is csatlakoztatható, és minden napló egy külön fájlban van a /dev könyvtárban.

A Megbízható naplózás lehetővé teszi, hogy több kliens LPAR partícióról származó naplóadatok egyetlen fájlrendszerben legyenek egyesítve, amely a VIOS rendszerről elérhető. Ezért a VIOS egyetlen helyet biztosít a rendszeren a naplóelemzéshez és archiváláshoz. A kliens LPAR adminisztrátora konfigurálhatja az alkalmazásokat és az AIX operációs rendszert, hogy az adatokat a virtuális naplóeszközökbe írják - ez hasonló az adatok helyi fájlokba történő írásához. Az AIX megfigyelési alrendszer beállítható úgy, hogy a megfigyelési rekordokat a virtuális naplókba irányítsa, és más AIX szolgáltatások, mint például a syslog, a saját meglévő konfigurációjuk szerint irányítsák az adatokat a virtuális naplókba.

A virtuális napló beállításához a VIOS adminisztrátornak meg kell adnia egy nevet a virtuális napló számára. A név a következő különálló összetevőkből áll:

- Kliens neve
- Napló neve

A két össztevő nevét a VIOS adminisztrátor bármilyen értékre beállíthatja, azonban a kliens neve tipikusan minden olyan virtuális napló esetén megegyezik, amelyek egy adott LPAR partícióhoz vannak csatolva (például az LPAR hosztneve). A naplóév a napló céljának azonosítására szolgál (például audit vagy syslog).

Egy AIX LPAR partíción az egyes virtuális naplóeszközök két, funkcionalitását tekintve egyenértékű fájlként vannak jelen a /dev fájlrendszeren. Az első fájl neve az eszköz nevét tükrözi, például /dev/vlog0, a második fájl neve pedig a vl előtag és a naplónév, valamint az eszközszám összefűzéséből adódik. Ha például a vlog0 virtuális naplóeszköz naplóneve audit, akkor az a /dev fájlrendszeren vlog0 és vlaudit0 néven is jelen van.

Kapcsolódó tájékoztatás:

Virtuális naplók létrehozása

Virtuális naplóeszközök észlelése

Miután egy VIOS adminisztrátor létrehozott virtuális naplóeszközöket és csatolta ezeket egy kliens LPAR partícióhoz, a kliens LPAR eszköz konfigurációját frissíteni kell, hogy az eszközök láthatóvá váljanak.

A kliens LPAR adminisztrátora a következő módszerek egyikével frissítheti a beállításokat:

- A kliens LPAR újrabetöltése
- A **cfgmgr** parancs futtatása

Futtassa az **lsdev** parancsot a virtuális naplóeszközök megjelenítéséhez. Az eszközök neve alapértelmezés szerint tartalmazza a vlog előtagot. Példa az **lsdev** parancs kimenetére egy AIX LPAR partíción, amelyen két virtuális naplóeszköz található:

```
lsdev
vlog0  Virtuális naplóeszköz
vlog1  Virtuális naplóeszköz
```

Vizsgálja meg az egyes virtuális naplóeszközök tulajdonságait az lsattr –El <*eszköznév*> parancs futtatásával, amely a következőhöz hasonló kimenetet eredményez:

```
lsattr –El vlog0
PCM                     Útvonalvezérlő modul          Hamis
client_name    dev-lpar-05 Kliens neve                  Hamis
device_name    vlsyslog0   Eszközneve                   Hamis
log_name       syslog      Napló neve                   Hamis
max_log_size   4194304     Naplóadatfájl max mérete     Hamis
max_state_size 2097152     Naplóállapotfájl max mérete  Hamis
pvid           none        Fizikai kötet azonosítója    Hamis
```

Ez a kimenet megjeleníti a kliens nevét, az eszköz nevét, valamint a naplóadatok mennyiségét, mit a VIOS tárolni képes.

A virtuális napló kétféle típusú naplóadatot tárol. Ezek:

- Naplóadatok: Az AIX LPAR partíción lévő alkalmazások által előállított nyers naplóadatok.
- Állapotadatok: Információk arról, hogy az eszközök mikor voltak konfigurálva, megnyitva, bezárva, valamint más műveletekről, amelyek a naplóelemzési tevékenység során felhasználásra kerültek.

A VIOS adminisztrátor adja meg az egyes virtuális naplókban tárolható **naplóadatok** és **állapotadatok** mennyiségét, és ezt a mennyiséget a max_log_size és a max_state_size attribútumok jelzik. Amikor a tárolt adatok mennyisége meghaladja a megadott korlátot, a legkorábbi adatok felül lesznek írva. A VIOS adminisztrátornak meg kell győződnie róla, hogy a naplóadatok gyakran vannak összegyűjtve és archiválva a naplók megőrzése érdekében.

Megbízható naplózás telepítése

A PowerSC Megbízható naplózás szolgáltatását a parancssori felület vagy az SMIT eszköz használatával telepítheti.

A Megbízható naplózás előfeltételei a VIOS 2.2.1.0 vagy újabb változat, és az IBM AIX 6 with Technology Level 7 vagy IBM AIX 7 with Technology Level 1.

A Megbízható naplózás szolgáltatás telepítéséhez szükséges fájl neve powerscStd.vlog, amit a PowerSC Standard Edition telepítő CD tartalmaz.

A Megbízható naplózás funkció telepítéséhez:

1. Győződjön meg róla, hogy VIOS 2.2.1.0 vagy újabb változatot futtat.
2. Helyezze be a PowerSC telepítő CD-t, vagy töltse le a telepítő CD képfájlját.
3. Használja az **installp** parancsot vagy az SMIT eszközt a powerscStd.vlog fájlkészlet telepítéséhez.

Kapcsolódó tájékoztatás:

“PowerSC Standard Edition telepítése” oldalszám: 7
A PowerSC Standard Edition minden egyes adott funkciójához telepítenie kell egy fájlkészletet.

Megbízható naplózás konfigurálása

Megismerheti az eljárást, amellyel a Megbízható naplózás összetevőt konfigurálhatja az AIX felülvizsgálati alrendszeren és a syslog szolgáltatáshoz.

AIX megfigyelési alrendszer konfigurálása

Az AIX megfigyelési alrendszer beállítható úgy, hogy a bináris adatokat a helyi fájlrendszeren lévők naplók mellett egy virtuális naplóeszközbe is beírja.

Megjegyzés: Mielőtt konfigurálná az AIX megfigyelési alrendszert, el kell végeznie a következő helyen leírt eljárást: “Virtuális naplóeszközök észlelése” oldalszám: 107.

Az AIX megfigyelési alrendszer konfigurálásához tegye a következőket:

1. Konfigurálja az AIX megfigyelési alrendszert úgy, hogy az adatokat bináris (auditbin) módban naplózza.
2. Aktiválja a Megbízható naplózás összetevőt az AIX megfigyeléshez az /etc/security/audit/config konfigurációs fájl szerkesztésével.
3. Adjon hozzá egy virtual_log = /dev/vlog0 paramétert a bin: szakaszhoz.

   Megjegyzés: Az utasítás akkor érvényes, ha az LPAR adminisztrátor az auditbin adatokat a /dev/vlog0 könyvtárba szeretné írni.
4. Indítsa újra az AIX megfigyelési alrendszert a következő sorrendben:

   ```
   audit shutdown
   audit start
   ```

A megfigyelés rekordokat az alrendszer a helyi fájlrendszer mellett a Virtual I/O Serveren (VIOS) lévő naplókba is beírja, a megadott virtuális naplóeszközön keresztül. A naplók tárolási helyét az /etc/security/audit/config konfigurációs fájl bin: szakaszában meglévő bin1 és bin2 paraméterek szabályozzák.

Kapcsolódó tájékoztatás:

Megfigyelési alrendszer

syslog konfigurálása

A syslog beállítható úgy, hogy az üzeneteket virtuális naplókba írja - ehhez szabályokat kell hozzáadni az /etc/syslog.conf fájlhoz.

Megjegyzés: Mielőtt konfigurálná az /etc/syslog.conf fájlt, el kell végeznie a következő helyen leírt eljárást: “Virtuális naplóeszközök észlelése” oldalszám: 107.

Az /etc/syslog.conf fájl szerkeszthető, hogy egyeztesse a naplóüzeneteket a következő feltételek alapján:

- Funkció
- Prioritási szint

Ha a virtuális naplókat szeretné használni a syslog üzenetekhez, akkor az /etc/syslog.conf fájlban be kell állítani szabályokat, hogy a kívánt üzenetek a /dev könyvtárban található megfelelő virtuális naplóba legyenek írva.

Például bármely funkció által előállított hibakeresés szintű üzenetek elküldéséhez a vlog0 virtuális naplóba, adja hozzá a következő sort az /etc/syslog.conf fájlhoz:

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

Megjegyzés: Az olyan parancsok esetén, amelyek az adatokat virtuális naplókba írják, ne használja a syslogd démonban elérhető naplórotációs funkciókat. A /dev fájlrendszeren lévő fájlok nem normál fájlok, és nem nevezhetők át vagy helyezhetők át. A VIOS adminisztrátornak a VIOS-on belül kell konfigurálnia a virtuális naplók rotációját.

A syslogd démont a konfiguráció után a következő parancs segítségével újra kell indítani:

```
refresh -s syslogd
```

Kapcsolódó tájékoztatás:

syslogd démon

Adatok írása virtuális naplóeszközökbe

Tetszőleges adatok írhatók egy virtuális naplóeszközbe is - nyissa meg a /dev könyvtárban lévő megfelelő fájlt, és írja az adatokat a fájlba. A virtuális naplót egyszerre egy folyamat nyithatja meg.

Például:

Üzenetek írásához a virtuális naplózó eszközbe az **echo** parancs használatával, adja ki a következő parancsot:

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

Fájlok tárolásához a virtuális naplóeszközbe a **cat** parancs használatával, adja ki a következő parancsot:

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

Az egyes írások mérete legfeljebb 32 KB lehet, és a programok, amelyek több adatot próbálnak írni egyetlen írási műveletben, I/O (EIO) hibát kapnak. A parancssori felület (CLI) segédprogramjai, mint például a **cat** parancs, automatikusan feldarabolják az átviteleket 32 KB-os írási műveletekre.

Megbízható hálózati kapcsolat (TNC)

A Megbízható hálózati kapcsolat (TNC) a Trusted Computing Group (TCG) része, amely specifikációkat biztosít a végpontok integritásának ellenőrzéséhez. A TNC meghatározott nyílt megoldás architektúrával rendelkezik, ami segítséget nyújt az adminisztrátoroknak irányelvek foganatosításában a hálózati infrastruktúra hozzáférésének hatékony szabályozásához.

A Megbízható hálózati kapcsolat (TNC) négy összetevőt tartalmaz:

- TNC szerver
- TNC javításkezelés
- TNC szerver
- TNC IP hivatkozó

Megbízható hálózati kapcsolat alapelvek

Megismerheti a Megbízható hálózati kapcsolat (TNC) összetevőit, a biztonságos kommunikáció konfigurálását és javításkezelési rendszerét.

Megbízható hálózati kapcsolat összetevői

A Megbízható hálózati kapcsolat (TNC) keretrendszer összetevőinek bemutatása.

A TNC modell a következő összetevőkből áll:

Megbízható hálózati kapcsolat (TNC) szerver

A Megbízható hálózati kapcsolat (TNC) szerver azonosítja a hálózathoz hozzáadott klienseket, és kezdeményezi az ellenőrzésüket.

A TNC kliens biztosítja a szükséges fájlkészlet szint információkat a szerver számára az ellenőrzéshez. A szerver megállapítja, hogy a kliens az adminisztrátor által beállított szinten van-e. Ha a kliens nem megfelelő, akkor a TNC szerver értesíti az adminisztrátort a szükséges kiigazításról.

A TNC szerver ellenőrzéseket kezdeményez a klienseken, amelyek megpróbálják elérni a hálózatot. A TNC szerver betölti az integritási mérőszám ellenőrzőket (IMV), amelyek lekérhetik a kliensektől az integritási mérőszámokat, és ellenőrizhetik azokat. Az AIX rendelkezik egy alapértelmezett IMV ellenőrzővel, ami ellenőrzi a rendszerek fájlkészletét és biztonsági javítás szintjét. A TNC szerver egy keretrendszer, amely több IMV modult tölt be és kezel. Egy kliens ellenőrzése esetén az IMV-kre támaszkodva lekéri az információkat a kliensektől, és ellenőrzi a klienseket.

TNC javításkezelés

A Megbízható hálózati csatlakozás (TNC) szerver a Szolgáltatásfrissítés-kezelő segéd (SUMA) funkcióval integrálva egy javításkezelési megoldást biztosít.

A javításmenedzser letölti az IBM ECC és javítóközpont webhelyeken elérhető legújabb javítócsomagokat és biztonsági javításokat. A TNC javításkezelés démon feltölti a legutóbbi frissített információkat a TNC szerverre, amely egy alapsor fájlkészletként szolgál a kliensek ellenőrzéséhez.

A **tncpmd** démont konfigurálni kell a SUMA letöltések kezeléséhez és a fájlkészlet információk feltöltéshez a TNC szerverre. A démont egy Internethez csatlakozó rendszeren kell futtatni a frissítések automatikus letöltéséhez. A TNC javításkezelő szerver Internet-kapcsolat nélküli használatához regisztrálhat egy felhasználó által megadott javításlerakatot a TNC javításkezelő szerveren.

Megjegyzés: A TNC szerver és a **tncpmd** démon futtatható egyazon rendszeren.

A javításkezelés az alábbi módszerek egyikében áll rendelkezésre:

- Parancssori felület (pmconf) használata
- Démon használata (tncpmd2)

Parancssori felület (pmconf) használata a javításkezelés biztosításához:

A SUMA és a cURL kerül meghívásra a javítócsomag szint (SP szint) letöltésekor a **pmconf add** paranccsal.

Ha a javítócsomag szint (SP szint) a **pmconf add** paranccsal kerül letöltésre, akkor a SUMA kerül meghívásra az SP szint letöltéséhez és regisztrálásához a TNC-vel. Ezenkívül a cURL is meghívásra kerül az új és a hiányzó biztonsági javítások letöltéséhez.

Az alábbi **pmconf get** parancsargumentumok további szabályozási lehetőséget biztosítanak a biztonsági javítások kezelésében:

- A **display-only** lehetővé teszi a felhasználó számára a sebezhetőségek leírásainak vizsgálatát, amelyeket az SP szinthez alkalmazható biztonsági javítások adtak meg. A biztonsági javítások nem kerülnek letöltésre ennek a parancsnak a használatával.
- A **download-only** lehetővé teszi a felhasználó számára a biztonsági javítások letöltését a felhasználó által megadott letöltési könyvtárba, de az alkalmazásukat nem. A javítások nem kerülnek alkalmazásra.

Démon (tncpmd2) használata a javításkezelés biztosításához:

A démon ütemező összetevője beállítható a TNC kliensek biztonságát érintő frissítések automatikus ellenőrzésére.

A letöltési időköz szabályozza, hogy az ütemező milyen gyakran ellenőrizze az új javítócsomag szinteket. Ha új javítócsomag szint található a TNC-vel aktuálisan regisztrált technológiai szinthez (TL), akkor az új javítócsomag szint, valamint minden hiányzó és új biztonsági javítás letöltésre kerül, majd hozzáadódik a lerakathoz. A letöltési időköz a **pmconf init** paranccsal állítható be. Az ajánlott érték legalább egyszer egy hónapban (43200 perc).

Az “ifix_download_interval” szabályozza, hogy az ütemező milyen gyakran ellenőrizze az új biztonsági köztes javításokat, amelyek közzé lettek téve. Minden új biztonsági javítás letöltésre kerül, majd hozzáadódik a lerakathoz. Az ajánlott ifix letöltési időköz naponta egyszer (1440 perc).

Megbízható hálózati kapcsolat kliens

A Megbízható hálózati kapcsolat (TNC) kliens a TNC szerver számára az ellenőrzéshez szükséges információkat biztosít.

A szerver megállapítja, hogy a kliens az adminisztrátor által beállított szinten van-e. Ha a kliens nem megfelelő, akkor a TNC szerver értesíti az adminisztrátort a szükséges frissítésekről.

A TNC kliens indításkor betölti az IMC-ket, és ezeket használja a szükséges információk összegyűjtéséhez.

Megbízható hálózati kapcsolat IP hivatkozó

A Megbízható hálózati kapcsolat (TNC) szerver automatikusan képes kezdeményezni az ügyfelek ellenőrzését, amelyek a hálózat részei. A Virtual I/O Server (VIOS) partíción futó IP hivatkozó észleli a VIOS által kiszolgált új ügyfeleket, és elküldi az IP címeiket a TNC szervernek. A TNC szerver ellenőrzi az ügyfelet a meghatározott irányelv tekintetében.

Megbízható hálózati kapcsolat - biztonságos kommunikáció

A Megbízható hálózati kapcsolat (TNC) démonok a Szállítási réteg biztonsága (TLS) vagy Védett socket réteg (SSL) protokoll használatával támogatott titkosított csatornákon keresztül kommunikálnak.

A biztonságos kommunikáció célja, hogy biztosítsa a hálózaton áramló adatok és parancsok hitelesítését és védelmét. Minden egyes rendszernek rendelkeznie kell egy saját kulccsal és tanúsítvánnyal, amelyek az összetevők inicializálási parancsának futtatásakor kerülnek előállításra. Ez a folyamat az adminisztrátor számára teljesen átlátszó, és kevesebb adminisztrátori beavatkozást igényel.

Egy új kliens ellenőrzéséhez a kliens tanúsítványát importálni kell a szerver adatbázisába. A tanúsítvány kezdetben megbízhatatlanként van megjelölve, és ezután az adminisztrátor a **psconf** parancs futtatásával tekintheti meg és jelölheti meg a megbízhatóként:

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

Egy eltérő kulcs és tanúsítvány használatához a **psconf** parancs biztosítja a tanúsítvány importálásához szükséges paramétert.

A tanúsítvány importálásához a szerverről, adja ki a következő parancsot:

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

A tanúsítvány importálásához a kliensből, adja ki a következő parancsot:

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

Megbízható hálózati kapcsolat protokoll

A TNC keretrendszer a Megbízható hálózati kapcsolat (TNC) protokollt használja a hálózat integritásának fenntartásához.

A TNC biztosít specifikációkat a végpontok integritásának ellenőrzéséhez. A hozzáférést kérő végpontok olyan kritikus összetevők integritás mérőszámain alapján vannak felmérve, amelyek hatással lehetnek a működési környezetre. A TNC keretrendszer adminisztrátorai megfigyelik a hálózatban lévő rendszerek integritását. A TNC integrálva van az AIX javításterjesztő infrastruktúrával, és így egy teljes javításkezelési megoldást biztosít.

A TNC specifikációknak teljesíteniük kell az AIX és POWER család rendszerarchitektúra követelményeit. A TNC összetevői úgy vannak tervezve, hogy egy teljes javításkezelési megoldást biztosítsanak az AIX operációs rendszeren. Ez a konfiguráció lehetővé teszi az adminisztrátorok számára az AIX telepítéseken lévő szoftverkonfigurációk hatékony kezelését. A termék biztosít eszközöket is a rendszerek javítási szintjeinek ellenőrzéséhez, és előállít egy jelentést a nem megfelelő kliensekről. Továbbá a javításkezelés leegyszerűsíti a javítások letöltésének és telepítésének folyamatát.

IMC és IMV modulok

A Megbízható hálózati kapcsolat (TNC) szerver vagy kliens belsőleg az integritási mérőszám adatgyűjtő (IMC) és az integritás mérőszám ellenőrző (IMV) modulokat használja a szerver ellenőrzéséhez.

Ez a keretrendszer több IMC és IMV modul betöltését teszi lehetővé a szerverre és a kliensekbe. A modul, amely az operációs rendszer (OS) és fájlkészlet szintű ellenőrzést végrehajtja, alapértelmezés szerint része az AIX operációs rendszernek. Az AIX operációs rendszerrel szállított modulok eléréséhez használja a következő útvonalak egyikét:

- /usr/lib/security/tnc/libfileset_imc.a: Összegyűjti az operációs rendszer szintjét és a telepített fájlkészletet a kliensrendszerekről, és elküldi az adatokat az IMV (TNC szerver) modulnak ellenőrzés céljából.
- /usr/lib/security/tnc/libfileset_imv.a: Lekéri az operációs rendszer szint és fájlkészlet információkat a klienstől, és összehasonlítja azokat az alapsor információkkal. Továbbá frissíti a kliens állapotát a TNC szerver adatbázisában. Az állapot megtekintéséhez adja ki a következő parancsot:

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

Kapcsolódó hivatkozás:

“psconf parancs” oldalszám: 155

TNC követelmények

A TNC összetevő összes szolgáltatásának teljes használatához ellenőrizze, hogy a minimális követelmények rendelkezésre állnak a környezetben.

TNC javításkezelés

AIX	SUMA	OpenSSL	Megjegyzések
7.2 TL1	7.2.1.0	1.0.2	Az operációs rendszerrel együtt szállított
7.2 TL0	7.2.1.0	1.0.2	A SUMA/Java telepítése külön szükséges.
7.1 TL4	7.2.1.0	1.0.2	A SUMA/Java telepítése külön szükséges.
7.1 TL1, TL2, TL3			Az AIX 7.2 javítócsomag szintek letöltése nem támogatott
7.1 TL0			TNCPM minimálisan támogatott kiadási szintje

TNC összetevők beállítása

A Megbízható hálózati kapcsolat (TNC) összetevőit be kell állítani egy adott környezetben történő futtatásra.

Az alábbi eljárásban szereplő lépések mindegyikét végre kell hajtani a TCN összetevők beállításához. További nem kötelező lépések is bemutatásra kerültek.

1. Azonosítsa azoknak a rendszereknek az IP címeit, ahol a TNC szerver, TNC Patch Management (TNCPM) szerver és a TNC IP hivatkozó a Virtual I/O Server termékhez (VIOS) beállításra kerül.
2. Állítsa be a hálózati telepítéskezelő (NIM) szervert. A TNCPM szerverként beállított rendszer az elsődleges NIM. A sets:bos.sysmgt.nim.master fájlkészletnek telepítve kell lenni ezen a rendszeren.
3. Engedélyezze az Autonóm egészség tanácsadót (AHA) az új javítócsomagok és biztonsági javítások automatikus értesítéséhez a TNC szerverhez. Ha az AHA nem engedélyezett, akkor a TNC ütemező a TNC szervert ütemezett időközönként frissíti. AHA engedélyezése az automatikus értesítéshez:

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

4. A TNC javításkezelés javításlerakatainak inicializálásához adja ki a következő parancsot: (a parancsot egyetlen sorba írja be):

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

   Példa a **pmconf** parancsra:

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

   Az **init** parancs letölti az egyes technológia szintekhez tartozó legfrissebb javítócsomagot, és elérhetővé teszi azt a TNC szerver számára. A frissített javítócsomagok lehetővé teszik, hogy a TNC szerver lefuttasson egy alapsor TNC kliens ellenőrzést, illetve a TNC javításkezelő szerver telepítse a TNC kliensfrissítéseket. Adja meg az **-A** kapcsolót az összes licencszerződés elfogadásához a kliensfrissítések futtatásakor. Alapértelmezés szerint a TNC javításkezelő szerver által letöltött javításlerakatok a /var/tnc/tncpm/fix_repository fájlban találhatók. A **-P** kapcsolóval megadhat egy eltérő könyvtárat.
5. TNCPM szerver beállítása. A TNCPM szerver beállítható a NIM rendszeren. A TNCPM szerver a SUMA használatával tölti le a javításokat az IBM Fix Central és ECC webhelyekről. A TNCPM szerver cURL használatával tölti le a ifiix javításokat az IBM biztonság webhelyéről. A frissítések letöltéséhez a rendszernek csatlakoznia kell az Internethez. Adja ki a következő parancsot a TNCPM szerver konfigurálásához:

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

   Például:

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

6. Konfigurálja az irányelveket a TNC szerveren. A kliensellenőrzések irányelveinek létrehozásához tekintse meg a "Irányelvek létrehozása a Megbízható hálózati kapcsolat klienshez" oldalszám: 119 részt.
7. Konfigurálja a klienseket a következő parancs használatával:

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

Például:

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

8. Fejezze be a TNC összetevők beállítását az egyes összetevőkhöz tartozó nem kötelező lépések végrehajtásával.

Kapcsolódó hivatkozás:

"psconf parancs" oldalszám: 155

Kapcsolódó tájékoztatás:

"PowerSC Standard Edition telepítése" oldalszám: 7
A PowerSC Standard Edition minden egyes adott funkciójához telepítenie kell egy fájlkészletet.

Telepítés NIM segítségével

IBM Fix Central

Passport Advantage Online súgóközpont

TNC összetevők beállításainak konfigurálása

Minden egyes TNC összetevőhöz konfigurálható legalább egy beállítás.

Trusted Network Connect (TNC) szerver konfigurációs beállításai

Megismerheti a TNC szerver konfigurálásához szükséges lépéseket.

A TNC szerver konfigurálásához az /etc/tnccs.conf fájlnak egy következőhöz hasonló értéket kell tartalmaznia:

```
component = SERVER
```

Egy rendszer konfigurálásához szerverként, adja ki a következő parancsot:

```
psconf mkserver tncport=<port> pmserver=<ip|hosztnév[,ip2|hosztnév2..]:port>
[recheck_interval=<idő percben>]
```

Például:

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

Megjegyzés: A tncport portot és a pmserver portot különböző értékekre kell beállítani, és ha a recheck_interval paraméter értéke nincs megadva, akkor az 1440 perces alapértelmezett érték kerül felhasználásra.

A rendszer a tncport porthoz a 42830-as értéket, a pmserver porthoz a 38240-es alapértelmezett portértéket használja.

Kapcsolódó hivatkozás:

"psconf parancs" oldalszám: 155

Megbízható hálózati kapcsolat kliens további beállításainak konfigurálása

Megismerheti a Megbízható hálózati kapcsolat (TNC) kliens konfigurálásához szükséges lépéseket, valamint a beállításhoz szükséges konfigurációs beállításokat.

A TNC kliens konfigurálásához az /etc/tnccs.conf fájlnak egy következőhöz hasonló értéket kell tartalmaznia:

```
component = CLIENT
```

Egy rendszer konfigurálásához kliensként, adja ki a következő parancsot:

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

Például:

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

Megjegyzés: A szerverport és a tncport (ami egy kliensport) értékének meg kell egyeznie.

Kapcsolódó hivatkozás:

"psconf parancs" oldalszám: 155

TNC Patch Management szerver beállításainak konfigurálása

A Trusted Network Connect Patch Manager (TNCPM) szerver integrál a SUMA és a cURL alkalmazással, ezáltal átfogó javításkezelő megoldást biztosít.

A TNCPM szervert a Hálózati telepítéskezelő (NIM) szerveren kell konfigurálni, így a TNC kliensek frissíthetők.

Az automatikus IBM biztonsági tanácsadó és köztes javítás letöltések engedélyezéséhez megadhat egy köztes javítás időközt. Ez a szolgáltatás automatikusan értesítést küld az újonnan közzétett biztonsági köztes javításokról és a hozzájuk tartozó Általános sebezhetőségek és veszélyeztetettségek (CVE) azonosítóiról. Minden biztonsági tanácsadó és köztes javítás ellenőrzésre kerül, mielőtt regisztrálva lenne a TNC keretrendszerben. Az IBM AIX sebezhetőségi nyilvános kulcs, amely a köztes javítások automatikus letöltéséhez szükséges, az IBM AIX biztonság webhelyen érhető el. Az automatikus javítócsomag és köztes javítás letöltések a letöltési időköz és a köztes javítás időköz 0-ra állításával letilthatók.

A javítócsomag és a köztes javítás regisztráció kézzel is frissíthető. Egy IBM biztonsági tanácsadó és vele együtt a megfelelő köztes javítások kézi regisztrálásához adja ki a következő parancsot:

```
pmconf add -y <tanácsadófájl> -v <aláírásfájl>  -e <ifix_tar_fájl>
```

Egy önálló köztes javítás kézi regisztrálásához adja ki a következő parancsot:

```
pmconf add -p <SP> -e <ifix_fájl>
```

Egy új technológia szint regisztrálásához és a hozzá tartozó legújabb javítócsomag letöltéséhez adja ki a következő parancsot:

```
pmconf add -l <TSZ_lista>
```

Egy olyan javítócsomag letöltéséhez, amely nem a legutóbbi változat, vagy egy ellenőrzéshez és kliensfrissítésekhez használandó technológia szint letöltéséhez adja ki a következő parancsot:

```
pmconf add -l <TSZ_lista> -d
pmconf add -s <SP_lista>
```

A rendszeren már létező javítócsomag vagy technológia szint javításlerakat regisztrálásához adja ki a következő parancsot:

```
pmconf add -s <SP> -p <felhasználó_által_megadott_javításlerakat>
pmconf add -l <TSZ> -p <felhasználó_által_megadott_javításlerakat>
```

Egy javításkezelő szerverként szolgáló rendszer konfigurálásához adja ki a következő parancsot:

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

Íme egy példa erre a parancsra:

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

A TNC javításkezelő szerver mindig támogatja a biztonsági Jogosult problémaelemzési jelentések (APAR) kezelését. Adja ki a következő parancsot a TNC javításkezelés konfigurálásához más típusú APAR jelentések kezelésére:

```
pmconf add -t <APAR_típusok_listája>
```

Az előző példában az <APAR_típusok_listája> a következő APAR-típusokat tartalmazó vesszővel elválasztott lista:

- HIPER
- PE
- Enhancement

A TNCPM nyílt csomaglerakatok kezeléséhez adja ki a következő parancsok legalább egyikét:

```
pmconf add -o <csomagnév> -V <verziószám> -T [installp|rqm] -D <felhasználó által megadott útvonal>
pmconf delete -o <csomagnév> -V <verziószám>
pmconf list -o <csomagnév> -V <verziószám>
pmconf list -O [-c] [-q]
```

A Nyílt csomagok az alábbi alapértelmezett könyvtárhoz kerülnek hozzáadásra:

/var/tnc/tncpm/fix_repository/packages.

Felhasználó által megadott útvonal = A csomag helye a rendszeren

A biztonsági javítások által megadott leíró információk megjelenítéséhez egy adott javítócsomag szinthez, a javítások alkalmazása nélkül a lerakathoz, adja ki a következő parancsot:

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

Például:

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

A biztonsági javítások letöltéséhez egy adott javítócsomag szinthez, a javítások alkalmazása nélkül a lerakathoz, adja ki a következő parancsot:

```
pmconf get -p <SP> -D <letöltési könyvtár>
```

Megjegyzés: A parancs futtatása előtt a *letöltési könyvtár* könyvtárnak létezni kell.

Például:

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

A TNC javításkezelő szerver a **syslog** parancsot támogatja a javítócsomag, technológia szint és kliensfrissítések letöltéséhez. Az eszköz a user, a prioritás pedig az info. Erre példa: user.info.

A TNC javításkezelő szerver fenntart egy naplót is a /var/tnc/tncpm/log/update/<ip>/<időpecsét> könyvtárban, amely az összes kliensfrissítést tartalmazza.

Kapcsolódó hivatkozás:

“psconf parancs” oldalszám: 155

Kapcsolódó tájékoztatás:

IBM AIX biztonság

Megbízható hálózati kapcsolat szerver e-mail értesítés konfigurálása

Megismerheti az eljárást, amellyel konfigurálhatja az e-mail értesítéseket a Megbízható hálózati kapcsolat (TNC) szerverhez.

A TNC szerver figyeli a kliens javítási szintjét, és ha azt találja, hogy a kliens nem kompatibilis, akkor az eredményről és a szükséges kiigazításról e-mail értesítést küld az adminisztrátornak.

Az adminisztrátor e-mail címének konfigurálásához adja ki a következő parancsot:

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

Például:

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

Az előző példában a *vayugrp1* és *vayugrp2* IP-csoport esetén a rendszer az abc@ibm.com e-mail címre küldi az értesítést.

Ha egy hozzárendelt e-mail címmel nem rendelkező IP-csoport globális e-mail címére szeretne e-mailt küldeni, akkor adja ki a következő parancsot:

```
psconf
add –e <e-mail_cím>
```

Például:

```
psconf add –e abc@ibm.com
```

Az előző példában, ha egy IP-csoporthoz nincs hozzárendelve e-mail cím, akkor az értesítés az abc@ibm.com e-mail címre lesz elküldve. Ez globális e-mail címként működik.

Kapcsolódó hivatkozás:

“psconf parancs” oldalszám: 155

IP hivatkozó konfigurálása VIOS rendszeren

Megtudhatja, hogy az IP hivatkozó hogyan konfigurálható Virtual I/O Serveren (VIOS) az ellenőrzés automatikus kezdeményezéséhez.

Megjegyzés: Az IP hivatkozó konfigurálása előtt be kell állítania az SVM kernel kiterjesztés a Virtuális Virtual I/O szerveren (VIOS).

A TNC IP hivatkozó konfigurálásához az /etc/tnccs.conf konfigurációs fájlnak rendelkeznie kell a következő component = IPREF beállításhoz hasonló beállítással.

Egy rendszert a következő parancs kiadásával konfigurálhat kliensként:

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

Például:

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

A tncserver port és a tncport (a kliensport) értékének meg kell egyeznie.

Konfigurálja a TNC IP hivatkozót a VIOS rendszeren. Ez a konfiguráció a VIOS rendszeren aktiválja az ellenőrzést a hálózathoz csatlakozó klienseken. Adja ki a következő parancsot a hivatkozó konfigurálásához:

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

Például:

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

Megjegyzés: A szerverport és a TNC port (egy kliensport) értékének meg kell egyeznie.

Kapcsolódó hivatkozás:

“psconf parancs” oldalszám: 155

Megbízható hálózati kapcsolat (TNC) összetevők kezelése

Megismerheti a Megbízható hálózati kapcsolat (TNC) kezelését feladatok megvalósításához, mint például az ügyfelek, irányelvek, naplók, ellenőrzési eredmények hozzáadása, ügyfelek, illetve a TNC keretrendszerrel kapcsolatos tanúsítványok frissítése.

Megbízható hálózati kapcsolat szervernaplók megtekintése

Megtudhatja, hogyan tekintheti meg a Megbízható hálózati kapcsolat (TNC) szerver naplóit.

A TNC szerver az összes kliens ellenőrzési eredményét naplózza. A napló megtekintéséhez futtassa a **psconf** parancsot:

```
psconf list –H –i <ip |ALL>
```

Kapcsolódó hivatkozás:

“psconf parancs” oldalszám: 155

Irányelvek létrehozása a Megbízható hálózati kapcsolat klienshez

A Megbízható hálózati kapcsolat (TNC) klienssel kapcsolatos irányelvek beállításának bemutatása.

A TNC irányelvek kezeléséhez szükséges felületet a psconf konzol biztosítja. Az egyes kliensek vagy klienscsoportok társíthatók egy irányelvvel.

A következő irányelvek hozhatók létre:

- Egy Internet protokoll (IP) csoport több kliens IP címet tartalmaz.
- Az egyes kliens IP címek csak egyetlen csoporthoz tartozhatnak.
- Az IP csoport társítva van egy irányelvcsoporttal.
- Az irányelvcsoport különböző fajta irányelveket tartalmaz. Például a fájlkészlet irányelv, amely megadja, hogy a kliens operációs rendszer szintjének (vagyis kiadás, technológia szint és javítócsomag) milyennek kell lennie. Egy irányelvcsoportban több fájlkészlet irányelv lehet, és a kliensnek, amely erre az irányelvre hivatkozik, az egyik fájlkészlet irányelv által meghatározott szinten kell lennie.

A következő parancsok bemutatják, hogy hogyan hozhat létre egy IP csoportot, egy irányelvcsoportot és fájlkészlet irányelveket.

Egy IP csoport létrehozásához adja ki a következő parancsot:

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

Például:

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

Megjegyzés: Egy csoport esetén legalább egy IP címet meg kell adni. Több IP címet vesszővel kell elválasztani egymástól.

Egy fájlkészlet irányelv létrehozásához adja ki a következő parancsot:

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

Például:

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

Megjegyzés: Az összeépítési információknak a <rel00-TL-sp> formátumban kell lenniük.

Egy irányelv létrehozásához és egy IP csoport hozzárendeléséhez adja ki a következő parancsot:

```
psconf add –P <irányelv_neve> ipgroup=[±] <ipcsop1, ipcsop2 ...]
```

Például:

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

Fájlkészlet irányelv hozzárendeléséhez egy irányelvhez, adja ki a következő parancsot:

```
psconf add –P <irányelv_neve> fspolicy=[±]<fkire1, fkire2 ...>
```

Például:

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

Az OpenPackage irányelvhez adja ki a következő parancsot:

```
pconf add -O <openpkggrp> <openpkgname:version>
```

Az alábbi az OpenPackage irányelv hozzáadási példája:

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

Az OpenPackage hozzárendeléséhez az Fspolicy irányelvhez, adja ki a következő parancsot:

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

Megjegyzés: Ha több fájlkészlet irányelvet ad meg, akkor a rendszer a legjobban illeszkedő irányelvet foganatosítja a kliensen. Ha például a kliens 6100-02-01 szinten van és a fájlkészlet irányelvet 7100-03-04 és 6100-02-03 irányelvként említi, akkor a 6100-02-03 irányelvet foganatosítja a kliensen.

Kapcsolódó hivatkozás:

“psconf parancs” oldalszám: 155

Megbízható hálózati kapcsolat kliens ellenőrzésének elindítása

Megtudhatja, hogyan ellenőrizheti a Megbízható hálózati kapcsolat (TNC) klienst.

A kliens ellenőrzéséhez a következő módszerek egyikét használhatja:

- A Virtual I/O Serveren (VIOS) futó IP hivatkozó démon továbbítja a kliens IP címét a TNC szervernek: A kliens LPAR beszerzi az IP címet, és megpróbálja elérni a hálózatot. A VIOS szerveren futó IP hivatkozó démon észleli az új IP címet, és továbbítja az a TNC szervernek: Amikor a TNC szerver megkapja az új IP címet, kezdeményezi az ellenőrzését.
- A TNC szerver rendszeres időközönként ellenőrzi a klienst: Az adminisztrátor hozzáadhatja a kliens IP címeket, amelyeket ellenőrizni kell a TNC irányelv adatbázisban. A TNC szerver ellenőrzi az adatbázisban lévő klienseket. Az újraellenőrzés rendszeres időközönként automatikusan megtörténik az /etc/tnccs.conf konfigurációs fájlban megadott recheck_interval attribútum értékének megfelelően.
- Az adminisztrátor kézzel kezdeményezi a kliens hitelesítését: A következő parancs futtatásával az adminisztrátor az ellenőrzést kézzel is kezdeményezheti annak ellenőrzését, hogy hozzá lett-e adva egy kliens a hálózathoz.

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

Megjegyzés: Olyan erőforrások esetén, amelyek nem csatlakoznak egy VIOS szerverhez, a kliensek akkor ellenőrizhetők és frissíthetők, amikor kézzel hozzáadásra kerülnek a TNC szerverhez.

Kapcsolódó hivatkozás:

“psconf parancs” oldalszám: 155

Megbízható hálózati kapcsolat hitelesítési eredményeinek megtekintése

Megismerkedhet a Megbízható hálózati kapcsolat (TNC) kliens hitelesítési eredményeinek megtekintésére szolgáló eljárással.

A hálózatban lévő kliensek hitelesítési eredményeinek megtekintéséhez adja ki a következő parancsot:

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

Ez a parancs az összes olyan klienst megjeleníti, amelynek állapota **IGNORED** (mellőzött), **COMPLIANT** (megfelelő) vagy **FAILED** (meghiúsult).

- **IGNORED**: A kliens IP címe figyelmen kívül maradt az IP listában (vagyis a kliens mentes az ellenőrzés alól).
- **COMPLIANT**: A kliens átment a hitelesítésen (vagyis a kliens megfelel az irányelvnek).
- **FAILED**: A kliens hitelesítése sikertelen volt (vagyis a kliens nem felel meg az irányelvnek, és adminisztrátori beavatkozás szükséges).

A hiba okának megállapítása érdekében futtassa a **psconf** parancsot a sikertelen kliens IP címével:

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

Kapcsolódó hivatkozás:

“psconf parancs” oldalszám: 155

Megbízható hálózati kapcsolat kliens frissítése

A Megbízható hálózati kapcsolat (TNC) szerver ellenőriz egy klienst, és frissíti az adatbázist a kliens állapotával és az ellenőrzés eredményével. Az adminisztrátor megtekintheti az eredményeket, és megteheti a kliens frissítéséhez szükséges lépéseket.

Egy korábbi szinten lévő kliens frissítéséhez adja ki a következő parancsot:

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

Például:

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

A **psconf** parancs frissíti a klienst az összeépítéssel és az APAR telepítésekkel, ha azok nincsenek telepítve.

Kliens frissítése nyílt csomagokkal:

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

Kapcsolódó hivatkozás:

“psconf parancs” oldalszám: 155

Javításkezelési irányelvek kezelése

A javításkezelési irányelvek konfigurálásához a **pmconf** parancs használható.

A javításkezelési irányelvek információkat biztosítanak egy SUMA frissítés kezdeményezéséhez (mint például a TNC szerver IP címét és az időközt).

A javításkezelési irányelv kezeléséhez adja ki a következő parancsot:

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

Például:

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

Megjegyzés: A pmport és a tncserver portoknak eltérőnek kell lenniük.

Kapcsolódó hivatkozás:

“pmconf parancs” oldalszám: 151

Megbízható hálózati kapcsolat tanúsítványok importálása

Megismerheti az eljárást, amellyel importálhat egy tanúsítványt és biztonságosan viheti át az adatokat a hálózaton.

A Megbízható hálózati kapcsolat (TNC) démonok a Szállítási réteg biztonsága (TLS) vagy Védett socket réteg (SSL) protokoll használatával támogatott titkosított csatornákon keresztül kommunikálnak. Ez a démon biztosítja, hogy a

hálózaton szállított adatok és parancsok hitelesítve és védve legyenek. Minden egyes rendszernek megvan a saját kulcsa és tanúsítványa, amelyek az összetevők inicializálási parancsának futtatásakor kerülnek előállításra. Ez a folyamat az adminisztrátor számára átlátszó, és kevesebb adminisztrátori beavatkozást igényel. Egy kliens első alkalommal történő ellenőrzésekor a kliens tanúsítványa importálásra kerül a szerver adatbázisába. A tanúsítvány kezdetben megbízhatatlanként van megjelölve, és az adminisztrátor a **psconf** parancs futtatásával tekintheti meg és jelölheti meg a megbízhatóként:

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

Ha az adminisztrátor egy eltérő kulcsot és tanúsítványt szeretne használni, akkor a **psconf** parancs segítségével importálhatja a kulcsot és a tanúsítványt.

A tanúsítvány importálásához egy szerverről, adja ki a következő parancsot:

```
psconf import  -S -k <kulcsfájl_neve> -f <fájlnév>
```

A tanúsítvány importálásához egy kliensből, adja ki a következő parancsot:

```
psconf import  -C -k <kulcsfájl_neve> -f <fájlnév>
```

Kapcsolódó hivatkozás:

“psconf parancs” oldalszám: 155

TNC szerver jelentéskészítés

A Megbízható hálózati kapcsolat (TNC) szerver a vesszővel elválasztott érték (CSV) formátumot és szöveges kimeneti formátumot egyaránt támogatja az általános sebezhetőségek és veszélyeztetettségek (CVE), az IBM biztonsági tanácsadó, a TNC szerver irányelvek, a TNC kliens biztonsági javítások, valamint a regisztrált javítócsomagok és köztes javítások jelentéseihez.

A CVE jelentés a regisztrált javítócsomagok összes általános sebezhetőségét és veszélyeztetettségét megjeleníti. A jelentés eredményének megtekintéséhez írja be a következő parancsot:

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

Az IBM biztonsági tanácsadó jelentés a telepített IBM szoftver ismert biztonsági sebezhetőségeit jeleníti meg. A jelentés eredményének megtekintéséhez írja be a következő parancsot:

```
psconf report -A
<tanácsadó_neve>
```

A TNC szerver irányelvek jelentés a TNC szerveren foganatosított biztonsági irányelveket jeleníti meg. A jelentés eredményének megtekintéséhez írja be a következő parancsot:

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

A TNC kliens javítás jelentés a TNC kliens telepített és hiányzó köztes javításait jeleníti meg. A jelentés eredményének megtekintéséhez írja be a következő parancsot:

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

Futtathat egy olyan jelentést is, amely előállítja a regisztrált javítócsomagok, valamint a kapcsolódó jogosult programelemzési jelentések (APAR) és köztes javítások listáját. A jelentés eredményének megtekintéséhez írja be a következő parancsot:

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

A regisztrált nyílt forrású csomagok listájának megjelenítéséhez adja ki a következő jelentésparancsot:

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

Kapcsolódó hivatkozás:

“psconf parancs” oldalszám: 155

Megbízható hálózati kapcsolat és javításkezelés hibaelhárítása

Megismerheti a hibák lehetséges okait, valamint a TNC és a javításkezelési rendszer hibaelhárításához szükséges lépéseket.

A TNC és a javításkezelési rendszer hibaelhárításához ellenőrizze a következő táblázatban felsorolt konfigurációs beállításokat.

13. táblázat: TNC és javításkezelési rendszer konfigurációs beállításainak hibaelhárítása

Probléma	Megoldás
A TNC szerver nem indul el vagy nem válaszol	Tegye a következőket: 1. A következő parancs kiadásával állapítsa meg, hogy a TNC szerver démon fut-e: `ps –eaf | grep tnccsd` 2. Ha nem fut, akkor törölje a /var/tnc/.tncsock fájlt. 3. Indítsa újra a szervert. Ha ez nem oldja meg a problémát, akkor a TNC szerveren ellenőrizze az /etc/tnccs.conf konfigurációs fájlban a component = SERVER bejegyzést.
A TNC javításkezelő nem indul el vagy nem válaszol	• A következő parancs kiadásával állapítsa meg, hogy a TNC javításkezelő szerver démon fut-e: `ps –eaf | grep tncpmd` • A TNC javításkezelő szerveren ellenőrizze az /etc/tnccs.conf konfigurációs fájlban a component = TNCPM bejegyzést.
A TNC kliens nem indul el vagy nem válaszol	• A következő parancs kiadásával állapítsa meg, hogy a TNC kliens démon fut-e: `ps –eaf | grep tnccsd` • A TNC kliensben ellenőrizze az /etc/tnccs.conf konfigurációs fájlban a component = CLIENT bejegyzést.
A TNC IP hivatkozó nem fut Virtual I/O Serveren (VIOS)	• A következő parancs kiadásával állapítsa meg, hogy a TNC IP hivatkozó démon fut-e: `ps –eaf | grep tnccsd` • A VIOS rendszeren ellenőrizze az /etc/tnccs.conf konfigurációs fájlban a component = IPREF bejegyzést.
Egy rendszer nem állítható be egyszerre TNC szerverként és kliensként	A TNC szerver és kliens nem futhat egyidejűleg egyazon rendszeren.
A démonok futnak, de az ellenőrzés nem történik meg	Engedélyezze a démonokhoz a naplóüzeneteket. Állítsa be a level=info naplózási szintet a /etc/tnccs.conf fájlban. Elemezheti a naplóüzeneteket.

PowerSC grafikus felhasználói felület (GUI)

Ez a rész az IBM PowerSC grafikus felhasználói felület (GUI) terméket mutatja be, beleértve a felület telepítését, karbantartását és használatát.

Az IBM PowerSC GUI növeli az PowerSC Standard Edition termék használhatóságát, egy alternatíva biztosításával a parancssori és a naplófájl interakcióval szemben. A PowerSC GUI központosított felügyeleti konzolt biztosít a végpontok és állapotuk megjelenítéséhez; a megfelelési szintek alkalmazásához, visszavonásához és ellenőrzéséhez; a rendszerek csoportosításához a megfelelési szint műveletek alkalmazásához; valamint a megfelelési konfigurációs profilok megjelenítéséhez és személyre szabásához.

A PowerSC GUI a fájlintegritás-figyelést (FIM) is tartalmaz. A FIM tartalmazza a valós idejű megfelelést (RTC) és a megbízható végrehajtást (TE). A PowerSC GUI segítségével beállítható az RTC és a TE, valamint megjeleníthetők a valós idejű események. Ezenkívül a PowerSC GUI kiterjedt profilszerkesztési és jelentéskészítési képességeket biztosít.

PowerSC GUI alapelvek

A PowerSC GUI használata előtt ismerje meg az általános alapelveket a biztonságra és a végpont feltérképezésre vonatkozóan.

PowerSC GUI biztonság

A PowerSC GUI a biztonságot kétirányú HTTPS kommunikáció használatával biztosítja a PowerSC GUI szerver és a PowerSC GUI ügynökök között, minden egyes AIX végponton.

A TLS egyeztetési folyamat olyan tanúsítványokat használ, amelyek a PowerSC GUI szerveren és a PowerSC GUI ügynökökön is elérhetők. A TLS egyeztetési folyamat egyetlen hitelesítést támogat mindkét irányban, mivel vagy a PowerSC GUI ügynök vagy a PowerSC GUI szerver kezdeményezheti a kommunikációt. Az ügynök létrehoz egy egyszeri értéket, amely egy véletlen szám, ami elküldésre kerül a PowerSC GUI szerverhez az első csatlakozás során. A PowerSC GUI szerver ezután belefoglalja ezt az egyszeri értéket minden parancsba, amely elküldésre kerül az adott ügynökhöz. Ez az egyszeri érték biztosítja a megerősítés másik rétegét a végponti ügynök számára, hogy olyan parancsot futtat, amely a hitelesítő PowerSC GUI szerverről származik. A végpontnak meg kell győződni róla, hogy a webszolgáltatás hívás forrása megbízható. A kezdeti egyeztetés és az egyszeri érték biztosítja a megbízhatóságot.

A PowerSC GUI ügynökök és a PowerSC GUI szerver között minden kommunikáció titkosításra kerül olyan protokollok és rejtjelkészletek használatával, amelyek konzisztensek a védett rendszer biztonsági követelményeivel. Jelenleg a protokollszint a TLS 1.2. A PowerSC GUI szerver az összes PowerSC GUI ügynökkel és az összes PowerSC GUI felhasználóval. Ezért a PowerSC GUI szervernek olyan tanúsítvánnyal kell rendelkeznie, amelyben az összes kapcsolat megbízik a felhasználó webböngészőjéből. Például olyan tanúsítvánnyal, amely egy közismert tanúsítványhatóságtól származik, mint például a Verisign vagy egy belül megbízhatónak tartott tanúsítványhatósággal.

A telepítés során a PowerSC GUI szerver létrehoz egy saját aláírású tanúsítványt saját felhasználásra. Ez a tanúsítvány korlátlanul használható, de ideiglenes használatra lett tervezve és kicserélhető egy felhasználó által megadott, széles körben ismert tanúsítvánnyal. A PowerSC GUI szerver egy olyan aláírói tanúsítványt is létrehoz, amely az összes végponti tanúsítvány aláírására szolgál.

A telepítési folyamat automatikusan létrehoz egy tanúsítványtároló fájlt minden egyes végponthoz. A tanúsítványtároló fájl minden egyes végponthoz megegyezik és a PowerSC GUI szerverről át kell másolni minden egyes végpontra. Ez a tanúsítványkombináció a PowerSC GUI szerveren és a végpontokon is magas szintű kommunikációs biztonságot biztosít.

További biztonsági szabályozás is rendelkezésre áll a UNIX csoportok használatával. Minden felhasználónak, például az LDAP felhasználónak vagy a helyi felhasználónak, aki az operációs rendszer által meg van adva, egy adott UNIX csoport tagjának kell lenni a bejelentkezéshez a PowerSC GUIre. Az adminisztrátor a csoporttagságot a **pscuiserverctl** paranccsal állathatja be és módosíthatja.

Bejelentkezés után előfordulhat, hogy csak megjelenítésre van korlátozva. A felhasználói jogosultság funkcióval végrehajthat műveleteket a UNIX csoporttagság által szabályozott végpontokon. A műveletek végrehajtásához olyan UNIX csoport tagjának kell lenni, amelynek van engedélye a végpont kezelésére. További információkért tekintse meg a Csoportok hozzáférésének meghatározása című témakört.

Alapértelmezésben bármeyik felhasználó, aki a biztonsági csoport tagja, kezelheti az összes végpontot, amely megjelenik a PowerSC GUIen. A PowerSC adminisztrátor korlátozhatja a felhasználói hozzáférést az egyéni végpontszintekhez a **setGroups.sh** paranccsal.

Több olyan konfigurációs parancs is van, amelyet csak adminisztrátor felhasználó hajthat végre. Erre példa a globális e-mail beállítások módosítása vagy az új profil létrehozása. Az adminisztrátor felhasználó jogosultságai a UNIX csoportokkal kerülnek beállításra, és a **pscuiserverctl** paranccsal állíthatók be.

Végponttartalom feltöltése a megfelelési oldalon

A megfelelési szint feltérképezéséhez a PowerSC GUI szerver és a PowerSC GUI ügynök a végpontokkal kommunikál.

Indításkor és időnként a sikerig az ügynök megpróbál kapcsolatot kezdeményezni a PowerSC GUI szerverrel. Amikor a kapcsolat létrejön, egyszeri ügynök-szerver biztonsági egyeztetés kerül végrehajtásra. Miután első alkalommal az ügynök-szerver biztonsági egyeztetés sikeresen megtörtént, a szerver létrehoz egy tartományelemet egy egyedi azonosítóval (UID) a végpont belső ábrázolásához és visszaadja az UID azonosítót a végpontnak. Az UID ezután belefoglalásra kerül az ügynök és a szerver minden kommunikációjába. Ez a művelet fejezi be a feltérképezési folyamatot. A PowerSC GUI szerver és a végpont biztonságosan tud kommunikálni bármelyik irányban.

A kezdeti feltérképezési egyeztetés végrehajtása után vagy a PowerSC GUI ügynök újraindítása után, a PowerSC GUI ügynök megkíséreli megállapítani az aktuális megfelelési állapotinformációkat a végpontjához, majd frissíti a PowerSC GUI szervert. A végpont megléte és az aktuális megfelelési információk kerülnek felhasználásra a PowerSC GUI megfelelési állapot oldalának feltöltésére. Ha nem határozható meg megfelelési állapotinformáció, akkor a bejegyzés nem érhető el a megfelelési állapot oldalon.

A PowerSC GUI szerver tartalmazza az összes ismert végpont ábrázolását, amely automatikusan kerül létrehozásra a kezdeti ügynök-szerver kapcsolat és kommunikáció eredményeként. Mivel a végpont ügynökök nyomon követik a végpont megfelelési állapotának változásait, a módosítások átadásra kerülnek a szerverhez és megmaradnak. A PowerSC GUIről minden felhasználói interakció a végponttal a PowerSC GUI szerveren keresztül kerül végrehajtásra. A felhasználói felület nem működik együtt közvetlenül a végponttal és a végponti ügynökkel.

PowerSC GUI telepítése

A PowerSC GUI ügynökök és a PowerSC GUI szerver összetevői a PowerSC Standard Edition telepítése közben kerülnek telepítésre. Mindegyik az installp fájlkészletből kerül telepítésre.

PowerSC GUI ügynök

A PowerSC GUI ügynök minden AIX végponton telepítésre kerül. A PowerSC GUI ügynök követi a tevékenységeket a végponton és megadja az információkat a PowerSC GUI szervernek.

A PowerSC GUI a PowerSC GUIről aktivált parancsokat is futtatja. A PowerSC GUI ügynökök és a PowerSC GUI szerver között minden kommunikáció titkosításra kerül.

Az installp parancs telepíti a központi PowerSC Standard Edition terméket és a PowerSC GUI ügynököt. A powerscStd.uiAgent.rteinstallp fájlkészlet kerül felhasználásra a PowerSC GUI ügynök telepítéséhez. Az alábbi példában látható az installp parancs, amelyet minden végponton futtatni kell:

Megjegyzés: Az alábbi példában a telepítőkészletek a /tmp/inst.images/ könyvtárban kerülnek kibontásra.

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

PowerSC GUI szerver

A PowerSC GUI szerver bármilyen AIX rendszeren futtatható, ajánlott létrehozni egy dedikált AIX LPAR-t, amelyen telepíti és futtatja a PowerSC GUI szervert.

Az **installp** parancs telepíti a központi PowerSC Standard Edition terméket és a PowerSC GUI szervert. A powerscStd.uiServer.rte **installp** fájlkészlet szolgál a PowerSC GUI szerver telepítésére. Az alábbi példában látható az **installp** parancs, amelyet a végponton futtatni kell:

Megjegyzés: Az alábbi példában a telepítőkészletek a /tmp/inst.images/ könyvtárban kerülnek kibontásra.

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

kPowerSC GUI követelmények

Ismerje meg a PowerSC GUI hardver- és szoftverkövetelményeit.

Hardver

- A PowerSC GUI szerver összetevőit olyan önálló LPAR-ra vagy VM-re kell telepíteni, amely AIX 7.1 vagy újabb változatot futtat.
- A PowerSC GUI ügynök összetevőit minden egyes AIX végponton telepíteni kell.

Szoftver

- A PowerSC GUI szerver AIX 7.1 vagy újabb változatot igényel.
- A PowerSC GUI szerver megköveteli a sendmail démon futtatását.
- A bos.loc.utf.<LANG> fájlkészletet telepíteni kell a PowerSC GUI a profilszabály-leírások megfelelő megjelenítéséhez nem Angol nyelveken.

Tanúsítványtároló biztonsági tanúsítvány terjesztése a végpontokra

A rendszeradminisztrátoroknak az összes végponton telepíteni kell a tanúsítványtároló biztonsági tanúsítványt.

A telepítés során létrehozásra kerül egy tanúsítványtároló fájl, amelyet az összes végpont használhat. A fájl neve endpointTruststore.jks. A fájl az /etc/security/powersc/uiServer/ könyvtárban található.

Telepítés után helyezze el az endpointtruststore.jks fájlt minden egyes végponton a PowerSC GUI ügynökhöz az adott végponton, hogy kapcsolatot létesítsen a PowerSC GUI szerverrel és inicializálja a folyamatot, amely a kulcstároló létrehozását eredményezi a végponton.

A tanúsítványtároló fájl az alábbi módok egyikén terjeszthető:

- Kézzel másolja az endpointTruststore.jks fájlt minden egyes végpontra.
- Ha a környezetben használatban van a PowerVC (vagy másik virtualizáció-kezelő), akkor az endpointTruststore.jks fájl elhelyezhető a PowerVC telepítőkészletében. Amikor a PowerVC telepítőkészlet telepítésre kerül egy végponton, akkor a PowerSC GUI ügynök és a tanúsítványtároló fájl is belefoglalásra kerül.

Miután az endpointTruststore.jks telepítve lett az egyik módszerrel, és amikor a végpont futtatása elkezdődik, a PowerSC GUI ügynök a tanúsítványtároló fájllal határozza meg a helyet, ahol a PowerSC GUI szerver fut. A PowerSC GUI ügynök ezután elküld egy üzenetet a PowerSC GUI szervernek egy részvételi kéréssel az elérhető és megfigyelt végpontok listáján.

Tanúsítványtároló fájl másolása a végpontokra kézzel

A rendszeradminisztrátoroknak a környezetben a tanúsítványtároló fájlt kézzel kell minden egyes meglévő végpontra másolni.

Ezenkívül a tanúsítványtároló fájlt minden egyes felvett új végpontra is másolni kell.

Megjegyzés: Ha rendelkezik olyan adatvirtualizáció-kezelővel, mint például a PowerVC, akkor a tanúsítványtároló fájlt másolhatja az új végpontra egy olyan telepítőkészlet létrehozásával, amely a PowerSC GUI ügynököt és a tanúsítványtároló fájlt is tartalmazza. Lásd: "Tanúsítványtároló fájl másolása a végpontokra a virtualizáció-kezelővel".

1. A végponti tanúsítványtároló /etc/security/powersc/uiServer/endpointTruststore.jks fájl másolásához az /etc/security/powersc/uiAgent/endpointTruststore.jks fájlba az egyes végpontokon, futtassa az alábbi **scp** parancsot:

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

2. A végpontügynökök újraindításához a biztonsági tanúsítvány telepítése után, a végponton futtassa a következő parancsokat:

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

3. Ismételje meg a 1 és 2 lépést minden egyes meglévő végponthoz és minden új végponthoz (ha nem rendelkezik adatvirtualizáció-kezelővel).

Tanúsítványtároló fájl másolása a végpontokra a virtualizáció-kezelővel

A rendszeradminisztrátorok olyan virtualizáció-kezelőket használhatnak, mint például a PowerVC a tanúsítványtároló fájl másolásához minden egyes új végpontra egy olyan telepítőkészlettel, amely tartalmazza a PowerSC ügynököt és a tanúsítványtároló fájlt.

1. Másolja a végponti tanúsítványtároló /etc/security/powersc/uiServer/endpointTruststore.jks fájlt a PowerVC telepítőkészletbe.
2. Telepítse a PowerVC telepítőkészletet a rendszerhez hozzáadott minden egyes új végponton.

Felhasználói fiókok beállítása

Alapértelmezésben minden felhasználónak függetlenül attól, hogy LDAP felhasználó vagy helyi felhasználó, akit az operációs rendszer adott meg, a biztonsági csoport tagjának kell lenni ahhoz, hogy bejelentkezzen a PowerSC GUIre.

Az adminisztrátor megváltoztathatja ezt a kötelező csoporttagságot s **pscuiserverctl** paranccsal. Bejelentkezés után a PowerSC GUIre, a felhasználó csak a végpontok állapotát tekintheti meg, ha a felhasználói fiókja olyan UNIX csoport tagja, amely számára a végpontkezelés engedélyezett. Az adminisztrátor megváltoztathatja a felhasználói fiók beállításait az egyéni végpont szinthez a **setGroups.sh** paranccsal.

Tartsa szem előtt tart az alábbi pontokat:

- Több-több kapcsolat van a végpontok és az AIX csoportok között:
  - Egy AIX csoport több végponttal társítható.
  - Egy végpont több AIX csoporttal társítható.
- Miután a felhasználó bejelentkezik a PowerSC GUIre, a csoporttársítások határozzák meg, hogy a felhasználó számára engedélyezett-e a parancsok futtatása bizonyos végpontokhoz, vagy a felhasználó számára csak a végpont állapotának a megjelenítése engedélyezett.
  - A parancsok futtatásához egy adott végponton a PowerSC GUI használatával, a felhasználónak társítva kell lenni a végponthoz tartozó egyik csoporttal.
  - A felhasználó csoporttagsága összehasonlításra kerül az egyes végpontokhoz tartozó csoportokkal. Ha a felhasználó csoporttagsága megegyezik az egyes végpontokhoz tartozó csoportokkal, akkor a felhasználó számára engedélyezett az olyan parancsok futtatása, mint például az **Apply profiles**, **Undo** és a **Check** a végponton. Ha a

felhasználó csoporttagsága nem egyezik meg az egyes végpontokhoz tartozó csoportok egyikével sem, akkor a felhasználó csak az adott végpont állapotát tekintheti meg.

Az alábbi parancsértelmező parancsfájlok érhetők el a PowerSC GUI szerveren az /opt/powersc/uiServer/bin/ könyvtárban.

14. táblázat: Csoport parancsértelmező parancsfájljai

Parancsértelmező parancsfájl	Leírás
pscuiserverctl	Megadja az AIX bejelentkezési (UNIX) csoportot, amelyben a felhasználónak tagnak kell lenni, hogy bejelentkezhessen a PowerSC GUIre. A felhasználónak csak az egyik csoport tagjának kell lenni.
setGroups.sh	Megad legalább egy AIX csoportot, amelyben a felhasználónak tagnak kell lenni a parancsok futtatásához bizonyos végpontokon.

Csoportbeállítási parancsok és parancsfájlok futtatása

A rendszeradminisztrátorok a **pscuiserverctl** parancs és a **setGroups** parancsfájl futtatásával adhatják meg, hogy mely operációs rendszercsoport számára legyen engedélyezett a bejelentkezés a PowerSC GUIre, illetve elvégzik az adminisztrátori feladatokat és parancsokat futtatnak adott végpontokon.

1. A PowerSC GUI szerveren lépjen az /opt/powersc/uiServer/bin/ könyvtárba.
2. A következő parancs futtatásával megadhatja azt az AIX csoportot, amelyben a felhasználónak tagnak kell lenni a bejelentkezéshez a PowerSC GUIre. A megadott csoport beírásra kerül az /etc/security/powersc/uiServer/uiServer.conf fájlba.

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

   Tipp: A parancs futtatása előtt a **groups** *felhasználónév* paranccsal megtekintheti a csoportokat, amelynek a felhasználó tagja.
3. Futtassa a következő parancsot azon UNIX csoportok megadásához, akik számára engedélyezett az adminisztrátori funkciók végrehajtása a PowerSC GUIen.

   ```
   pscuiserverctl set administratorGroupList unixgrpadmin1,unixgrpadmin2
   ```
4. Futtassa a következő parancsfájlt azon AIX csoportok megadásához, amelyekben a felhasználónak tagnak kel lenni a parancsok futtatásához adott végpontokon. Meg kell adni a végpontok teljes képzésű hosztnevét. A megadott csoportok az /etc/security/powersc/uiServer/groups.txt fájlba kerülnek beírásra.

   ```
   ./setGroups.sh csoportnév "végpont hosztnevek vesszővel tagolt listája"
   ```

   Megjegyzés: A végpontok keresésekor korlátozott számú helyettesítő karakter használata támogatott. Például az alábbi specifikációk érvényesek az összes olyan végpont megadásához, amelyek neve "Boston_" kezdetű vagy ".rs.com" végű:
   - ./setGroups.sh groupname "Boston_*"
   - ./setGroups.sh groupname "*.rs.com"

   Tipp: Ehhez a parancshoz a csillag (*) az egyetlen támogatott helyettesítő karakter. Csak a karaktersorozat elején vagy végén lehet használni.

PowerSC GUI használata

A PowerSC GUI segítségével megjelenítheti a rendszeren feltérképezett végpontokat, létrehozhat egyéni csoportokat, létrehozhat egyéni profilokat, az egyéni profilokat a végpontokra másolhatja és alkalmazhatja a profilokat. Ezenkívül ellenőrizheti a kommunikációt a végpontok és a PowerSC GUI szerver között, valamint leállíthatja a kommunikációt a végpont és a PowerSC GUI szerver között.

A PowerSC GUI főoldala a következő szakaszokat tartalmazza:

- **Csoportok** tálca: Felsorolja a környezetben meghatározott csoportokat. A csoportok olyan végpontgyűjtemények, amelyek hasonlóság alapján lettek összecsoportosítva. Az **Összes rendszer** csoport automatikusan létrehozásra kerül a végpontok feltérképezésekor a környezetben. Egyéni csoportok is létrehozhatók. Létrehozhat például olyan végpontcsoportot, amelyben a HIPPA a közös.
- A **Megfelelés** oldal három szakaszt tartalmaz:
  - A felső panelen jelennek meg a statisztikai információk a **Csoportok** tálcán kiválasztott csoportról. A statisztikai információk megjelenítik a legutóbbi megfelelési szintek eredményeit, amelyek a kiválasztott csoport végpontjaihoz alkalmazva lettek. A kiválasztott csoporthoz megjelenítheti a rendszersikerek és sikertelenségek százalékos arányát, az ellenőrzött szabályok összesített számát, valamint a meghiúsult szabályokat.
  - A központi panel egy olyan tálca, amely segítségével műveletek hajthatók végre legalább egy végponton. A megfelelési szint alkalmazható, visszavonható és ellenőrizhető.
  - Az alsó panelen látható az a táblázat, amely az összes végpontot vagy a környezetben elérhető végpontok csoportját tartalmazza. A táblázat minden egyes végponthoz a következő információkat tartalmazza:
    - Rendszer neve
    - Megfelelési szabály típusa
    - A megfelelési szint alkalmazásának dátuma és időpontja a végponton
    - A megfelelési szint ellenőrzésének dátuma és időpontja a végponton
    - Megfelelési szint állapota
    - A végponton meghiúsult szabályok száma
    - A végponton sikeresen átadott szabályok száma a megfelelési szint ellenőrzése során
- A **Biztonság** oldal két szakaszból áll:
  - A felső panelen megjelennek a valós idejű biztonsági információk a **Csoportok** tálcán kiválasztott végpontcsoportról. A kiválasztott csoporthoz megjelenítheti a valós idejű megfelelési (RTC) események összesített számát, a Megbízható végrehajtás (TE) eseményeinek összesített számát, a legújabb végpontok százalékos arányát a TNC javításokkal, azon végpontok százalékos arányát, amelyeken a megbízható rendszerbetöltés telepítve van, a végpontok számát, amelyeken a Megbízható tűzfal telepítve van, valamint azon végpontok százalékos arányát, amelyeken a megbízható naplózás telepítve van.
  - Az alsó panelen jelenik meg a táblázat, amely tartalmazza a csoportban szereplő rendszer végpontokat. A táblázat minden egyes végponthoz a következő információkat tartalmazza:
    - Rendszer végpont neve
    - Fájlintegritás esemény jelzők
    - RTC aktiválási állapot
    - TE aktiválási állapot
    - Legújabb TNC javítás állapota
- A **Jelentések** oldal tartalmazza a megfelelési és a fájlintegritás jelentéseket. Az áttekintő és a részletes jelentéseket is tartalmazza.
- A **Profilszerkesztő** oldal három részből áll:
  - A felső panelen van egy legördülő menü, amely felsorolja az elérhető beépített és egyéni profilokat
  - A központi panelen van egy tálca, amely felhasználható a profilok törlésére, új profilok létrehozására és a profilok másolására a csoport részét képező végpontokra.
  - Az alsó panelen jelenik meg az a táblázat, amely a kiválasztott profilban szereplő összes szabályt tartalmazza. Minden egyes szabályhoz megjelennek az alábbi információk:
    - Megfelelési szabály neve
    - Megfelelési szabály típusa
    - A szabály leírása

PowerSC GUI nyelv meghatározása

A PowerSC GUI különböző nyelveken állítható elő.

A PowerSC GUI nyelvének kiválasztásához a főoldal menüsorán kattintson a **Nyelvek és beállítások** ikonra. A felület előállításához használt aktuális nyelv megjelenik a menüben. A nyelv módosításához kattintson a hozzá tartozó ikonra. Az elérhető nyelvek listájáról válassza ki a kívánt nyelvet a szekcióhoz.

Navigáció a PowerSC GUIen

A PowerSC GUIről beállíthatja és adminisztrálhatja a kommunikációt a végpont és a szerver között; rendszerezheti és csoportosíthatja a végpontokat; figyelheti és alkalmazhatja a beépített és az egyéni megfelelési szinteket és profilokat; figyelheti és beállíthatja a végpontok biztonságát; valamint előállíthatja és terjesztheti a jelentéseket ütemezés alapján.

1. Nyissa meg a PowerSC GUIet. A PowerSC GUI megjeleníti a kezdőlapot.
2. A végpont és a szerver közötti kommunikáció adminisztrálásához a főoldal menüsorán kattintson a **Nyelvek és beállítások** ikonra. Kattintson a **Végpont adminisztrációja** ikonra a kommunikáció ellenőrzéséhez vagy leállításához a végpontok és a PowerSC GUI szerver között. További információkért lásd: “Végpont és szerver kommunikációjának adminisztrálása”.
3. A Megfelelés vagy a Biztonság oldal navigációs panelén kattintson a vízszintes ellipszisre a Csoportszerkesztő megnyitásához. A csoportszerkesztő segítségével létrehozhatja a végpontok egyéni csoportjait. További információkért lásd: “Egyéni csoportok létrehozása” oldalszám: 133.
4. Egyénii megfelelési profilok létrehozásához és a profilok másolásához a végpontokra, kattintson a **Profilszerkesztő** lapra. További információkért lásd: “Megfelelési profilok kezelése” oldalszám: 134.
5. A beépített és az egyéni megfelelési szintek és profilok megfigyeléséhez és alkalmazásához kattintson a **Megfelelés** lapra. További információkért tekintse meg a Megfelelési szintek és profilok alkalmazása című részt.
6. A végponti biztonság figyeléséhez és beállításához kattintson a **Biztonság** lapra. További információkért tekintse meg a Végponti biztonság figyelése című részt.
7. A jelentések előállításához és terjesztéséhez igény szerinti vagy ütemezett alapon, kattintson a **Jelentések** lapra. További információkért tekintse meg a Jelentések kezelése című részt.

Végpont és szerver kommunikációjának adminisztrálása

A **Végpont adminisztráció** oldalon ellenőrizheti és leállíthatja a kommunikációt a végpontok és a PowerSC GUI szerver között. Ezenkívül kulcstároló kéréseket is ellenőrizhet és előállíthat.

Végpont és szerver kommunikációjának ellenőrzése

A kommunikáció ellenőrizhető a feltérképezett végpontok és a PowerSC GUI szerver között.

1. A főoldal menüsorán kattintson a **Nyelvek és beállítások** ikonra. Kattintson a **Végpont adminisztrációja** elemre. Megnyílik a Végpont adminisztrációja oldal.
2. A **Csoportok** tálcáról válassza ki azt a csoportot, amely tartalmazza az ellenőrizni kívánt végpontokat. Az adott csoport végpontjai a végponttáblázatban vannak felsorolva.
3. A kiválasztott csoporthoz az összes rendszervégpont megjelenik a megfelelési táblázatban. A megjelenő végpontok szűrhetők a **Szűrés szöveg szerint** mező használatával. A mezőben adja meg a szöveget, amely alapján szűrni kíván, majd nyomja meg az Entert. A kiválasztott csoportból a végpontok listája dinamikusan szűrésre kerül és csak a megadott szöveget tartalmazó sorok jelennek meg.
4. A megjelenített állapotinformációk frissítéséhez kattintson a **Táblázat frissítése** elemre.
5. Jelölje be minden egyes végpont jelölőnégyzetét, amelyet ellenőrizni kíván.
6. Kattintson az **Ellenőrzés** ikonra.
7. Megjelenik egy megerősítési üzenet az érvényes kapcsolatról az **Ellenőrizve** és a **Csatlakozási diagnosztika** oszlopban.

Végpontok eltávolítása a PowerSC GUI figyelésből

Amint egy adott végpont feltérképezésre kerül, folyamatosan megfigyelés alatt áll. Ha a végpont eltávolításra kerül a környezetből, akkor a PowerSC GUI szerverről is el kell távolítani.

A végpontok eltávolításához a megfigyelés alól a PowerSC GUIen, tegye a következőket:

1. A főoldal menüsorán kattintson a **Nyelvek és beállítások** ikonra. Kattintson a **Végpont adminisztrációja** elemre. Megnyílik a Végpont adminisztrációja oldal.
2. A **Csoportok** tálcáról válassza ki azt a csoportot, amely tartalmazza az eltávolítani kívánt végpontokat. Az adott csoport végpontjai a végponttáblázatban vannak felsorolva.
3. A kiválasztott csoporthoz az összes rendszervégpont megjelenik a megfelelési táblázatban. A megjelenő végpontok szűrhetők a **Szűrés szöveg szerint** mező használatával. A mezőben adja meg a szöveget, amely alapján szűrni kíván, majd nyomja meg az Entert. A kiválasztott csoportból a végpontok listája dinamikusan szűrésre kerül és csak a megadott szöveget tartalmazó sorok jelennek meg.
4. A megjelenített állapotinformációk frissítéséhez kattintson a **Táblázat frissítése** elemre.
5. Jelölje be minden egyes végpont jelölőnégyzetét, amelynek a megfigyelését le kívánja állítani.
6. Kattintson a **Törlés** ikonra.
7. Megjelenik egy megerősítési üzenet a végpont törlésével kapcsolatban az **Ellenőrzési időpecsét** és a **Csatlakozási diagnosztika** oszlopban.

Kulcstároló kérések ellenőrzése és előállítása

Minden egyes végpont esetében ellenőrizni kell, hogy a kulcstároló kérés érvényes-e, és ha érvényes, akkor előállíthat egy kulcstárolót a végponthoz.

Az első alkalommal, amikor egy végpont elkezd futni, a PowerSC GUI ügynök a tanúsítványtároló fájlt használja a PowerSC GUI futtatási helyének meghatározására. A PowerSC GUI ügynök ezután egy üzenetet küld a PowerSC GUI szervernek egy kéréssel, hogy csatlakozzon az elérhető megfigyelendő végpontok listájához.

A **Végpont adminisztrátor Kulcstároló kérések** oldalon ellenőrizheti, hogy a kulcstároló kérés érvényes-e, és ha érvényes, akkor előállíthat egy kulcstárolót a végponthoz.

1. A főoldal menüsorán kattintson a **Nyelvek és beállítások** ikonra. Kattintson a **Végpont adminisztrációja** elemre. Megnyílik a **Végpont - Összes rendszer** adminisztrációs oldal.
2. Minden egyes ismert végpont felsorolásra kerül a **Rendszernév** oszlopban. Kattintson a **Kulcstároló kérések** elemre és ellenőrizze, hogy van-e függőben lévő kulcstároló kérés. Megnyílik a **Végpont adminisztráció Kulcstároló kérések** oldal.
3. A kulcstároló kérések az összes új és hozzáadott szerverhez felsorolásra kerülnek a **Hosztnév** oszlopban. Miután megerősíti, hogy ki kíván terjeszteni egy kulcstárolót a végponthoz, jelölje be a végpont jelölőnégyzetét, majd kattintson az **Ellenőrzés** elemre.
4. Az ellenőrzést a PowerVC hajtja végre. Adja meg a felhasználói azonosítót és a jelszót a **PowerVC hitelesítési adatok megadása kötelező** ablakban. Kattintson az **OK** gombra. Ha a PowerVC nincs telepítve, akkor hagyja ki ezt a lépést és a következőt.

   Megjegyzés: Az ellenőrzés az Openstack alkalmazásprogramozási felületek használatának folyamata annak ellenőrzésére, hogy a PowerVC számára ismert-e az újonnan meghatározott végpont. Ha a PowerVC nem található meg a felhasználói környezetben, vagy ha a powervcKeystoneUrl nem megfelelően lett beállítva (pscuiserverctl használatával), akkor a PowerSC nem tudja ellenőrizni a végpontot.
5. Ellenőrzés után megjelenik egy üzenet lebegő szövegként a **Hosztnév** oszlopban. Az üzenet megerősíti, hogy a PowerVC felismeri-e az új végpontot. Az üzenetben szereplő információk alapján kiválaszthatja a kulcstároló előállítását.
6. A kulcstároló előállításához kattintson a **Kulcstároló előállítása** elemre. A táblázatban a kulcstároló sora villog a kulcstároló előállítása közben. A befejezést követően az **Kulcstároló előállítva** oszlopban az érték **no** értékről **yes** értékre változik.

   Megjegyzés: Ha nem ellenőrizte a végpontot a PowerVC segítségével, akkor megjelenik egy üzenet és rákérdez, hogy folytatja-e az ellenőrzést. Kattintson a **Folytatás** elemre, ha felismeri a végpontot, és ha elő kívánja állítani a kulcstárolót.

A PowerSC ügynök igénybe vehet néhány percet annak feltérképezésére, hogy a kulcstároló elő lett-e állítva. Miután az ügynök telepíti a kulcstárolót, az új végpont felsorolásra kerül teljesen felügyelt végpontként a PowerSC GUI **Végpont adminisztráció - összes rendszer**, **Megfelelés**, **Biztonság** és **Jelentések** oldalán.

7. Ha nem kíván kulcstárolót előállítani a végponthoz, akkor eltávolíthatja a kérést. Jelölje be az eltávolítani kívánt végpont jelölőnégyzetét, majd kattintson a **Törlés** ikonra.
8. A kulcstároló-ellenőrzésre várakozó összes végpont megjelenik a végponttáblázatban. A megjelenő végpontokat szűrheti a **Szűrés szöveg alapján** mező segítségével. A mezőben adja meg a szöveget, amely alapján szűrni kíván, majd nyomja meg az **Entert**. A végpontok listája dinamikusan szűrésre kerül és csak a megadott szöveget tartalmazó sorok jelennek meg.
9. A végponttáblázat információinak frissítéséhez kattintson a **Táblázat frissítése** elemre.

Végpontok rendszerezése és csoportosítása

A rendszeradminisztrátorok rendszerezhetik és csoportosíthatják a végpontokat néhány általános tulajdonságuk alapján. Egyéni csoportok határozhatók meg és tartalmazhatják a végpontok kifejezetten kiválasztott készletét, amelyek kezelése a PowerSC GUI segítségével történik.

Ha például 3 - 4 környezettel rendelkezik, akkor előfordulhat, hogy létre szeretne hozni olyan csoportokat, amelyek tartalmaznak éles végpontokat, teszt végpontokat és minőségbiztosítási végpontokat.

Az alapértelmezett csoport, amelynek neve **Összes rendszer**, a telepítés során kerül létrehozásra. Ez a csoport tartalmazza a környezetben feltérképezett összes végpontot.

Egyéni csoportok létrehozása

Létrehozhat egy egyéni csoportot a végpontok egy pontosan kijelölt, felsorolt listájával.

1. A **Csoportok** tálcáról válassza ki az **Új csoport létrehozása** elemet. Megnyílik az **Új csoport létrehozása** tálca. Ha a **Csoportok** tálca nem kerül kibontásra, akkor kattintson a vízszintes ellipszisre a felület főoldalának bal oldali panelén.
2. Adjon egy egyedi nevet az új csoportnak, majd nyomja meg az Entert. Az új csoport hozzáadásra kerül a **Csoportok** tálcához.
3. Adja hozzá a rendszereket, amelyeket bele kíván foglalni a csoportba. Az elérhető végpont rendszerek **Összes rendszer** listájáról válassza ki a csoportba belefoglalandó rendszereket. Kattintson a jobbra mutató nyílra az összes kiválasztott rendszer áthelyezéséhez az új csoportba. A végpont rendszerek eltávolításához a csoportból, emelje ki a végpontot a csoportlistán, majd kattintson a balra mutató nyílra.
4. A csoporttagok hozzáadása vagy eltávolítása után mentse a módosításokat a **Mentés** ikonra kattintva a tartalompanel menüsorán.
5. Kattintson a vízszintes sor ellipszisre a visszatéréshez a **Csoportok** tálcára. Az új csoport felsorolásra kerül.

Meglévő csoporthoz hozzárendelt rendszerek hozzáadása és eltávolítása

Felveheti vagy eltávolíthatja a meglévő csoporthoz hozzárendelt végpontokat.

1. A **Csoportok** tálcáról kattintson az ellipszisre a csoporttól jobbra, amelyhez a végpont rendszert hozzá kívánja adni vagy el kívánja távolítani róla. Ha a **Csoportok** tálca nem kerül kibontásra, akkor kattintson a vízszintes ellipszisre a felület főoldalának bal oldali panelén.
2. Kattintson a **Csoport szerkesztése** elemre.
3. Végpont rendszer hozzáadásához a csoporthoz, válassza ki a rendszert az **Összes rendszer** listáról, majd kattintson a jobbra mutató nyílra. A rendszer hozzáadásra került a ***Csoportnév*** listához.
4. Végpont eltávolításához a csoportból, válassza ki a rendszert a **Csoportrendszerek** listáról, majd kattintson a balra mutató nyílra. A rendszer eltávolításra került a ***Csoportnév*** listáról.
5. Kattintson a **Csoportmódosítások mentése** ikonra a módosítások mentéséhez.
6. Rendszer törléséhez a csoportból válassza ki a kívánt rendszert, majd kattintson a balra mutató nyílra.

7. A csoport módosításainak visszavonásához kattintson a **Csoportmódosítások megszakítása** elemre.
8. Kattintson a **Csoportok** ellipszisre a visszatéréshez a **Csoportok** tálcára.

Csoport törlése

A már nem megfelelő csoportok törölhetők.

1. A **Csoportok** tálcáról kattintson az ellipszisre a törölni kívánt csoporttól jobba. Ha a **Csoportok** tálca nem kerül kibontásra, akkor kattintson a vízszintes ellipszisre a felület főoldalának navigációs panelén.
2. Kattintson a **Csoport törlése** elemre. A csoport törlésre kerül és a rendszer eltávolítja a csoportok listájáról a **Csoportok** tálcán.

Csoport átnevezése

A végpontok csoportja átnevezhető.

1. A **Csoportok** tálcáról kattintson az ellipszisre az átnevezni kívánt csoporttól jobba. Ha a **Csoportok** tálca nem kerül kibontásra, akkor kattintson a vízszintes ellipszisre a felület főoldalának navigációs panelén.
2. Kattintson a **Csoport átnevezése** elemre. Adja meg a csoport új nevét a **Csoport neve** mezőben.

Csoport klónozása

A csoport klónozásával létrehozhat egy másodpéldányt ugyanazokkal a végpontokkal és egy új névvel.

1. A **Csoportok** tálcáról kattintson az ellipszisre a törölni kívánt csoporttól jobba. Ha a **Csoportok** tálca nem kerül kibontásra, akkor kattintson a vízszintes ellipszisre a felület főoldalának navigációs panelén.
2. Kattintson a **Csoport klónozása** elemre. A csoport másolása kerül és hozzárendelésre kerül egy új név.

Megfelelési profilok kezelése

A PowerSC GUI profilszerkesztő használatával megjelenítheti a beépített megfelelési profilokat, létrehozhat egyéni profilokat és a profilokat a rendszer végpontjaira másolhatja,

A PowerSC Standard Edition termék olyan beépített profilkészlettel kerül szállításra, amely felhasználható a rendszervégpontok konfigurálására, ezáltal minden egyes végpont megfelel az alábbi biztonsági szabványoknak:

- Fizetőkártya iparág - Adatbiztonsági szabványnak megfelelés (PCI)
- Sarbanes-Oxley törvény és COBIT megfelelés (SOX-COBIT)
- US Department of Defense STIG megfelelés (DoD)
- Az egészségbiztosítás hordozhatóságát és elszámoltathatóságát előíró törvény (HIPAA)
- North American Electric Reliability Corporation megfelelés (NERC)

További információkért a beépített profilokkal kapcsolatban tekintse meg a “Biztonság és megfelelés automatizálásának alapelvei” oldalszám: 9 című témakört.

A beépített profilok mindegyike tartalmaz olyan szabályokat, amelyeket alkalmazni kell a végponthoz, hogy megfeleljen a biztonsági követelményeknek. Ha a szabályok különböző kombinációinak csak egy részhalmazára van szükség; vagy egyéni megfelelési szintekre, akkor létrehozhat egyéni profilt.

A legtöbb környezetben az adminisztrátorok gyakran módosítják a megfelelési fájlokat a problémás szabályok eltávolítása érdekében. Miután a kompatibilitási ellenőrzések végrehajtásra kerülnek, a rendszer a megfelelési szabályfájlokat stabilként veszi figyelembe és telepítésre kerülnek az éles szerverekre.

A PowerSC GUI használható egyéni profilok létrehozására, a szabályok kombinálásával a beépített (vagy más egyéni) profilokból.

Megfelelési profilok megjelenítése

Megjelenítheti az egyes beépített és egyéni profilokba belefoglalt szabályokat.

1. A főoldalon válassza ki a **Profilszerkesztő** lapot. Megnyílik a **Profilszerkesztő** oldal.
2. A profillista megnyitásához kattintson a lefelé mutató nyílra. A legördülő menüben felsorolásra kerülnek az elérhető **Beépített profilok** és **Egyéni profilok**.
3. Válassza ki a megjeleníteni kívánt profilt. A profilban található minden egyes szabály megjelenik a nevével, típusával és a leírásával. További információkért a szabályokkal kapcsolatban tekintse meg a “Biztonság és megfelelés automatizálásának alapelvei” oldalszám: 9 című témakört.
4. A kiválasztott profilhoz minden szabály megjelenik a profiltáblázatban. A megjelenő profilok szűrhetők a **Szűrés szöveg szerint** mező használatával. A szövegmezőben adja meg a szöveget, amely alapján szűrni kíván. A kiválasztott profilban a szabályok listája frissítésre kerül.

Egyéni profil létrehozása

Létrehozhat egy új profilt, amely egy meglévő profilon alapul, majd személyre szabhatja at új profilt, hogy csak bizonyos szabályokat tartalmazzon.

1. A főoldalon válassza ki a **Profilszerkesztő** lapot. Megnyílik a **Profilszerkesztő** oldal.
2. A profillista megnyitásához kattintson a lefelé mutató nyílra. A legördülő menüben felsorolásra kerülnek az elérhető **Beépített profilok** és **Egyéni profilok**.
3. Válassza ki azt a profilt, amelyen az új profil alapuljon.
4. Kattintson az **Új profil létrehozása** ikonra. Megnyílik az Új profil neve és típusa ablak.
5. Adja meg az új profil nevét a **Profil neve** mezőben.
6. Adja meg a típust a **Profil típusa** mezőben. A megadott típus általában azonosítja a beépített irányelv típusát, amelyen az új profil alapul, plusz egy egyedi azonosítót. Például: PCIxx, SOX-COBITxy, DoDxyz, HIPAAwxyz vagy NERCabc.
7. Kattintson a **Megerősítés** elemre.
8. Ha szabályt kíván hozzáadni az egyéni profilhoz, akkor válassza ki a szabályt az eredeti profilból, amelyen az egyéni profil alapul, majd kattintson a jobbra mutató nyílra. A szabály hozzáadásra kerül az új egyéni profilhoz. Ismételje meg minden egyes szabály esetében, amelyet bele kíván foglalni.
9. Ha szabályt kíván eltávolítani az egyéni profilból, akkor válassza ki a kívánt szabályt az egyéni profilból, majd kattintson a balra mutató nyílra. A szabály eltávolításra kerül az új egyéni profilból. Ismételje meg minden egyes szabály esetében, amelyet el kíván távolítani.
10. Ha végzett a szabályok hozzáadásával, akkor kattintson a **Mentés** gombra.

Profilok másolása a csoporttagokhoz

Az egyéni profilok a végpontok csoportjához másolhatók. Miután az egyéni profil másolásra kerül a végpontra, elérhetővé válik alkalmazásra a végponthoz. Ezenkívül elérhető annak ellenőrzéséhez, hogy alkalmazható-e a végponthoz hiba nélkül.

1. A főoldalon válassza ki a **Profilszerkesztő** lapot. Megnyílik a **Profilszerkesztő** oldal.
2. A profillista megnyitásához kattintson a lefelé mutató nyílra. A legördülő menüben felsorolásra kerülnek az elérhető **Beépített profilok** és **Egyéni profilok**.
3. Válassza ki azt a profilt, amelyet a csoporttagokra kíván másolni.
4. Kattintson a **Profil másolása csoporttagokra** ikonra. Megnyílik a ***profilnév*** **másolása a következőre:** ablak.
5. A szervezethez létrehozott minden egyes csoport felsorolásra kerül egy társított jelölőnégyzettel. Jelölje be a jelölőnégyzetet minden egyes csoport mellett, amelybe a kiválasztott profilt másolni kívánja.
6. Kattintson a **Másolás** gombra.
7. A profil alkalmazásához és ellenőrzéséhez térjen vissza a **Megfelelés** oldalra a **Megfelelés** lapra kattintva.

Egyéni profil törlése

Az egyéni profilok törölhetők.

1. A főoldalon válassza ki a **Profilszerkesztő** lapot. Megnyílik a **Profilszerkesztő** oldal.
2. A profillista megnyitásához kattintson a lefelé mutató nyílra. A legördülő menüben felsorolásra kerülnek az elérhető **Beépített profilok** és **Egyéni profilok**.
3. Bontsa ki az **Egyéni profilok** listát.
4. Válassza ki a törölni kívánt profilt.
5. Kattintson a **Profil törlése** ikonra. A kiválasztott egyéni profil törlésre kerül.

Megfelelési szintek és profilok adminisztrálása

A rendszeradminisztrátorok alkalmazhatják, ellenőrizhetik és visszavonhatják a beépített és az egyéni megfelelési szinteket és profilokat több végponton is.

Az alábbi táblázat a PowerSC Standard Edition által támogatott előre meghatározott profilokat tartalmazza.

15. táblázat: PowerSC Standard Edition által támogatott előre meghatározott profilok és megfelelési szintek

Profilok	Szintek
Adatbázis	alacsony
DoD	közepes
DoD_to_AIXDefault	magas
DoDv2	alapértelmezett
DoDv2_to_AIXDefault	
HIPAA	
NERC	
NERC_to_AIXDefault	
NERCv5	
NERCv5_to_AIXDefault	
PCI	
PCI_to_AIXDefault	
PCIv3	
PCIv3_to_AIXDefault	
SOX-COBIT	

A **Megfelelés** oldalról a PowerSC GUIen a következő feladatokat végezheti el:

- Meghatározott profil vagy szint kiválasztása és alkalmazása több végponthoz.
- Visszavonás művelet aktiválása több végponton.
- Megadott szint vagy szint ellenőrzése egy vagy több végpont aktuális állapotához. Az ellenőrzési művelet nem eredményez változást a végponton, de beállítja az **Ellenőrzés időpecsétje** értéket, hogy jelezze az utolsó ellenőrzés időpontját.

Megfelelési szintek és profilok alkalmazása

A kiválasztott csoportban több végponthoz is alkalmazhat megfelelési szintet és profilokat.

1. A főoldalon válassza ki a **Megfelelés** lapot. Megnyílik a **Megfelelés** oldal.
2. A **Csoportok** tálcáról válassza ki azt a csoportot, amely tartalmazza azokat a végpontokat, amelyekhez megfelelési szinteket és profilokat kíván alkalmazni.
3. A kiválasztott csoporthoz az összes rendszervégpont megjelenik a megfelelési táblázatban. A megjelenő végpontok szűrhetők a **Szűrés szöveg szerint** szövegmező használatával. A szövegmezőben adja meg a szöveget, amely

alapján szűrni kíván, majd nyomja meg az Entert. A kiválasztott csoportból a végpontok listája dinamikusan szűrésre kerül és csak a megadott szöveget tartalmazó sorok jelennek meg.

4. A megjelenített állapotinformációk frissítéséhez kattintson a **Táblázat frissítése** elemre. A megjelenítés automatikus frissítési gyakoriságának beállításához kattintson a **Frissítési időköz** elemre.
5. A **Megfelelési szabály típusa** oszlopban megjelenítheti a társított végpontra másolt szinteket és profilokat. Válassza ki a végponthoz alkalmazni kívánt szintet vagy profilt. Jelölje be a hozzá tartozó jelölőnégyzetet.
6. Ismételje meg az 5. lépést a csoport minden egyes végpontjához, amelyhez megfelelési szinteket és profilokat kíván alkalmazni.
7. Kattintson a **Profilok alkalmazása** ikonra.
8. A kiválasztott megfelelési szintek és profilok alkalmazásra kerülnek minden egyes kiválasztott végponthoz. Ha legalább egy szabály nem alkalmazható, akkor a rendszer sikertelenként veszi figyelembe. Ha legalább egy szabály meghiúsul, akkor a végpont megjelölésre kerül egy vörös sávval; és a **Sikertelen** szöveg jelenik meg a **#Meghiúsult szabályok** oszlopban.
9. A **#Meghiúsult szabályok** oszlopban minden egyes megjelölt végpont esetében megtekintheti a szabály meghiúsulásának okát. Az alkalmazott szabályokat beállíthatja egy egyéni profil létrehozásával vagy egy egyéni profil módosításával.

Megfelelési szintek visszavonása

Visszavonhatja a legutóbbi megfelelési szintet és profilt, amely legalább egy végponthoz alkalmazva lett a kiválasztott csoportban.

A megfelelési szint visszavonásához tegye a következőket:

1. A főoldalon válassza ki a **Megfelelés** lapot. Megnyílik a **Megfelelés** oldal.
2. A **Csoportok** tálcáról válassza ki azt a csoportot, amely tartalmazza azokat a végpontokat, amelyekhez vissza kívánja vonni a megfelelési szinteket és profilokat.
3. A kiválasztott csoporthoz az összes végpont megjelenik a megfelelési táblázatban. A megjelenő végpontok szűrhetők a **Szűrés szöveg szerint** szövegmező használatával. A szövegmezőben adja meg a szöveget, amely alapján szűrni kíván, majd nyomja meg az Entert. A kiválasztott csoportból a végpontok listája dinamikusan szűrésre kerül és csak a megadott szöveget tartalmazó sorok jelennek meg.
4. A megjelenített állapotinformációk frissítéséhez kattintson a **Táblázat frissítése** elemre. A megjelenítés automatikus frissítési gyakoriságának beállításához kattintson a **Frissítési időköz** elemre.
5. Végponthoz alkalmazott szint vagy profil visszavonása:
   a. Jelölje be a végponthoz tartozó jelölőnégyzetet.
   b. Kattintson a **Visszavonás** ikonra.

Legutóbb alkalmazott megfelelési szint és profil ellenőrzése

Ellenőrizheti a legutóbbi megfelelési szintet és profilt, amely legalább egy végponthoz alkalmazva lett a kiválasztott csoportban.

1. A főoldalon válassza ki a **Megfelelés** lapot. Megnyílik a **Megfelelés** oldal.
2. A **Csoportok** tálcáról válassza ki azt a csoportot, amely tartalmazza azokat a végpontokat, amelyekhez ellenőrizni kívánja a megfelelési szinteket és profilokat.
3. A kiválasztott csoporthoz az összes végpont megjelenik a megfelelési táblázatban. A megjelenő végpontok szűrhetők a **Szűrés szöveg szerint** szövegmező használatával. A szövegmezőben adja meg a szöveget, amely alapján szűrni kíván, majd nyomja meg az Entert. A kiválasztott csoportból a végpontok listája dinamikusan szűrésre kerül és csak a megadott szöveget tartalmazó sorok jelennek meg.
4. A megjelenített állapotinformációk frissítéséhez kattintson a **Táblázat frissítése** elemre. A megjelenítés automatikus frissítési gyakoriságának beállításához kattintson a **Frissítési időköz** elemre.
5. Jelölje be a végpont rendszer nevéhez tartozó jelölőnégyzetet, amelyhez ellenőrizni kívánja a legutóbb alkalmazott szintet és profilt.

6. Ismételje meg az 5 oldalszám: 137. lépést a csoport minden egyes végpontja esetében, amelyhez ellenőrizni kívánja a megfelelési szinteket és profilokat.
7. Kattintson az **Ellenőrzés** ikonra.
8. A végpont ellenőrzésre kerül és megtekinthető, hogy a megfelelési szintben és profilban szereplő szabályok alkalmazhatók-e. A végpontok nem frissülnek. Ha valamelyik szabály nem alkalmazható, akkor a rendszer úgy tartja, hogy meghiúsul, ha alkalmazásra kerül. Ha legalább egy szabály meghiúsul, akkor a végpont megjelölésre kerül egy vörös sávval; és a **Sikertelen** szöveg jelenik meg a **#Meghiúsult szabályok** oszlopban.
9. A **#Meghiúsult szabályok** listájáról minden egyes megjelölt végponthoz megtekintheti az üzenetet, amely jelzi a szabály meghiúsulásának okát. Az alkalmazott szabályokat beállíthatja egy egyéni profil létrehozásával.

Nem alkalmazott megfelelési szint és profil ellenőrzése

Azok a megfelelési szintek és profilok is ellenőrizhetők, amelyek nem lettek alkalmazva legalább egy végponthoz a kiválasztott csoportban.

1. A főoldalon válassza ki a **Megfelelés** lapot. Megnyílik a **Megfelelés** oldal.
2. A **Csoportok** tálcáról válassza ki azt a csoportot, amely tartalmazza azokat a végpontokat, amelyekhez ellenőrizni kívánja a megfelelési szintek és profil hatását.
3. A kiválasztott csoporthoz az összes végpont megjelenik a megfelelési táblázatban. A megjelenő végpontok szűrhetők a **Szűrés szöveg szerint** szövegmező használatával. A szövegmezőben adja meg a szöveget, amely alapján szűrni kíván, majd nyomja meg az Entert. A kiválasztott csoportból a végpontok listája dinamikusan szűrésre kerül és csak a megadott szöveget tartalmazó sorok jelennek meg.
4. A megjelenített állapotinformációk frissítéséhez kattintson a **Táblázat frissítése** elemre. A megjelenítés automatikus frissítési gyakoriságának beállításához kattintson a **Frissítési időköz** elemre.
5. Jelölje be a végpont rendszer nevéhez tartozó jelölőnégyzetet, amelyhez ellenőrizni kívánja a legutóbb alkalmazott szintet és profilt. Több végpont is kijelölhető.
6. Nyissa meg a **Legutóbb ellenőrzött típus** legördülő listát. Válassza ki a következők egyikét:
   - **Összes elérhető szint** Megjeleníti az összes elérhető szintet, amely ellenőrizhető a kívánt végponthoz.
   - **Összes elérhető profil** Megjeleníti az összes elérhető profilt, amely ellenőrizhető a kívánt végponthoz.
7. Válassza ki az adott végponthoz ellenőrizni kívánt szintet vagy profilt.
8. Kattintson az **Ellenőrzés** ikonra. A rendszer visszaadja az ellenőrzés eredményeit, amelyek a végpont alatt kerülnek felsorolásra.

E-mail értesítés küldése megfelelési esemény előfordulásakor

A Megfelelés oldalról e-mail értesítést küldhet legalább egy címzettnek, ha megfelelési esemény történik.

1. A főoldalon válassza ki a **Megfelelés** lapot. Megnyílik a **Megfelelés** oldal.
2. A menüsoros jobb felső részén kattintson az **E-mail beállítások** ikonra. Megnyílik az **E-mail beállítások** ablak.
3. Jelölje be a **Küldés nekem** e-mail jelölőnégyzetet.
4. Adja meg minden egyes címzett e-mail címét vesszővel tagolva a **Címek (vesszővel tagolt)** mezőben.

Végpont biztonság figyelése

A **Biztonság** oldalról valós időben figyelheti a végpont biztonságát.

A Biztonság oldalon megjelenik azoknak a végpontoknak az állapota, amelyek megfigyelési a Valós idejű megfelelés (RTC) és a Megbízható végrehajtás (TE) segítségével történik.

Az RTC, a PowerSC részösszetevője, illetve a TE, az AIX összetevője a Fájlintegritás megfigyelését (FIM) képviseli. A FIM figyeli a változásokat a fontos fájlokon és biztosítja, hogy a fájlokat befolyásoló események hitelesítve legyenek. A biztonságot érintő események közé tartozik, ha egy engedély a fájlmódosításokhoz váratlan, a fájl tartalma frissül vagy nem ütemezett alkalmazás kerül telepítésre. A fontos fájlok és alkalmazások védelme érdekében ezeket az eseményeket fel kell ismerni.

A **Biztonság** oldal a PowerSC GUI valós idejű megfigyelési oldala. Az oldalon megjelennek az események, amelyek az RTC vagy a TE által figyelt fájlok módosításakor kerülnek előállításra. Az események tartalmazzák a részleteket a fájltartalom változásának időpontjáról, a végpont elérésének időpontjáról vagy a konfiguráció módosításának időpontjáról.

A **Biztonság** oldalon a következő feladatok végezhetők el:

- RTC és TE valós idejű megfigyelési információk megjelenítése
- RTC és TE beállítása az összes végponthoz
- Más PowerSC termékek állapotának megjelenítése a végpontokon
- TE be- és kikapcsolása

Valós idejű megfelelés (RTC) konfigurálása

A **Biztonság** oldalon beállíthatja a Valós idejű megfelelés (RTC) terméket egy adott végponthoz vagy egy végpontcsoporthoz.

1. Kattintson a végpont jobb oldalán található ellipszisre, amelyhez módosítani kívánja az RTC konfigurációt.
2. Kattintson az **RTC konfigurálása** elemre. Megnyílik az RTC irányelvek beállítása ablak.
3. Az összes elérhető RTC konfigurációs beállítás felsorolásra kerül egy magyarázattal. Legalább egy RTC konfigurációs beállítás módosításához jelölje be a beállítás melletti jelölőnégyzetet vagy szüntesse meg a kijelölését. Néhány esetben a beállításokon végzett módosítások nem kerülnek megvalósításra a szerver újraindításáig.
4. Kattintson a **Mentés** gombra.

Valós idejű megfelelés (RTC) konfigurációs beállításainak visszaállítása egy korábbi dátumra és időpontra

Az RTC konfiguráció visszaállítható egy korábbi dátumra és időpontra.

1. Kattintson a végpont jobb oldalán található ellipszisre, amelyhez vissza kívánja görgetni az RTC konfigurációs beállításait az előző változatra.
2. Kattintson az **RTC visszagörgetése** elemre. Az RTC minden egyes konfigurációs változatához felsorolásra kerülnek az időpecsétek.
3. Kattintson a konfigurációs változat azon időpecsétjére, amelyhez vissza kíván térni. Az adott dátumhoz és időponthoz tartozó RTC konfigurációs beállítások visszaállításra kerülnek.

Valós idejű megfelelés (RTC) konfigurációs beállításainak másolása más csoportokba

Az RTC konfigurációs beállítások a végpontok másik csoportjába vagy egy adott végponthalmazba másolhatók.

1. Kattintson az ellipszisre annak a végpontnak a jobb oldalán, amelynek a konfigurációs beállításait másolni kívánja egy másik végpontcsoportba vagy egy adott végponthalmazba.
2. Kattintson az **RTC konfiguráció másolása** elemre. Minden egyes csoportvégpont, beleértve az **Összes rendszer** csoportot, felsorolásra kerül.
3. Válassza ki a kívánt csoportot vagy a specifikus végpontokat az alábbi módszerek egyikével:
   - Az elérhető csoportok listáján jelölje be a kívánt végpontcsoport jelölőnégyzetét. A konfigurációs beállítások másolásra kerülnek a csoportban található minden egyes végpontra.
   - A csoport kibontásához használja a jobbra mutató nyilat és tekintse meg a csoportban található összes végpont listáját. Jelölje be a csoport minden egyes végpontjának a jelölőnégyzetét, amelyre másolni kívánja a konfigurációs beállításokat.
   - Bontsa ki a végpontok listáját az **Összes rendszer** csoportban. Jelölje be a csoport minden egyes végpontjának a jelölőnégyzetét, amelyre a végpontokat másolni kívánja.
4. Kattintson az **OK** gombra. A konfigurációs beállítások másolásra kerültek a kiválasztott csoportba vagy a kijelölt végpontokra.

Valós idejű megfelelés (RTC) fájllista módosítása

Az RTC megfigyelési beállításokat egy végpont minden egyes fájljához megjelenítheti és módosíthatja.

1. Kattintson azon fájlokat állomásoztató végpontnak a jobb oldalán található ellipszisre, amelyek RTC megfigyelési beállításait megjeleníteni vagy módosítani kívánja.
2. Kattintson az **RTC fájllista módosítása** elemre. Megnyílik az **RTC fájllista konfiguráció** oldal, felsorolva az összes könyvtárat és fájlt, amely a végponton található. A könyvtármappa ikonon egy pipa jelzi, hogy legalább egy fájl a könyvtárban megfigyelés alatt áll.
3. Ha az a fájl, amelynek a beállításait módosítani kívánja egy könyvtárban található, akkor kattintson duplán a könyvtárra a fájlok felsorolásához. A könyvtárban található összes fájl felsorolásra kerül.
4. A végpont minden egyes fájljához felsorolásra kerülnek a megfigyelési beállítások a **Tartalom** és az **Attribútumok** oszlopban. Ha a fájlban a tartalomváltozások állnak megfigyelés alatt, akkor a jelölőnégyzet a **Tartalom** oszlopban van bejelölve. Ha a fájlban az attribútumváltozások állnak megfigyelés alatt, akkor a jelölőnégyzet az **Attribútumok** oszlopban van bejelölve. A megfigyelési beállítások módosításához jelölje be a végponton legalább egy fájl jelölőnégyzetét vagy szüntesse meg a kijelölését.
5. Kattintson a **Mentés** gombra.

Valós idejű megfelelés (RTC) fájl megfigyelési beállításainak visszaállítása az előző konfigurációra

Visszagörgethet az RTC által megfigyelt fájlok előző változatára.

1. Kattintson a végpont jobb oldalán található ellipszisre, amelyhez vissza kívánja görgetni az RTC fájl megfigyelési beállításait az előző változatra.
2. Kattintson az **RTC fájllista visszagörgetése** elemre. A megfigyelési fájlok minden egyes konfigurációs változatának időpecsétje felsorolásra kerül.
3. Kattintson azon megfigyelési beállítás konfigurációs változatának időpecsétjére, amelyhez vissza kíván térni. Az adott dátumhoz és időponthoz tartozó konfigurációs beállítások visszaállításra kerülnek.

Valós idejű megfelelés (RTC) fájllista figyelési beállításainak másolása más csoportokba

Az RTC fájlfigyelő beállítások átmásolhatók másik végpontcsoportba vagy egy specifikus végpontkészletbe.

1. Kattintson az ellipszisre annak a végpontnak a jobb oldalán, amelynek a fájlfigyelési beállításait másolni kívánja egy másik végpontcsoportba vagy egy adott végponthalmazba.
2. Kattintson az **RTC fájllista másolása** elemre. Minden egyes csoportvégpont, beleértve az **Összes rendszer** csoportot, felsorolásra kerül.
3. Válassza ki a kívánt csoportot vagy a specifikus végpontokat az alábbi módszerek egyikével:
   - Az elérhető csoportok listáján jelölje be a kívánt végpontcsoport jelölőnégyzetét. A fájllista figyelő beállítások másolásra kerülnek a csoportban található minden egyes végpontra.
   - A csoport kibontásához használja a jobbra mutató nyilat és tekintse meg a csoportban található összes végpont listáját. Jelölje be a csoport minden egyes végpontjának a jelölőnégyzetét, amelyre másolni kívánja a fájlfigyelési beállításokat.
   - Bontsa ki a végpontok listáját az **Összes rendszer** csoportban. Jelölje be a csoport minden egyes végpontjának a jelölőnégyzetét, amelyre a végpontokat másolni kívánja.
4. Kattintson az **OK** gombra. A fájlfigyelési beállítások másolásra kerültek a kiválasztott csoportba vagy a kijelölt végpontokra.

Valós idejű megfelelés (RTC) ellenőrzés futtatása

A Biztonság oldalról futtatható a valós idejű megfelelés ellenőrzés, amellyel a végpont megfelelése ellenőrizhető.

1. A végpont jobb oldalán kattintson az ellipszisre, amelyhez a valós idejű megfelelés (RTC) ellenőrzést futtatni kívánja.

2. Kattintson a **Megfelelés ellenőrzés futtatása** elemre. Megnyílik a **Megfelelés** oldal, amelyen villog a végpont sora, ezzel jelezve, hogy az ellenőrzés fut.
3. Ha valamelyik szabály alkalmazása meghiúsult, akkor a **#Meghiúsult szabályok** oszlopban megjelenik egy hibát jelző üzenet. A meghiúsult szabály megjelenítéséhez használja a végpont bal oldalán található lefelé mutató nyilat.

Megbízható végrehajtás (TE) konfigurálása

A **Biztonság** oldalon beállíthatja a Megbízható végrehajtás (TE) terméket egy adott végponthoz vagy egy végpontcsoporthoz.

1. Kattintson a végpont jobb oldalán található ellipszisre, amelyhez módosítani kívánja a TE konfigurációs beállításokat.
2. Kattintson a **TE konfigurálása** elemre. Megnyílik az TE irányelvek beállítása ablak.
3. Az összes TE konfigurációs beállítás felsorolásra kerül egy magyarázattal. Legalább egy TE konfigurációs beállítás módosításához jelölje be a jelölőnégyzetet vagy szüntesse meg a kijelölését. Néhány esetben a beállításokon végzett módosítások nem kerülnek megvalósításra a szerver újraindításáig.
4. Kattintson a **Mentés** gombra.

Megbízható végrehajtás (TE) beállításainak másolása más csoportokba

A TE konfigurációs beállításai átmásolhatók másik végpontcsoportba vagy egy specifikus végpontkészletbe.

1. Kattintson az ellipszisre annak a végpontnak a jobb oldalán, amelynek a konfigurációs beállításait másolni kívánja egy másik végpontcsoportba vagy egy adott végponthalmazba.
2. Kattintson a **TE konfiguráció másolása** elemre. Minden egyes csoportvégpont, beleértve az **Összes rendszer** csoportot, felsorolásra kerül.
3. Válassza ki a kívánt csoportot vagy a specifikus végpontokat az alábbi módszerek egyikével:
   - Az elérhető csoportok listáján jelölje be a kívánt végpontcsoport jelölőnégyzetét. A konfigurációs beállítások másolásra kerülnek a csoportban található minden egyes végpontra.
   - Bontsa ki a csoportot és tekintse meg a csoportban található összes végpont listáját. Jelölje be a csoport minden egyes végpontjának a jelölőnégyzetét, amelyre másolni kívánja a konfigurációs beállításokat.
   - Bontsa ki a végpontok listáját az **Összes rendszer** csoportban. Jelölje be a csoport minden egyes végpontjának a jelölőnégyzetét, amelyre a végpontokat másolni kívánja.
4. Kattintson az **OK** gombra. A konfigurációs beállítások másolásra kerültek a kiválasztott csoportba vagy a kijelölt végpontokra.

Megbízható végrehajtás (TE) fájllista módosítása

Az TE megfigyelési beállításokat egy végpont minden egyes fájljához megjelenítheti és módosíthatja.

1. Kattintson azon fájlokat állomásoztató végpontnak a jobb oldalán található ellipszisre, amelyek TE megfigyelési beállításait megjeleníteni vagy módosítani kívánja.
2. Kattintson a **TE fájllista módosítása** elemre. Megnyílik a **TE fájllista konfiguráció** oldal, felsorolva az összes könyvtárat és fájlt, amely a végponton található. A könyvtármappa ikonon egy pipa jelzi, hogy legalább egy fájl a könyvtárban megfigyelés alatt áll.
3. Ha az a fájl, amelynek a beállításait megjeleníteni vagy módosítani kívánja egy könyvtárban található, akkor kattintson duplán a könyvtárra a fájlok felsorolásához. A könyvtárban található összes fájl felsorolásra kerül.
4. A végpont minden egyes fájljához felsorolásra kerülnek a megfigyelési beállítások a **TE** és a **Változékony** oszlopban. Ha a fájlban a tartalomváltozások figyelése történik, akkor a jelölőnégyzet a **TE** oszlopban van bejelölve. Ha a fájlban csak az engedélyváltozások figyelése történik, akkor a jelölőnégyzet a **Változékony** oszlopban van bejelölve. A megfigyelési beállítások módosításához jelölje be a végponton legalább egy fájl jelölőnégyzetét vagy szüntesse meg a kijelölését.
5. Kattintson a **Mentés** gombra.

Megbízható végrehajtás (TE) fájllista megfigyelési beállításainak másolása más csoportokba

A TE fájlfigyelő beállítások átmásolhatók másik végpontcsoportba vagy egy specifikus végpontkészletbe.

1. Kattintson az ellipszisre annak a végpontnak a jobb oldalán, amelynek a fájlfigyelési beállításait másolni kívánja egy másik végpontcsoportba vagy egy adott végponthalmazba.
2. Kattintson a **TE fájllista másolása** elemre. Minden egyes csoportvégpont, beleértve az **Összes rendszer** csoportot, felsorolásra kerül.
3. Válassza ki a kívánt csoportot vagy a specifikus végpontokat az alábbi módszerek egyikével:
   - Az elérhető csoportok listáján jelölje be a kívánt végpontcsoport jelölőnégyzetét. A fájllista figyelő beállítások másolásra kerülnek a csoportban található minden egyes végpontra.
   - Bontsa ki a csoportot és tekintse meg a csoportban található összes végpont listáját. Jelölje be a csoport minden egyes végpontjának a jelölőnégyzetét, amelyre másolni kívánja a fájlfigyelési beállításokat.
   - Bontsa ki a végpontok listáját az **Összes rendszer** csoportban. Jelölje be a csoport minden egyes végpontjának a jelölőnégyzetét, amelyre a végpontokat másolni kívánja.
4. Kattintson az **OK** gombra. A fájlfigyelési beállítások másolásra kerültek a kiválasztott csoportba vagy a kijelölt végpontokra.

További PowerSC szolgáltatások állapotának megjelenítése

A Biztonság oldalról megjelenítheti a PowerSC szolgáltatások állapotát, mint például a Megbízható rendszerbetöltés, Megbízható tűzfal és a Megbízható naplózás. Ezenkívül megjelenítheti a Megbízható hálózati kapcsolat (TNC) frissítések állapotát a végponton.

1. A főoldalon válassza ki a **Biztonság** lapot. Megnyílik a **Biztonság** oldal.
2. A PowerSC TNC összetevője szolgál a biztonsági javítások ellenőrzésére és frissítésére az egyes végpontokon. A végpontok táblázatában a **Naprakész TNC-n keresztül** oszlop jelzi, hogy a végpont naprakész-e a TNC szerver perspektívájából. A műszerfal fejléccsíkján a **Naprakész TNC-n keresztül** szakasz megjeleníti a csoportban található végpontok százalékos arányát, amelyek naprakészek. Ha el kívánja távolítani a TNC frissítési információk megjelenítését a **Biztonság** oldalról, akkor tegye a következőket:
   a. A főoldal menüsorán kattintson a **Nyelvek és beállítások** ikonra.
   b. Kattintson a **Résztermék használat** elemre.
   c. Állítsa be a **Naprakész TNC-n keresztül** váltókapcsolót kikapcsolva állásba.
   d. A megjelenítés visszaállításához húzza a **Naprakész TNC-n keresztül** váltókapcsolót bekapcsolva állásba.
3. A végponttáblázatban a **TB** oszlop jelzi, hogy a PowerSC megbízható rendszerbetöltés elérhető-e a végponton. A műszerfal fejléccsíkján a **Megbízható rendszerbetöltés** rész megjeleníti a jelenleg kiválasztott csoport végpontjainak százalékos arányát, amelyen a PowerSC Megbízható rendszerbetöltés aktiválva van. Ha el kívánja távolítani a PowerSC megbízható rendszerbetöltési információk megjelenítését a **Biztonság** oldalról, akkor tegye a következőket:
   a. A főoldal menüsorán kattintson a **Nyelvek és beállítások** ikonra.
   b. Kattintson a **Résztermék használat** elemre.
   c. Húzza a **Megbízható rendszerbetöltés** elemhez tartozó váltókapcsolót kikapcsolva állásba.
   d. A megjelenítés visszaállításához húzza a váltókapcsolót bekapcsolva állásba.
4. A végponttáblázatban a **TF** oszlop jelzi, hogy a PowerSC megbízható tűzfal elérhető-e a végponton. A műszerfal fejléccsíkján a **Megbízható tűzfal** rész megjeleníti a jelenleg kiválasztott csoport végpontjainak százalékos arányát, amelyen a PowerSC Megbízható tűzfal aktív. Ha el kívánja távolítani a Megbízható tűzfal információinak megjelenítését a **Biztonság** oldalról, akkor tegye a következőket:
   a. A főoldal menüsorán kattintson a **Nyelvek és beállítások** ikonra.
   b. Kattintson a **Résztermék használat** elemre.
   c. Húzza a **Megbízható tűzfal** elemhez tartozó váltókapcsolót kikapcsolva állásba.
   d. A megjelenítés visszaállításához húzza a váltókapcsolót bekapcsolva állásba.

5. A végponttáblázatban a **TL** oszlop jelzi, hogy a PowerSC megbízható naplózás elérhető-e a végponton. A műszerfal fejléccsíkján a **Megbízható naplózás** rész megjeleníti a jelenleg kiválasztott csoport végpontjainak százalékos arányát, amelyen a PowerSC Megbízható naplózás aktív. Ha el kívánja távolítani a Megbízható naplózás információinak megjelenítését a **Biztonság** oldalról, akkor tegye a következőket:
   a. A főoldal menüsorán kattintson a **Nyelvek és beállítások** ikonra.
   b. Kattintson a **Résztermék használat** elemre.
   c. Húzza a **Megbízható naplózás** elemhez tartozó váltókapcsolót kikapcsolva állásba.
   d. A megjelenítés visszaállításához húzza a váltókapcsolót bekapcsolva állásba.

Megbízható végrehajtás figyelésének ki/bekapcsolása

A Megbízható végrehajtás (TE) figyelése be- és kikapcsolható. A TE figyelés kikapcsolható és a bekapcsolása ütemezhető egy adott időköz alapján.

1. A **Megbízható végrehajtás átkapcsolása** ikonra.
2. A legördülő menüből válassza ki az alábbi beállítások egyikét:
   - **Összes végpont bekapcsolása** a TE figyelés bekapcsolásához minden egyes végponthoz.
   - **Összes végpont kikapcsolása** a TE figyelés kikapcsolásához minden egyes végponthoz.
3. Ha a TE figyelés kivan kapcsolva, akkor elérhetővé válnak a beállítások a TE figyelés újraindítási időpontjának beállításához. Az alábbi újraindítási időpontok közül választhat:
   - **1 óra**
   - **5 óra**
   - **1 nap**
   - **1 hét**
   - **Soha**
4. Kattintson a **Mentés** gombra.

E-mail értesítés küldése biztonsági esemény előfordulásakor

A Biztonság oldalról e-mail értesítést küldhet legalább egy címzettnek, ha biztonsági esemény történik.

1. A főoldalon válassza ki a **Biztonság** lapot. Megnyílik a **Biztonság** oldal.
2. A menüsoros jobb sarkában kattintson az **E-mail beállítások** ikonra. Megnyílik az **E-mail beállítások** ablak.
3. Jelölje be a **Küldés nekem** e-mail jelölőnégyzetet.
4. Adja meg minden egyes címzett e-mail címét vesszővel tagolva a **Címek (vesszővel tagolt)** mezőben.

Jelentések kezelése

A PowerSC grafikus felhasználói felület Jelentések oldaláról számos jelentés elérhető.

Az alábbi jelentések érhetők el:

- A **Megfelelés áttekintése** jelentés a magas szintű információk pillanatképe, amely a felület **Megfelelés** oldalán tekinthető meg.
- A **Megfelelés részletei** jelentés a magas szintű és a részletes információk pillanatképe, amely a **Megfelelés** oldalon tekinthető meg.
- A **Fájlintegritás áttekintése** jelentés a magas szintű információk pillanatképe, amely a felület **Biztonság** oldalán tekinthető meg.
- A **Fájlintegritás részletei** jelentés a magas szintű és a részletes információk pillanatképe, amely a **Biztonság** oldalon tekinthető meg.
- **Kombinált megfelelés és FIM**

Alapértelmezésben a **Jelentések** oldalon megjelenik a **Megfelelés áttekintése** és a **Fájlintegritás áttekintése** jelentés az **Összes rendszer** csoporthoz. Nincs megadva alapértelmezett csoport a **Megfelelés részletei**, **Fájlintegritás részletei** és a **Kombinált megfelelés és FIM** jelentéshez.

Az **Összes rendszer** csoporthoz és a felhasználó által megadott csoportokhoz előállítható bármelyik jelentéstípus. A jelentés előállítható a csoport összes végpontjához vagy a végpontok egy részhalmazához. A jelentés előállítása után a jelentés terjesztése ütemezhető HTML formátumú e-mail és CSV fájl formátumban, igény szerint legalább egy címzetthez vagy minden napos gyakoriságban.

A **Jelentések** oldalon megjelenő jelentések listája a felhasználó bejelentkezési azonosítójától függően változik. A jelentések előállíthatók csak azokhoz a végpontokhoz, amelyeket a felhasználó kezel a bejelentkezési azonosítója alapján. Minden egyes jelentés, amely egy adott munkamenetben kerül előállításra, a következő munkamenet megnyitásakor felsorolásra kerül.

Jelentéscsoport kiválasztása

Minden egyes jelentés futtatható az **Összes rendszer** csoporthoz és a felhasználó által megadott csoportokhoz. A jelentés futtatása választható a csoportba tartozó összes végponthoz vagy a végpontok egy részhalmazához.

1. A főoldalon kattintson a **Jelentések** lapra. Megnyílik a **Jelentések** oldal.
2. A futtatni kívánt jelentéstípus jobb oldalán kattintson az ellipszisre.
3. Kattintson a **Csoport módosítása** elemre.
4. Megnyílik az összes elérhető csoportot felsoroló legördülő lista. Kattintson a választógombra a csoport mellett, amelyhez a jelentést futtatni kívánja. Kattintson a **Megerősítés** elemre. A jelentés fut és a főoldal tartalma frissül a kiválasztott csoport információival.
5. A jelentés futtatásához a végpontok egy részhalmazához, bontsa ki az **Összes rendszer** csoportot. Megjelenik az összes elérhető végpont listája. Jelölje be a jelölőnégyzetet minden egyes végpont mellett, amelyet bele kíván foglalni a jelentésbe. A jelentés futtatásához kattintson a **Megerősítés** elemre.

   Megjegyzés: Ha a jelentést egy specifikus végpontcsoporton kívánja futtatni, akkor létrehozhatja az adott végpontokat tartalmazó csoportot. A csoport létrehozásával időt spórolhat és azt az összes felhasználó használhatja, mivel a csoportok globálisak (a felület összes felhasználója számára megtekinthető).
6. Kikereshet egy adott végpontot is a végpont nevének megadásával a keresési mezőben. A jelentés futtatásához a kívánt végponthoz kattintson a **Megerősítés** elemre.

Jelentések terjesztése e-mailben

Miután beállította a csoportot egy adott jelentéshez, a jelentést ütemezheti terjesztésre HTML-formátumú e-mail vagy CSV fájl formájában. Az e-mail elküldését ütemezheti több e-mail címzettnek is azonnali vagy minden napos gyakoriságban.

A jelentés CSV változatának elküldése lehetővé teszi a címzett számára a jelentésadatok betöltését egy táblázatkezelőbe vagy a jelentés importálását egy másik szoftveralkalmazásba, amely feldolgozza a CSV fájlokat. A CSV fájloknak nincs grafikus vagy kezelőfelület alapelve. Az áttekintő jelentésből előállított CSV fájl első sorként az egyes oszlopfejléceket tartalmazza vesszővel tagolva. Az ezt követő sorok minden egyes oszlophoz felsorolják a végpontot és az értékeket.

A részletes jelentésekből több CSV fájl kerül előállításra. Az első CSV fájl formátuma hasonló az áttekintő jelentéshez. A jelentés minden egyes részletszintjéhez egy önálló CSV fájl kerül előállításra. Például a Fájlintegritás részletei jelentésben a következő részletszintek állítanak elő önálló CSV fájlt:

- **TE konfiguráció**
- **RTC konfiguráció**
- **Résztermék állapota**

1. A főoldalon kattintson a **Jelentések** lapra. Megnyílik a **Jelentések** oldal.

2. Az elérhető jelentések listájáról válassza ki a terjeszteni kívánt jelentést. A jelentés fut és a főoldal tartalma frissítésre kerül.
3. A terjeszteni kívánt jelentés jobb oldalán kattintson az ellipszisre.
4. Kattintson az **E-mail beállítások** elemre. Megnyílik a Jelentés küldése e-mailben ablak.
5. Adja meg minden egyes címzett e-mail címét a **Címek** mezőben. Válassza el az egyes címzettek címeit pontosvesszővel (;).
6. Adja meg az e-mail leírását a **Tárgy** mezőben.
7. Válasszon az alábbi lehetőségek közül:
   - Jelölje be a **Küldés minden nap a következő időpontban** jelölőnégyzetet a jelentés elküldéséhez a címzetteknek minden nap. Adja meg a helyi időpontot a jelentés elküldéséhez az időpont kiválasztásával órában és percben. Kattintson a **Mentés és bezárás** elemre. A jelentés minden nap a megadott időpontban kerül elküldésre.
   - A jelentés elküldéséhez kattintson a **KÜLDÉS AZONNAL** elemre. A jelentés elküldésre kerül és az ablak bezárul.

PowerSC Standard Edition parancsok

A PowerSC Standard Edition biztosít parancsokat, amelyek lehetővé teszik a parancssori kommunikációt a Megbízható tűzfal összetevővel és a Megbízható hálózati kapcsolat összetevővel.

chvfilt parancs

Cél

Módosítja a meglévő virtuális LAN kereszteződési szűrőszabály értékeit.

Szintaxis

chvfilt [**-v <4|6>**] **-n fid** [**-a <D|P>**] [**-z <forrás_vlan>**] [**-Z <cél_vlan>**] [**-s <forrás_cím>**] [**-d <cél_cím>**] [**-o <forrás_port_műv>**] [**-p <forrás_port>**] [**-O <cél_port_műv>**] [**-P <cél_port>**] [**-c <protokoll>**]

Leírás

A **chvfilt** parancs segítségével módosíthatja egy virtuális LAN kereszteződési szűrőszabály meghatározását a szűrőszabály táblában.

Kapcsolók

-a Megadja a műveletet. Az érvényes értékek a következők:
- D (Megtagadás): Forgalom blokkolása
- P (Engedélyezés): Forgalom engedélyezése

-c Különböző protokollokat ad meg, amelyekre a szűrőszabály alkalmazható. Az érvényes értékek a következők:
- udp
- icmp
- icmpv6
- tcp
- any

-d A cél címet adja meg IPv4 vagy IPv6 formátumban.

-m Megadja a forrás cím maszkját.

-M Megadja a cél cím maszkját.

-n Megadja a módosítandó szűrőszabály szűrőazonosítóját.

-o Megadja a forrás portot vagy az Internet vezérlőüzenet protokoll (ICMP) típus műveletet. Az érvényes értékek a következők:
- lt
- gt
- eq
- any

-O Megadja a cél portot vagy az ICMP kód műveletet. Az érvényes értékek a következők:
- lt
- gt
- eq

- any

-p Megadja a forrás portot vagy az ICMP típust.

-P Megadja a cél portot vagy az ICMP kódot.

-s A forrás címet adja meg v4 vagy v6 formátumban.

-v Megadja a szűrőszabály tábla IP változatát. Az érvényes értékek 4 és 6.

-z Megadja a forrás logikai partíció virtuális LAN azonosítóját.

-Z Megadja a cél logikai partíció virtuális LAN azonosítóját.

Kilépési állapot

Ez a parancs a következő kilépési értékeket adja vissza:

0 Sikeres befejeződés.

>0 Hiba történt.

Példák

1. Egy kernelben létező érvényes szűrőszabály módosításához írja be a parancsot a következők szerint:
   ```
   chvfilt -n 1 -v4 -a P -z 100 -Z 300 -o eq -p 23 -O lt -P 345 -c tcp
   ```
2. Ha egy szűrőszabály (n=2) nem létezik a kernelben, akkor a kimenet a következő lesz:
   ```
   chvfilt -n 2 -v4 -a P -z 100 -Z 300 -o eq -p 23 -O lt -P 345 -c tcp
   ```

   A rendszer a kimenetet a következőképpen jeleníti meg:
   ```
   ioctl(QUERY_FILTER) failed no filter rule err=2
   A szűrőszabály nem módosítható.
   ```

---

genvfilt parancs

Cél

Hozzáad egy virtuális szűrőszabályt a virtuális LAN (VLAN) kereszteződéshez az azonos IBM Power Systems szerveren lévő logikai partíciók között.

Szintaxis

genvfilt -v <4|6> -a <D|P> -z <forrás_vlan> -Z <cél_vlan> [**-s <forrás_cím>**] [**-d <cél_cím>**] [**-o <forrás_port_műv>**] [**-p <forrás_port>**] [**-O <cél_port_műv>**] [**-P <cél_port>**] [**-c <protokoll>**]

Leírás

A **genvfilt** parancs hozzáad egy virtuális szűrőszabályt a virtuális LAN (VLAN) kereszteződéshez az azonos IBM Power Systems szerveren lévő logikai partíciók (LPAR) között.

Kapcsolók

-a Megadja a műveletet. Az érvényes értékek a következők:
- D (Megtagadás): Forgalom blokkolása
- P (Engedélyezés): Forgalom engedélyezése

-c Különböző protokollokat ad meg, amelyekre a szűrőszabály alkalmazható. Az érvényes értékek a következők:
- udp
- icmp
- icmpv6

- tcp
- any

-d A cél címet adja meg v4 vagy v6 formátumban.

-m Megadja a forrás cím maszkját

-M Megadja a cél cím maszkját.

-o Megadja a forrás portot vagy az Internet vezérlőüzenet protokoll (ICMP) típus műveletet. Az érvényes értékek a következők:
- lt
- gt
- eq
- any

-O Megadja a cél portot vagy az ICMP kód műveletet. Az érvényes értékek a következők:
- lt
- gt
- eq
- any

-p Megadja a forrás portot vagy az ICMP típust.

-P Megadja a cél portot vagy az ICMP kódot.

-s A forrás címet adja meg IPv4 vagy IPv6 formátumban.

-v Megadja a szűrőszabály tábla IP változatát. Az érvényes értékek 4 és 6.

-z Megadja a forrás LPAR virtuális LAN azonosítóját. A virtuális LAN azonosítónak az 1 - 4096 tartományba kell esnie.

-Z Megadja a cél LPAR virtuális LAN azonosítóját. A virtuális LAN azonosítónak az 1 - 4096 tartományba kell esnie.

Kilépési állapot

Ez a parancs a következő kilépési értékeket adja vissza:

0 Sikeres befejeződés.

>0 Hiba történt.

Példák

1. Egy szűrőszabály hozzáadásához, amely engedélyezi a TCP adatokat a 100-as forrás VLAN azonosítóról a 200-as cél VLAN azonosítóra megadott portokon keresztül, írja be a parancsot a következők szerint:

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

Kapcsolódó hivatkozás:

“mkvfilt parancs” oldalszám: 150

“vlantfw parancs” oldalszám: 169

lsvfilt parancs

Cél

Felsorolja a virtuális LAN kereszteződési szűrőszabályokat a szűrő táblából.

Szintaxis

lsvfilt [**-a**]

Leírás

Az **lsvfilt** parancs arra szolgál, hogy felsorolja a virtuális LAN kereszteződési szűrőszabályokat és azok állapotát.

Kapcsolók

-a Csak az aktív szűrőszabályokat sorolja fel.

Kilépési állapot

Ez a parancs a következő kilépési értékeket adja vissza:

0 Sikeres befejeződés.

>0 Hiba történt.

Példák

1. A kernelben lévő összes aktív szűrőszabály felsorolásához írja be a parancsot a következők szerint:

```
lsvfilt -a
```

Kapcsolódó fogalmak:

“Szabályok deaktiválása” oldalszám: 105
A Megbízható tűzfal szolgáltatásban a VLAN hálózatok közötti továbbítást engedélyező szabályok deaktiválhatók.

---

mkvfilt parancs

Cél

Aktiválja a **genvfilt** parancs által meghatározott virtuális LAN kereszteződési szűrőszabályokat.

Szintaxis

mkvfilt -u

Leírás

Az **mkvfilt** parancs aktiválja a **genvfilt** parancs által meghatározott virtuális LAN kereszteződési szűrőszabályokat.

Kapcsolók

-u Aktiválja a szűrőszabály táblában lévő szűrőszabályokat.

Kilépési állapot

Ez a parancs a következő kilépési értékeket adja vissza:

0 Sikeres befejeződés.

>0 Hiba történt.

Példák

1. A szűrőszabályok aktiválásához a kernelben, írja be a parancsot a következők szerint:

```
mkvfilt -u
```

Kapcsolódó hivatkozás:

“genvfilt parancs” oldalszám: 148

pmconf parancs

Cél

Jelentéseket készít és felügyeli a Megbízható hálózati kapcsolat javításkezelő (TNCPM) szervert a technológia szintek és TNC szerverek regisztrálásával a legújabb frissítések beszerzéséhez, illetve a TNCPM állapotára vonatkozó jelentések előállításával.

Megjegyzés: A TNCPM szerver csak AIX 7.2. változaton, a 7100-02 technológia szinten futtatható, hogy a javítócsomagok metaadatai letölthetők legyenek.

Szintaxis

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

pmconf rmtncpm

pmconf start

pmconf stop

pmconf init -i <*letöltési időköz*> **-l** <*TL lista*> **-A** [**-P** <*letöltési útvonal*>] [**-x** <*ifix időköz*>] [**-K** <*ifix kulcs*>]

pmconf add -l *TL_lista*

pmconf add -o <*csomagnév*> -V <*verziószám*> -T [installp|rqm] -D <*felhasználó által megadott útvonal*>

pmconf add -p <*SP_lista*> [**-U** <*felhasználó_által_meghatározott_SP_útvonal*>]

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

pmconf add -y <*tanácsadó fájl*> **-v** <*aláírási fájl*> **-e**

pmconf chtncpm attribute = *érték*

pmconf delete -l <*TL_lista*>

pmconf delete -o <*csomagnév*> -V <*verziószám*>

pmconf delete -p <*SP_lista*>

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

pmconf export -f *fájlnév*

pmconf get -o <package> -V <version> -T <installp | rpm> -D <download directory>

pmconf get -L -o <package> -V <version | all> -T <installp | rpm>

pmconf get -L -p <SP>

pmconf get -p <SP> -D <download directory>

pmconf hist -d

pmconf hist -u

pmconf import -f *tanúsítványfájl_neve* **-k** *kulcsfájl_neve*

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

pmconf list -a *SP*

pmconf list -C

pmconf list -l *SP*

pmconf list -o <*csomagnév*> -V <*verziószám*>

pmconf list -o [-c] [-q]

pmconf log loglevel = info | error | none

pmconf modify -i <*letöltési_időköz*>

pmconf modify -P <*letöltési_útvonal*>

pmconf modify -g <*yes vagy no az összes licenc elfogadásához*>

pmconf modify -t <*APAR_típusok_listája*>

pmconf modify -x <*ifix_időköz*>

pmconf modify -K <*ifix_kulcs*>

pmconf proxy display

pmconf proxy [enable=yes | no] [host=<hostname>] [port=<portnum>]

pmconf restart

pmconf status

Leírás

A **pmconf** parancs függvényei a következők:

Javításlerakat kezelése
Technológia szinteket regisztrál vagy megszünteti ezek regisztrálását; megszünteti TNC szerverek regisztrálását. A TNCPM minden olyan technológia szinthez létrehoz egy javításlerakatot, amely a legutóbbi javításokat, **lslpp** információkat (például a telepített fájlkészletekkel vagy fájlkészletfrissítésekkel kapcsolatos információkat), illetve az adott technológia szintre vonatkozó biztonsági javítási információkat tartalmazza.

Jelentéskészítés
Jelentéseket állít elő a TNCPM állapotáról.

A **pmconf** parancs segítségével a következő műveletek hajthatók végre:

Elem	Leírás
add	Regisztrál egy új technológia szintet a TNCPM használatával.
chtncpm	Módosítja a tnccs.conf fájlban lévő attribútumokat. Ahhoz, hogy a módosítások érvénybe lépjenek a TNCPM szerveren, egy kifejezett **start** utasítás kiadása szükséges.
delete	Megszünteti egy technológia szint regisztrálását a TNCPM szerver használatával.
get	Információk megjelenítése és letöltése az elérhető biztonsági javításokról és nyílt forrású csomagokról.
history	Megjeleníti a frissítési és letöltési előzményeket.
list	Megjeleníti a TNCPM információit.
log	Beállítja a TNC összetevők naplózási szintjét.
mktncpm	Létrehozza a TNCPM szervert.
modify	Módosítja a tncpm.conf attribútumokat.
proxy	Proxy szerver paraméter beállításainak kezelése.
rmtncpm	Eltávolítja a TNCPM szervert.
start	Elindítja a TNCPM szervert.
stop	Leállítja a TNCPM szervert.

Kapcsolók

Elem	Leírás
-A	Elfogadja az összes licencszerződést a kliensfrissítések végrehajtásakor.
-a <tanácsadófájl>	Megadja az **ifix** paraméternek megfelelő tanácsadófájlt. Ha nincs megadva tanácsadófájl, akkor az **ifix** paraméter nem tekinti a köztes javítás Általános sebezhetőségek és veszélyeztetettség (CVE) címeként.
-a *SP*	Előállít egy jelentést a javítócsomag biztonsági jogosult programelemzési jelentés (APAR) információiról. Az *SP* paraméter formátuma REL00-TL-SP (például 6100-01-04 a 6.1 változat 01-es technológia szintjéhez tartozó 04-es javítócsomagot ábrázolja).
-e <ifix_fájl>	Megadja a TNCPM szerverhez hozzáadott köztes javításokat.
-i *letöltési_időköz*	Megadja az időközt, amely alapján a TNCPM ellenőrzi az új javítócsomagok megjelenését a regisztrált technológia szintekhez. Az időköz egy egész szám érték, amely perceket vagy napokat ábrázol a következő formátumban: **d** (nincs megadva, ha nincsenek napok): **h** (órák): **m** (perc). A *letöltési_időköz* támogatott tartománya 30 - 525600 perc.
-K <ifix_kulcs>	Megadja a tanácsadók és köztes javítások hitelesítéséhez használt IBM AIX Product Security Incident Response Tool (PSIRT) nyilvános kulcsát. Ez a nyilvános kulcs egy PGP nyilvános kulcs szerverről tölthető le, a **0x28BFAA12** azonosító használatával.
-L	Megadja a listázás vagy a csak keresés módot.
o *csomagnév*	A nyílt forrású csomag neve, amelyen a keresést vagy letöltést végre kell hajtani.
-P *javításlerakat_útvonala*	Megadja a TNCPM által letöltésre kerülő javításlerakatok letöltési könyvtárát. Az alapértelmezett könyvtár a **/var/tnc/tncpm/fix_repository**.
-p *SP_lista*	Megadja a letöltendő javítócsomagok listáját. A lista egy REL00-TL-SP formátumú elemekből álló vesszővel elválasztott lista (például 6100-01-04 a 6.1 változat 01-es technológia szintjéhez tartozó 04-es javítócsomagot ábrázolja). Az -U kapcsoló használata esetén csak a javítócsomagot (SP) adja meg.
-t *APAR_típusok_listája*	Megadja az APAR típusokat, amelyeket a TNCPM a kliensfrissítésekhez és TNC szerver felsorolásokhoz támogat. A biztonsági APAR javítások mindig támogatottak. Az APAR_típusok_listája paraméter a következő típusok vesszővel elválasztott listáját tartalmazhatja: HIPER, FileNet Process Engine, Enhancement.
T *csomagtípus*	Megadja a nyílt forrású csomag típusát, amelyen a keresést vagy letöltést végre kell hajtani
-U *felhasználó_által_megadott_javításlerakat*	Megadja a felhasználó által megadott javításlerakat útvonalát. Adja meg a kliensek ellenőrzéséhez és frissítéseihez használt javításlerakattal társított kiadást, technológia szintet és javítócsomagot.
-s	Előállít egy jelentést a regisztrált javítócsomagokról.
-l *SP*	Előállít egy jelentést a javítócsomag **lslpp** információiról. Az *SP* paraméter formátuma REL00-TL-SP (például 6100-01-04 a 6.1 változat 01-es technológia szintjéhez tartozó 04-es javítócsomagot ábrázolja).
-u	Előállít egy jelentés a kliens frissítési előzményeiről.
V *verziószám*	A nyílt forrású csomag verziószáma, amelyen a keresést vagy letöltést végre kell hajtani. Az (-L) keresési módban az “all” értéket kell megadni a megadott csomag összes elérhető verziószámának kikereséséhez.
-d	Előállít egy jelentés a javítócsomag letöltések előzményeiről.
-C	Előállít egy jelentés a szervertanúsítványról.
-f *fájlnév*	Megadja a tanúsítványfáj nevét.
-k	Megadja a fájlt, amelyből a tanúsítványkulcsot egy importálási művelet során be kell olvasni.

-c	Megjeleníti a felhasználói attribútumokat pontosvesszővel elválasztott rekordokban, az alábbiak szerint:
	`# name: attribútum1: attribútum2: ...`
	`policy: érték1: érték2: ...`

-v <*aláírásfájl*>	Megadja az aláírásfájlt az IBM AIX sebezhetőségi tanácsadóhoz.
-y <*tanácsadófájl*>	Megad egy IBM AIX sebezhetőségi tanácsadó fájlt.
-q	Kikapcsolja a fejlécinformációkat.

Elem	Leírás
-x <*ifix_időköz*>	Percekben megadja az időközt, amely szerint új köztes javításokat kell keresni és letölteni. Ha az érték 0-ra van beállítva, akkor a köztes javítások automatikus letöltése és az értesítés le van tiltva. Az alapbeállítás 24 óra. Az <*ifix interval*> támogatott tartománya 30 - 525600 perc.

Kilépési állapot

Ez a parancs a következő kilépési értékeket adja vissza:

Elem	Leírás
0	A parancs sikeresen lefutott, és minden kért módosítás megtörtént.
>0	Hiba történt. A kiírt hibaüzenet további részleteket biztosít a hiba típusáról.

Példák

1. A TNCPM, inicializálásához adja ki a következő parancsot:
   ```
   pmconf init -f 10080 -l 5300-11,6100-00
   ```
2. A TNCPM démon létrehozásához adja ki a következő parancsot:
   ```
   mktncpm pmport=55777 tncserver=11.11.11.11:77555
   ```
3. A szerver elindításához adja ki a következő parancsot:
   ```
   pmconf start
   ```
4. A szerver leállításához adja meg a következő parancsot:
   ```
   pmconf stop
   ```
5. Egy új technológia szint regisztrálásához a TNCPM használatával, adja ki a következő parancsot:
   ```
   pmconf add -l 6100-01
   ```
6. Egy technológia szint regisztrálásának megszüntetéséhez a TNCPM összetevőben, adja ki a következő parancsot:
   ```
   pmconf delete -l 6100-01
   ```
7. Egy 11.11.11.11 IP címmel rendelkező TNC szerver regisztrációjának megszüntetéséhez a TNCPM szerveren, adja ki a következő parancsot:
   ```
   pmconf delete -t 11.11.11.11
   ```
8. Egy korábbi javítócsomag újabb változatának regisztrálásához a TNCPM szerveren, adja ki a következő parancsot:
   ```
   pmconf add -s 6100-01-04
   ```
9. Egy korábbi javítócsomag regisztrálásának megszüntetéséhez a TNCPM összetevőben, adja ki a következő parancsot:
   ```
   pmconf delete -s 6100-01-04
   ```
10. Az egyes regisztrált technológia szintekhez tartozó javításlerakatokról készült jelentés előállításához adja ki a következő parancsot:
    ```
    pmconf list -s
    ```
11. Egy regisztrált technológia szint **lslpp** információiról készült jelentés előállításához adja ki a következő parancsot:
    ```
    pmconf list -l 6100-01-02
    ```
12. A frissítési előzményekből készült jelentés előállításához adja ki a következő parancsot:
    ```
    pmconf hist -u
    ```
13. A letöltési előzményekből készült jelentés előállításához adja ki a következő parancsot:
    ```
    pmconf hist -d
    ```
14. A szervertanúsítványról készült jelentés előállításához adja ki a következő parancsot:
    ```
    pmconf list -C
    ```
15. Egy javítócsomag biztonsági APAR információiról készült jelentés előállításához adja ki a következő parancsot:
    ```
    pmconf list -a 6100-01-02
    ```
16. Egy szervertanúsítvány importálásához adja ki a következő parancsot:

```
pmconf import -f /tmp/server.txt -k /tmp/server-cert-key.txt
```

17. Egy szervertanúsítvány exportálásához adja ki a következő parancsot:

```
pmconf export -f /tmp/server.txt
```

18. Az ‘emacs’ nyílt forrású csomag összes elérhető rpm formátumú változatának megjelenítéséhez adja ki a következő parancsot:

```
pmconf get -L -o emacs -V all -T rpm
```

19. Az ‘lsof’ nyílt forrású csomag 4.5.1. változatának letöltéséhez rpm formátumban a /tmp/new_lsof könyvtárba, adja ki a következő parancsot:

```
mkdir /tmp/new_lsof
pmconf get -o lsof -V 4.5.1 -T rpm -D /tmp/new_lsof
```

20. Az OpenSSH összes elérhető változatának megjelenítéséhez installp formátumban, adja ki a következő parancsot:

```
pmconf get -o openssh -T installp -L -V all
```

21. Az aktuális proxy konfigurációs beállítások megjelenítéséhez, amelyeket a cURL használt a nyílt forrású csomagok vagy biztonsági javítások letöltésekor, adja ki a következő parancsot:

```
pmconf proxy display
```

22. A proxykonfiguráció beállításához tiltott állapotra, adja ki a következő parancsot:

```
pmconf proxy enable=no
```

23. A proxy engedélyezéséhez és a hoszt beállításához ‘myProxyServer’ értékre a 9876-os porton, adja ki a következő parancsot:

```
pmconf proxy enable=yes host=myProxyServer port=9876
```

24. A használandó proxy szerver port módosításához adja ki a következő parancsot:

```
pmconf proxy port=1234
```

25. Az ismert sebezhetőségek megjelenítéséhez, amelyeket a a biztonsági javítások megadtak a 7100-03-02-es javítócsomag szinthez, adja ki a következő parancsot:

```
 pmconf get -L -p 7100-03-02
```

26. A 7200-00-01-es javítócsomag szint letöltéséhez a /tmp/ifixes_for_7.2.0.1 könyvtárba, de nem alkalmazva, adja ki a következő parancsokat:

```
mkdir /tmp/ifixes_for_7.2.0.1
pmconf get -p 7200-00-01 -D /tmp/ifixes_for_7.2.0.1
```

psconf parancs

Cél

Jelentéseket készít és felügyeli a Megbízható hálózati kapcsolat (TNC) szervert, a TNC klienst, a TNC IP hivatkozót (IPRef) és a Szolgáltatásfrissítés-kezelő segéd (SUMA) összetevőt. Felügyeli a fájlkészlet és javításkezelési irányelveket a végpont (szerver és kliens) integritása tekintetében a hálózati kapcsolat létrejöttekor vagy az után, hogy megvédje a hálózatot a fenyegetésektől és támadásoktól.

Szintaxis

TNC szerver műveletek:

psconf mkserver [**tncport=**<*port*>] **pmserver=**<*hoszt:port*> [tsserver=<host>] [**recheck_interval=**<*idő_percben*> | **d** (days) : **h** (hours) : **m** (minutes)] [**dbpath** = <*felhasználó által megadott könyvtár*>] [**default_policy=**<*igen* | *nem* >] [**clientData_interval=**<*idő_percben*> | **d** (days) : **h** (hours) : **m** (minutes)] [**clientDataPath=**<*teljes_útvonal*>]

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

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

psconf chserver attribute = *érték*

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

psconf add -F <*FS_irányelv_neve*> -r <*összeépítési_info*> [**apargrp=** [**±**]<*aparcsop1, aparcsop2.. >*] [*ifixgrp*=[+|-]<*ifixgrp1,ifixgrp2...>*]

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

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

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

psconf add -I ip= [**±**]<*hoszt1, hoszt2...*>

psconf delete { **-F** <*FS_irányelv_neve*> | **-G** <*ip_csoport_neve*> | **-P** <*irányelvnév*> | **-A** <*apar_csoport*> | **-V** <*ifix_csoport*>}

psconf delete -H -i <*hoszt* | **ALL**> **-D** <*éééé-hh-nn*>

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

psconf certdel -i <*hoszt*>

psconf verify -i <*hoszt*> | **-G** <*ip_csoport*>

psconf update [-p] {**-i**<*host*>| **-G** <*ipcsoport*>[**-r** <*buildinfo*> | **-a** <*apar1, apar2...*> | [**-u**] **-v** <*ifix1, ifix2,...*> | **-O** <*openpkggrp1, openkggrp2,...*>}

psconf log loglevel=<info | error | none>

psconf import -C -i <*hoszt*> **-f** <*fájlnév*> | **–d** <*import_adatbázis_fájlnév*>

psconf { **import -k** <*kulcsfájl_neve*> | **export**} **-S -f** <*fájlnév*>

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

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

psconf export -d <export_könyvtár_útvonala>

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

psconf report -A <tanácsadó_neve>

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

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

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

psconf clientData {-l | -g} -i <*ip*|*hoszt*>

psconf add -O <*nyíltcsomagcsoport*> <*nyíltcsomagnév*>

psconf delete -O <*nyíltcsomagcsoport*> <*nyíltcsomagnév:változat*>

psconf delete -O <*nyíltcsomagcsoport*>

psconf delete -O ALL

psconf add -O <*nyíltcsomagcsoport*> fspolicy=<*fsirányelv neve*>

psconf report -O ALL -o TEXT

psconf add -V <*ifixcsoport*> autoupdate=<yes|no>

psconf reboot -i <*hoszt*> last one

TNC kliens műveletek:

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

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

psconf { **rmclient | status** }

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

psconf chclient attribute = *érték*

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

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

psconf import { **-S | -C -k** <*kulcsfájl_neve*> } **-f** <*fájlnév*>

TNC IPRef műveletek:

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

psconf { **rmipref | status**}

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

psconf chipref attribute = *érték*

psconf { **import -k** <*kulcsfájl_neve*> **| export** } **-R -f** <*fájlnév*>

psconf list -R

Leírás

A TNC technológia egy nyílt szabványon alapuló architektúra a végpontok hitelesítéséhez, a platform integritás méréséhez, valamint biztonsági rendszerek integrálásához. A TNC architektúra megvizsgálja a végpontokat (hálózati kliensek és szerverek) a biztonsági irányelveknek való megfelelés tekintetében, mielőtt beengedné azokat a védett hálózatba. A TNC IPRef értesíti a TNC szervert bármilyen új IP címről, amelyet a virtuális I/O szerveren (VIOS) észlel.

A SUMA mentesíti a rendszergazdákat attól, hogy kézzel kelljen letölteniük a webről a karbantartási frissítéseket. Rugalmas beállításokat biztosít, amelyekkel a rendszeradminsztrátor beállíthat egy automatizált felületet a javítások letöltéséhez egy javításterjesztő webhelyről a helyi rendszerekre.

A hálózati szervert és klienseket a **psconf** paranccsal kezelheti: biztonsági irányelveket vehet fel és törölhet, klienseket érvényesíthet megbízhatóként vagy megbízhatatlanként, jelentéseket állíthat elő és frissítheti a szervert és a klienst.

A **psconf** parancs segítségével a következő műveletek hajthatók végre:

Elem	Leírás
add	Hozzáad egy irányelvet, egy klienst vagy az e-mail információkat a TNC szerveren.
apargrp	Megadja a TNC kliensek ellenőrzéséhez használt APAR csoportneveket a fájlkészlet irányelv részeként.
aparlist	Megadja az APAR csoport részét képező APAR jelentések listáját.
certadd	Megbízhatóként vagy megbízhatatlanként jelöli meg a tanúsítványt.
certdel	Törli a kliensinformációkat.
chclient	Módosítja a tnccs.conf fájlban lévő attribútumokat. Ahhoz, hogy a módosítások érvénybe lépjenek a TNC kliensben, egy kifejezett **start** utasítás kiadása szükséges. Az attribútum=érték szintaxis ugyanaz lesz, mint az **mkclient** esetén.
chipref	Módosítja a tnccs.conf fájlban lévő attribútumokat. Ahhoz, hogy a módosítások érvénybe lépjenek az IPRef összetevőben, egy kifejezett **start** utasítás kiadása szükséges. Az attribútum=érték szintaxisa ugyanaz, mint az **mkipref** esetén.
chserver	Módosítja a tnccs.conf fájlban lévő attribútumokat. Ahhoz, hogy a módosítások érvénybe lépjenek a TNC szerveren, egy kifejezett **start** utasítás kiadása szükséges. Az attribútum=érték szintaxisa ugyanaz, mint az **mkserver** esetén. **Megjegyzés:** A **dbpath** attribútum nem módosítható a **chserver** parancs használatával. Ez csak az **mkserver** parancs futtatásakor állítható be.
clientData	Létrehozza az információk pillanatképét (telepített operációs rendszer szint és fájlkészletek) a TNC kliensről. A *clientDataPath* útvonal azonosítja a pillanatkép gyűjtemény információinak tárolási helyét. Az alapértelmezett hely a TNC szerveren a /var/tnc/clientData/ könyvtár. A *clientDataPath* útvonal a **chserver** vagy az **mkserver** alparanccsal módosítható vagy állítható be. A TNC kliens pillanatkép adatgyűjtése kezdeményezhető a parancssorból a **clientData** alparancs futtatásával a TNC szerverről. A parancssorból futtatott **clientData** alparancs független a **clientData_interval** időköztől.
clientData_interval	A **chserver** és az **mkserver** alparanccsal állíthatja be a pillanatkép adatgyűjtést rendszeres időközönként egy érték megadásával a **clientData_interval** időközhöz. A pillanatkép adatgyűjtés automatikusan elindul, ha a **clientData_interval** időköz értéke nem 0 (nulla). Alapértelmezésben a pillanatkép adatgyűjtést az ütemező tiltja le. Az ütemező engedélyezéséhez adjon meg egy olyan **clientData_interval** értéket, amely nagyobb vagy egyenlő, mint 30. Az ütemező letiltásához adjon meg a 0 (nulla) **clientData_interval** értéket. A **clientData_interval** időköz támogatott tartománya 30 - 525600 perc.
dbpath	Megadja a TNC adatbázis helyét. Az alapértelmezett érték /var/tnc.
default_policy	Engedélyezi vagy letiltja a TNC ügyfelek automatikus ellenőrzését a köztes javításokhoz (ifix) és APAR-okhoz a klienssel megegyező szinten. Az automatikus ellenőrzés engedélyezéséhez a *yes* értéket adja meg. Az automatikus ellenőrzés letiltásához a *no* értéket adja meg. További információkért a **default_policy** alparanccsal kapcsolatban, tekintse meg a default_policy table részt.
delete	Töröl egy irányelvet vagy a kliensinformációkat.
export	Exportálja a TNC szerveren lévő kliens- vagy szervertanúsítványt, vagy adatbázist.
fspolicy	Megadja a TNC kliensek ellenőrzéséhez használt kiadás, technológia szint és javítócsomag fájlkészlet irányelvét.

Elem	Leírás
import	Importál egy tanúsítványt a kliensen vagy a szerveren, vagy egy adatbázist a TNC szerveren.
ipgroup	Megadja az Internet protokoll (IP) csoportot, amely több kliens IP címet vagy hosztnevet tartalmaz.
list	Megjeleníti a TNC szerver, a TNC kliens vagy a SUMA információit.
log	Beállítja a TNC összetevők naplózási szintjét.
mkclient	Konfigurálja a TNC klienst.
mkipref	Konfigurálja a TNC IPRef összetevőt.
mkserver	Konfigurálja a TNC szervert.
Openpkggrp	Megadja az nyílt forrású csomag csoport nevét a fájlkészlet irányelv részeként, amely az ügyfelek ellenőrzésére szolgál.
pmport	Megadja a portszámot, amelyen a **pmserver** figyel. Az alapértelmezett érték 38240.
pmserver	Megadja a **suma** parancs hosztnevét vagy IP címét, amely az IBM® ECC webhelyen és az IBM Fix Central webhelyen elérhető legfrissebb javítócsomagokat és biztonsági javításokat tölti le.
reboot	Újra betölti a TNC ügyfelet, amelyet az IP cím és a <*hoszt*> változó azonosít.
recheck_interval	Megadja az időközt percekben vagy d (nap) : h (óra) : m (perc) formátumban a TNC szerver számára a TNC kliensek ellenőrzéséhez. A **recheck_interval** időköz támogatott tartománya 30 - 525600 perc. **Megjegyzés:** A **recheck_interval=0** érték azt jelenti, hogy az ütemező nem kezdeményei rendszeres időközönként a kliensek ellenőrzését, és a regisztrált kliensek automatikusan lesznek érvényesítve indításkor. Ilyen esetekben a kliens kézzel érvényesíthető.
report	Előállít egy .txt vagy .csv fájlkiterjesztéssel rendelkező jelentést.
restart	Újraindítja a TNC klienst, a TNC szervert vagy a TNC TNC IPRef összetevőt.
rmclient	Megszünteti a TNC kliens konfigurációját.
rmipref	Megszünteti a TNC IPRef összetevő konfigurációját.
rmserver	Megszünteti a TNC szerver konfigurációját.
start	Elindítja a TNC klienst, a TNC szervert vagy a TNC TNC IPRef összetevőt.
status	Megjeleníti a TNC konfiguráció állapotát.
stop	Leállítja a TNC klienst, a TNC szervert vagy a TNC TNC IPRef összetevőt.
tncport	Megadja a portszámot, amelyen a TNC szerver figyel. Az alapértelmezett érték 42830.
tncserver	Megadja a TNC szervert, amely a TNC klienseket ellenőrzi vagy frissíti.
tssserver	Megadja a Trusted Surveyor szerver IP címét vagy hosztnevét.
update	Javításokat telepít a kliensen.
verify	A kliens kézi ellenőrzését kezdeményezi.

Az alábbi táblázat a

16. táblázat: default_policy alparancs eredményei

FSpolicy (fájlkészlet irányelv)	**default policy=***yes*	**default policy=***no*
A TNC kliens fájlkészlet irányelvhez tartozik köztes javítással (iFix) és APAR csoportokkal meghatározva	Az alapértelmezett irányelv felülbírálatra kerül a fájlkészlet irányelvben megadott iFix és APAR elemekkel.	Az alapértelmezett irányelv nem kerül felhasználásra. A fájlkészlet irányelvben megadott iFix-et és APAR-t a rendszer figyelembe veszi a TNC kliens ellenőrzési folyamata során.
A TNC kliens fájlkészlet irányelvhez tartozik megadott iFix és APAR csoport nélkül	Az alapértelmezett irányelv az iFix-el és az APAR-al kerül felhasználásra a TNC kliens ellenőrzési folyamata során. Csak a TNC kliens szintjével megegyező iFix és APAR kerül felhasználásra az ellenőrzési folyamat során.	Az alapértelmezett irányelv nem kerül felhasználásra.

Kapcsolók

Elem	Leírás
-A <tanácsadó_neve>	Megadja a jelentéshez tartozó tanácsadó nevét.
-B <összeépítési_info>	Megadja az összeépítési információkat egy javítási jelentés előkészítéséhez.

-c	Megjeleníti a felhasználói attribútumokat pontosvesszővel elválasztott rekordokban, az alábbiak szerint:
	`# name: attribútum1: attribútum2: ...`
	`policy: érték1: érték2: ...`

-C	Megadja, hogy a művelet egy klienshez összetevőhöz tartozik.
-d *adatbázis_fájl_helye/ adatbázis_könyvtárútvonala*	Megadja a az adatbázis importálásának fájlútvonalát/megadja az adatbázis exportálásának könyvtárútvonalát.
-D *éééé-hh-nn*	Megadja egy adott kliens bejegyzés dátumát a napló előzményekben; *éééé* az év, *hh* a hónap, *nn* pedig a nap.
-e *email_azonosító* **ipgroup=[±]***g1, g2...*	Megadja az e-mail azonosítót, amelyet egy vesszővel elválasztott IP csoportnévlista követ.
-E | FAIL | COMPLIANT | ALL |	Megadja az eseményt, amelyek esetén az e-maileket el kell küldeni a konfigurált e-mail azonosítóra. FAIL- Akkor küld leveleket, ha a kliens ellenőrzési állapota FAILED (meghiúsult). COMPLIANT- Akkor küld leveleket, ha a kliens ellenőrzési állapota COMPLIANT (megfelelő). ALL - A kliens ellenőrzésének minden állapotáról küld levelet.
-f *fájlnév*	Importálási művelet esetén megadja a fájlt, amelyből a tanúsítványt be kell olvasni, vagy exportálási művelet esetén megadja a helyet, ahová a tanúsítványt írni kell.
-F *fsirányelv_összeépítési_info*	Megadja a fájlrendszer irányelv nevét, amit az összeépítési információk követnek. Az összeépítési információk a következő formátumban adhatók meg: 6100-04-01, ahol 6100 a 6.1-es változatot ábrázolja, a 04 a karbantartási szintet, 01 pedig a javítócsomagot.
-g	A **clientData** alparancs futtatása a megadott TNC kliensen. Ez a kapcsoló csak a **clientData** alparanccsal érhető el.
-G*ip_csoport_neve* **ip=[±]***ip1, ip2...*	Megadja az IP csoport nevét, utána pedig egy vesszővel elválasztott IP listát.
-H	Felsorolja a történetnaplót.
-i *hoszt*	Megadja az IP címet vagy hosztnevet.
-I ip=[±]*ip1, ip2...* | [±] hoszt1,hoszt2...	Megadja az ellenőrzés során mellőzendő IP címeket/hosztneveket.
-k *fájlnév*	Megadja a fájlt, amelyből a tanúsítványkulcsot egy importálási művelet során be kell olvasni.
-l	Felsorolja a pillanatkép részleteket a TNC szerveren a megadott TNC klienshez. Ez a kapcsoló csak a **clientData** alparanccsal érhető el.
-O <openpkggrp>	Megadja az irányelv openpkg csoportnevét.
-p	Megjeleníti a TNC kliens frissítésének előképét.
-P <irányelvnév>	Megadja az irányelv nevét egy kliens irányelv jelentés előkészítéséhez.
-q	Kikapcsolja a fejlécinformációkat.
-r *összeépítési_információk*	Előállítja a jelentést az összeépítési információk alapján. Az összeépítési információk a következő formátumban adhatók meg: 6100-04-01, ahol 6100 a 6.1-es változatot ábrázolja, a 04 a karbantartási szintet, 01 pedig a javítócsomagot.
-R	Megadja, hogy a művelet egy IPRef összetevőhöz tartozik.
-s COMPLIANT | IGNORE | FAILED | ALL	A kliens állapotát jeleníti meg az alábbiak szerint: **COMPLIANT** Az aktív klienseket jeleníti meg. **IGNORE** A mindenfajta ellenőrzésből kizárt klienseket jeleníti meg. **FAILED** Azokat a klienseket jeleníti meg, melyek ellenőrzése a konfigurált irányelvet illetően meghiúsult. **ALL** Az összes klienst jeleníti meg, tekintet nélkül azok állapotára.
-S <hoszt>	Megadja a hosztnevet egy kliens biztonsági javítás jelentés előkészítéshez.
-t TRUSTED | UNTRUSTED	Megbízhatóként vagy megbízhatatlanként jelöli meg a megadott klienst. **Megjegyzés:** Csak rendszeradminisztrátorok igazolhatják a szervert vagy klienst megbízhatóként vagy megbízhatatlanként.
-T	Megadja, hogy a kliens elfogadhat-e kéréseket bármely, érvényes tanúsítvánnyal rendelkező TS szerverről.
-u	Eltávolítja a TNC kliensen telepített köztes javítást.

Elem	Leírás
-v<*CVEid|ALL*>	Megjeleníti az általános veszélyeztetettségeket és sebezhetőségeket a regisztrált javítócsomagokhoz. **CVEid** **All** Megjeleníti az összes általános veszélyeztetettséget és sebezhetőséget a regisztrált javítócsomagokhoz.
-v<*ifix1, ifix2,...*>	Megadja a köztes javítások vesszővel elválasztott listáját.
-V<*ifixgrp*>	Megadja a köztes javítás csoport nevét.
-V <*ifixgrp*> autoupdate=<yes|no>	Megadja, hogy az ifix-ek a megadott ifix csoportnév alatt automatikusan frissítésre kerülnek-e. **Igen** Automatikusan frissíti az fspolicy-hez megadott irányelvet, ha új ifix-ek érkeznek a TNC szerveren. **Nem** Megadja, hogy az új ifix-ek kézzel kerülnek hozzárendelése az irányelvhez, amint a TNC szerver fogadja őket. A nem az alapértelmezett érték.

Kilépési állapot

Ez a parancs a következő kilépési értékeket adja vissza:

Elem	Leírás
0	A parancs sikeresen lefutott, és minden kért módosítás megtörtént.
>0	Hiba történt. A kiírt hibaüzenet további részleteket biztosít a hiba típusáról.

Példák

1. A TNC szerver elindításához írja be a következő parancsot:
   ```
   psconf start server
   ```
2. Egy 71D_latest nevű fájlrendszer irányelv hozzáadásához a 7100-04-02 összeépítéshez, írja be a következő parancsot:
   ```
   psconf add -F 71D_latest 7100-04-02
   ```
3. Egy 71D_old nevű fájlrendszer irányelv törléséhez írja be a következő parancsot:
   ```
   psconf delete -F 71D_old
   ```
4. Annak ellenőrzéséhez, hogy a 11.11.11.11 IP címmel rendelkező kliens **megbízható**-e írja be a következő parancsot:
   ```
   psconf certadd -i 11.11.11.11 -t TRUSTED
   ```
5. A 11.11.11.11 IP címmel rendelkező kliens törléséhez a szerverről, írja be a következő parancsot:
   ```
   psconf certdel -i 11.11.11.11
   ```
6. A 11.11.11.11 IP címmel rendelkező kliens információinak ellenőrzéséhez írja be a következő parancsot:
   ```
   psconf verify -i 11.11.11.11
   ```
7. A 11.11.11.11 IP címmel rendelkező kliens információinak megjelenítéséhez írja be a következő parancsot:
   ```
   psconf list -i 11.11.11.11
   ```
8. A **COMPLIANT** (megfelel) állapotban lévő kliensekre vonatkozó jelentés előállításához írja be a következő parancsot:
   ```
   psconf list -s CPMPLIANT -i ALL
   ```
9. A 7100-04-02 összeépítésre vonatkozó jelentés előállításához írja be a következő parancsot:
   ```
   psconf list -r 7100-04-02
   ```
10. A 11.11.11.11 IP címmel rendelkező kliens csatlakozási előzményeinek megjelenítéséhez írja be a következő parancsot:
    ```
    psconf list -H -i 11.11.11.11
    ```
11. A 11.11.11.11 IP címmel rendelkező kliens bejegyzésének törléséhez a 2009. február 1-i vagy ennél régebbi naplóelőzményekből, írja be a következő parancsot:
    ```
    psconf delete -H -i 11.11.11.11 -D 2009-02-01
    ```
12. A 11.11.11.11 IP címmel rendelkező kliens klienstanúsítványának importálásához a szerverről, írja be a következő parancsot:

```
psconf import -C -i 11.11.11.11 -f /tmp/client.txt
```

13. A szervertanúsítvány exportálásához egy kliensből, adja ki a következő parancsot:
    ```
    psconf export -S -f /tmp/server.txt
    ```
14. A 11.11.11.11 IP címmel rendelkező kliens frissítéséhez egy megfelelő szintre a szerverről, írja be a következő parancsot:
    ```
    psconf update -i 11.11.11.11
    ```
15. A kliensállapotok megjelenítéséhez írja be a következő parancsot:
    ```
    psconf status
    ```
16. A klienstanúsítványok megjelenítéséhez írja be a következő parancsot:
    ```
    psconf list -C
    ```
17. A kliens indításához írja be a következő parancsot:
    ```
    psconf start client
    ```
18. A **clientData** alparanccsal összegyűjtött pillanatkép információk megjelenítéséhez adja ki a következő parancsot:
    ```
    psconf clientData -l [ip|host]
    ```
19. A TNC kliens történetének megjelenítéséhez adja ki a következő parancsot:
    ```
    psconf list –H –i [ip|ALL]
    ```

Biztonság

RBAC felhasználók és Megbízható AIX felhasználók figyelmébe:

A parancs privilegizált műveleteket is végrehajthat. A privilegizált műveleteket csak a megfelelő jogosultságokkal rendelkező felhasználók futtathatják. A jogosultságokról és privilégiumokról további információkat a Biztonság című rész Privilegizált parancsok adatbázisa szakaszában talál. A parancsra vonatkozó privilégiumok és jogosultságok listáját az **lssecattr** parancsnál vagy a **getcmdattr** alparancsnál találja

---

pscuiserverctl parancs

Rendeltetés

A PowerSC GUI szerver beállításainak megadására szolgál.

Szintaxis

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]

Kapcsolók

-r Újraindítja a PowerSC GUI szervert egy paraméterérték alkalmazása után.

set
Megadja vagy lekéri a PowerSC GUI szerver beállítását.

Paraméterek

httpPort *httpPortno*
A PowerSC GUI által használt alapértelmezett port megjelenítése vagy megadása.

httpsPort *httpsPortno*
A PowerSC GUI által használt alapértelmezett biztonságos port megjelenítése vagy megadása.

administratorGroupList *unixgrp1,unixgrp2,...*
UNIX csoportok megjelenítése vagy meghatározása, amelyek számára engedélyezett az adminisztrátori funkciók végrehajtása a PowerSC GUI használatával.

logonGroupList *unixgrp1,unixgrp2,...*
UNIX csoportok megjelenítése vagy meghatározása, amelyek számra engedélyezett a bejelentkezés a PowerSC GUIre.

powervcKeystoneUrl *powervcKeystoneurl*
A PowerVC kulcstároló szerver URL címének megjelenítése vagy megadása.

QRadarSyslogResponseEnabled on | off
Syslog naplózás aktuális beállításának megjelenítése a PowerSC GUIről vagy a Syslog naplózás be- és kikapcsolása.

tncServer *tncserver.abc.com*
TNC szerver hosztnevének megjelenítése vagy megadása. Ha módosítja a TNC szerver hosztnevét, akkor újra kell indítani a PowerSC GUI szervert.

Kilépési állapot

Ez a parancs a következő kilépési értékeket adja vissza:

0 Sikeres befejeződés.

>0 Hiba történt.

Példák

1. Annak megtekintése, hogy jelenleg mi van megadva a PowerSC GUI által használt alapértelmezett portként:
   ```
   pscuiserverctl set httpPort
   ```
2. A PowerSC GUI által használt alapértelmezett port beállítása:
   ```
   pscuiserverctl set httpPort 80
   ```
3. Annak megtekintése, hogy jelenleg mi van megadva a PowerSC GUI által használt alapértelmezett biztonsági portként:
   ```
   pscuiserverctl set httpsPort
   ```
4. A PowerSC GUI által használt alapértelmezett biztonsági port beállítása:
   ```
   pscuiserverctl set httpsPort 483
   ```
5. Annak megtekintése, hogy mely UNIX csoportok számára engedélyezett az adminisztrátori funkciók végrehajtása a PowerSC GUI használatával:
   ```
   pscuiserverctl set administratorGroupList
   ```
6. UNIX csoportok beállítása, amelyek számára engedélyezett az adminisztrátori funkciók végrehajtása a PowerSC GUI használatával:
   ```
   pscuiserverctl set administratorGroupList securitygroup1,admingrp1
   ```
7. Annak megtekintése, hogy mely UNIX csoportok számára engedélyezett a bejelentkezés a PowerSC GUIre:
   ```
   pscuiserverctl set logonGroupList
   ```
8. UNIX csoportok beállítása, amelyek számra engedélyezett a bejelentkezés a PowerSC GUIre:

```
pscuiserverctl set logonGroupList unixgroup1,unixgrp2
```

9. A PowerVC kulcstároló szerver URL címének megtekintése:

```
pscuiserverctl set powervcKeystoneUrl
```

10. A PowerVC kulcstároló szerver URL címének beállítása:

```
pscuiserverctl set powervcKeystoneUrl https://powervc/server/example/
```

11. Annak megtekintése, hogy a Syslog naplózás a PowerSC GUIen be- vagy ki van kapcsolva:

```
pscuiserverctl set QRadarSyslogResponseEnabled
```

12. Syslog naplózás beállítása a PowerSC GUIen be- vagy kikapcsolt állapotra:

```
pscuiserverctl set QRadarSyslogResponseEnabled on
pscuiserverctl set QRadarSyslogResponseEnabled off
```

13. TNC szerver hosztnevének megtekintése:

```
pscuiserverctl set tncServer
```

14. TNC szerver hosztnevének beállítása:

```
pscuiserverctl set tncServer tncserver.abc.com
```

15. A TNC szerver nevének beállításához újra kell indítani a PowerSC GUI szervert. A PowerSC GUI szerver újraindítása:

```
pscuiserverctl -r set tncServer tncs1.rs.com
```

---

pscxpert parancs

Cél

A rendszeradminisztrátor számára segítséget nyújt a biztonsági konfiguráció beállításában.

Szintaxis

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

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

pscxpert -f Profile [**-p**] [**-r**|**-R**]

pscxpert -u [**-p**]

pscxpert -c [**-p**] [**-r**|**-R**] [**-P** Profile] [**-l** Level]

pscxpert -t

pscxpert -l <Level> [**-p**] <**-a** *1. fájl* | **-n** *2. fájl* | **-a** *3. fájl* **-n** *4. fájl*>

pscxpert -f Profile **-a** File [**-p**]

pscxpert -d

Leírás

A **pscxpert** parancs különböző rendszerkonfigurációs beállításokat ad meg a megadott biztonsági szint biztosításához.

A **pscxpert** parancs futtatása az **-l** paraméterkészlet használatával rákérdezés nélkül valósítja meg a biztonsági beállításokat, anélkül, hogy a felhasználó számára lehetővé tenné a beállítások konfigurálását. Például a **pscxpert -l high** parancs futtatása automatikusan alkalmazza az összes magas szintű biztonsági beállítást. Azonban a **pscxpert -l** parancs futtatása az **-n** és az **-a** paraméterrel, a biztonsági beállításokat a *fájl* paraméter által megadott fájlba menti. Az **-f** paraméter ezután alkalmazza az új beállításokat.

A kezdeti beállítások után megjelenik egy menü az összes biztonsági konfigurációs beállítással, amely a kiválasztott biztonsági szinthez tartozik. Ezek a beállítások elfogadhatók egyben vagy egyenként ki-be lehet kapcsolni őket. A másodlagos módosítások után a **pscxpert** parancs folytatja a biztonsági beállítások alkalmazását a számítógéprendszeren.

A **pscxpert** parancsot a Virtuális I/O szerver root felhasználójaként futtassa. Ha nem a Virtual I/O Server root felhasználójaként van bejelentkezve, akkor a parancs futtatása előtt futtassa az **oem_setup_env** parancsot.

Ha akkor futtatja a **pscxpert** parancsot, amikor a **pscxpert** parancs egy másik példánya fut, akkor a **pscxpert** parancs egy hibaüzenettel kilép.

Megjegyzés: Futtassa újra a **pscxpert** parancsot minden olyan jelentős rendszermódosítás után, mint például a szoftvertelepítés vagy a szoftverfrissítés. Ha nincs kiválasztva egy adott biztonsági konfigurációs elem, amikor a **pscxpert** parancs újrafut, akkor az adott konfigurációs elem átlépésre kerül.

Paraméterek

Elem	Leírás
-a	A beállítások és a társított biztonsági szint beállításai a megadott fájlba kerülnek beírásra rövidített formátumban.
-c	A biztonsági beállítások ellenőrzése a korábban alkalmazott szabálykészlet szerint. Ha egy szabályra az ellenőrzés meghiúsul, akkor a szabály korábbi változatait szintén megvizsgálja a rendszer. Ez a folyamat addig folytatódik, amíg az ellenőrzés sikeres nem lesz, vagy amíg a meghiúsult szabály összes példánya az /etc/security/aixpert/core/appliedaixpert.xml fájlban ellenőrzésre nem kerül. Ez az ellenőrzés bármely alapértelmezett profilhoz vagy egyéni profilhoz futtatható.
-d	A dokumentumtípus meghatározásának megjelenítése (DTD).

Elem	Leírás
-f	A megadott *profil* fájlban meghatározott biztonsági beállítások alkalmazása. A profilok az /etc/security/aixpert/custom könyvtárban találhatók. A rendelkezésre álló profilok az alábbi szabványos profilokat tartalmazzák: **DataBase.xml** Ez a fájl tartalmazza az alapértelmezett adatbázis-beállítások követelményeit. **DoD.xml** Ez a fájl tartalmazza a Department of Defense Security Technical Implementation Guide (STIG) beállítások követelményeit. **DoD_to_AIXDefault.xml** Ez módosítja a beállításokat az alapértelmezett AIX beállításokhoz. **DoDv2.xml** Ez a fájl tartalmazza a Department of Defense Security Technical Implementation Guide (STIG) 2. változatához tartozó beállítások követelményeit. **DoDv2_to_AIXDefault.xml** Ez módosítja a beállításokat az alapértelmezett AIX beállításokhoz. **Hipaa.xml** Ez a fájl tartalmazza a Health Insurance Portability and Accountability Act (HIPAA) beállítások követelményeit. **NERC.xml** Ez a fájl tartalmazza a North American Electric Reliability Corporation (NERC) beállítások követelményeit. **NERC_to_AIXDefault.xml** Ez a fájl módosítja a NERC beállításokat az alapértelmezett AIX beállításokhoz. **PCI.xml** Ez a fájl tartalmazza a Payment card industry Data Security Standard beállítások követelményeit. **PCIv3.xml** Ez a fájl tartalmazza a Payment card industry Data Security Standard Version 3 beállítások követelményeit. **PCI_to_AIXDefault.xml** Ez a fájl módosítja a beállításokat az alapértelmezett AIX beállításokhoz. **PCIv3_to_AIXDefault.xml** Ez a fájl módosítja a beállításokat az alapértelmezett AIX beállításokhoz. **SOX-COBIT.xml** Ez a fájl tartalmazza a Sarbanes-Oxley Act and COBIT beállítások követelményeit. Ugyanebben a könyvtárban egyéni profilokat is létrehozhat, és alkalmazhatja azokat a beállításaira a meglévő XML fájlok átnevezésével és módosításával. Például a következő parancs a rendszerre a HIPAA profilt alkalmazza: `pscxpert -f /etc/security/aixpert/custom/Hipaa.xml` A **-f** paraméter megadásakor a biztonsági beállítások konzisztensen alkalmazásra kerülnek rendszerről rendszerre az **appliedaixpert.xml** fájl biztonságos átvitelével és alkalmazásával rendszerről rendszerre. Minden sikeresen alkalmazott szabály az /etc/security/aixpert/core/appliedaixpert.xml fájlba kerül beírásra, a vonatkozó undo műveleti szabályok pedig az /etc/security/aixpert/core/undo.xml fájlba kerülnek beírásra.

Elem	Leírás
-l	A rendszer biztonsági beállításainak beállítása a megadott szinthez. A kapcsoló paraméterei az alábbiak: **h|high** Magas szintű biztonsági beállítások megadása. **m|medium** Közepes szintű biztonsági beállítások megadása. **l|low** Alacsony szintű biztonsági beállítások megadása. **d|default** AIX szabvány szintű biztonsági beállítások megadása. **s|sox-cobit** A Sarbanes-Oxley Act and COBIT biztonsági beállítások megadása. Ha az **-l** és az **-n** paraméter is meg van adva, akkor a biztonsági beállítások nem kerülnek megvalósításra a rendszeren; azonban csak a megadott fájlba kerülnek beírásra. Minden sikeresen alkalmazott szabály beírásra kerül az /etc/security/aixpert/core/appliedaixpert.xml fájlba, a vonatkozó visszavonási műveleti szabályok pedig az /etc/security/aixpert/core/undo.xml fájlba kerülnek beírásra. **FIGYELEM:** A **d|default** paraméter használatakor a paraméter felülírhatja a konfigurált biztonsági beállításokat, amelyeket korábban beállított a **pscxpert** paranccsal vagy függetlenül, és visszaállítja a rendszert a hagyományos nyílt konfigurációjára.
-n	A beállításokat a társított biztonsági szint beállításaival a megadott fájlba írja.
-p	Megadja, hogy a biztonsági szabályok kimenete részletes kimenet használatával jelenjen meg. A **-p** paraméter naplózza a szabályokat, amelyek fel lettek dolgozva a megfigyelési alrendszerhez, ha az **auditing** opció be van kapcsolva. Ez az opció bármelyik **-l**, **-u**, **-c** és **-f** paraméterrel használható. A **-p** paraméter lehetővé teszi a részletes kimenetet a terminál és az aixpert.log fájlba is.
-P	A profilnevet bemenetként fogadja el. Ez az opció a **-c** paraméterekkel együtt kerül felhasználásra. A **-c** és a **-P** paraméter szolgál a rendszer és az átadott profil kompatibilitásának ellenőrzésére.
-r	A rendszer meglévő beállításait az /etc/security/aixpert/check_report.txt fájlba írja. A kimenetet használhatja a biztonsági és a megfelelési felülvizsgálati jelentésekben. A jelentés leírja az egyes beállításokat, azt, hogy hogyan viszonyul adott szabályozás megfelelési követelményeihez, valamint hogy az ellenőrzés sikeres-e vagy meghiúsult. **Megjegyzés:** • Az -r paraméter csak az alkalmazás műveletet támogatja a profilokhoz. A szintekhez nem támogatja az alkalmazás műveletet. • Az -r paraméter megjeleníti a teljes üzenetet (legalább egy sorban) a szabályhoz.
-R	Ugyanazt a kimenetet állítja elő, mint az **-r** paraméter. Ezenkívül ez a paraméter annak a szabálynak a parancsfájl vagy program leírását is hozzáfűzi, amely a konfigurációs beállítás megvalósítására szolgált. **Megjegyzés:** • Az -R paraméter csak az alkalmazás műveletet támogatja a profilokhoz. A szintekhez nem támogatja az alkalmazás műveletet.
-t	Megjeleníti a rendszeren alkalmazott profil típusát.
-u	Visszavonja az alkalmazott biztonsági beállításokat. **Megjegyzés:** • Az **-u** paraméter nem használható a DoD, DoDv2, NERC, PCI és PCIv3 profilok alkalmazásainak megfordítására. Ha el kívánja távolítani ezeket a profilokat hozzáadás után, akkor alkalmazza az _AIXDefault.xml végű profilt. Például a NERC.xml profil eltávolításához a NERC_to_AIXDefault.xml profilt kell alkalmazni. • Változások a rendszeren, miután az alkalmazás művelet elveszik egy visszavonás művelettel. A beállítások arra az értékre térnek vissza, amelyen az alkalmazás művelet előtt voltak.

Paraméterek

Elem	Leírás
Fájl	A biztonsági beállításokat tároló kimeneti fájl. A fájl hozzáféréséhez root engedély szükséges.
Szint	Az egyéni szint az ellenőrzéshez a korábban alkalmazott beállítások alapján.
Profil	A rendszer megfelelési szabályait megadó profil fájlneve. A fájl hozzáféréséhez root engedély szükséges.

Biztonság

A **pscxpert** parancsot csak root felhasználó futtathatja.

Példák

1. Az összes magasszintű biztonsági beállítás kimeneti fájlba történő írásához adja ki a következő parancsot:

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

   A parancs futtatása után a kimeneti fájl módosítható és bizonyos biztonsági szerepek kikommentezhetők, ha szabványos XML megjegyzés karaktersorozat közé zárja őket (a megjegyzést <-- kezdi és -\> zárja le).
2. A biztonsági beállításoknak a Department of Defense STIG konfigurációs fájlból megvalósuló alkalmazásához adja ki a következő parancsot:

   ```
   pscxpert -f /etc/security/aixpert/custom/DoD.xml
   ```
3. A biztonsági beállításoknak a HIPAA konfigurációs fájlból megvalósuló alkalmazásához adja ki a következő parancsot:

   ```
   pscxpert -f /etc/security/aixpert/custom/Hipaa.xml
   ```
4. A rendszer biztonsági beállításainak ellenőrzéséhez, valamint azon szabályok naplózásához, amelyek meghiúsultak a felülvizsgálati alrendszerhez, adja ki a következő parancsot:

   ```
   pscxpert -c -p
   ```
5. A biztonsági beállítások egyéni szintjének ellenőrzéséhez a NERC profilhoz a rendszeren, valamint a felülvizsgálati alrendszerhez meghiúsult szabályok naplózásához, adja ki a következő parancsot:

   ```
   pscxpert -c -p -l NERC
   ```
6. Jelentések előállításához és a beírásukhoz az /etc/security/aixpert/check_report.txt fájlba. adja ki a következő parancsot:

   ```
   pscxpert -c -r
   ```

Hely

Elem	Leírás
/usr/sbin/pscxpert	A **pscxpert** parancsot tartalmazza.

Fájlok

Elem	Leírás
/etc/security/aixpert/log/aixpert.log	Az alkalmazott biztonsági beállítások nyomkövetési naplóját tartalmazza. Ez a fájl nem a syslog szabványt használja. A **pscxpert** parancs közvetlenül a fájlba ír, olvasás/írás engedélyei vannak és root biztonságot igényel.
/etc/security/aixpert/log/firstboot.log	Azoknak a biztonsági beállításoknak a nyomkövetési naplóját tartalmazza, amelyek az első, Alapértelmezésben védett (SbD) telepítés során kerültek alkalmazásra.
/etc/security/aixpert/core/undo.xml	A visszavonható biztonsági beállítások XML listáját tartalmazza.

rmvfilt parancs

Cél

Eltávolítja a virtuális LAN kereszteződési szűrőszabályokat a szűrőtáblázatból.

Szintaxis

rmvfilt -n [**fid|all>**]

Leírás

Az **rmvfilt** parancs arra szolgál, hogy eltávolítsa a virtuális LAN kereszteződési szűrőszabályokat a szűrő táblából.

Kapcsolók

-n Megadja az eltávolítandó szűrőszabály azonosítóját. Az **all** paraméter használatával az összes szűrőszabály eltávolítható.

Kilépési állapot

Ez a parancs a következő kilépési értékeket adja vissza:

0 Sikeres befejeződés.

>0 Hiba történt.

Példák

1. Az összes szűrőszabály eltávolításához, vagy a kernelben lévő összes szűrőszabály deaktiválásához írja be a parancsot a következők szerint:

   ```
   rmvfilt -n all
   ```

Kapcsolódó fogalmak:

“Szabályok deaktiválása” oldalszám: 105
A Megbízható tűzfal szolgáltatásban a VLAN hálózatok közötti továbbítást engedélyező szabályok deaktiválhatók.

---

vlantfw parancs

Cél

Megjeleníti vagy törli az IP és Adathordozó hozzáférés-felügyelet (MAC) leképezési információkat, és vezérli a naplózási funkciót.

Szintaxis

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

Leírás

A **vlantfw** parancs megjeleníti vagy törli az IP és MAC leképezési bejegyzéseket. Biztosítja továbbá a Megbízható tűzfal szolgáltatás elindításának vagy leállításának képességét.

Kapcsolók

-d Megjeleníti az összes IP leképezési információt.

-D Megjeleníti az összegyűjtött kapcsolatadatokat.

-E Megjeleníti a logikai partíciók (LPAR) közötti kapcsolatadatokat a különböző központi feldolgozó komplexumokhoz.

-f Eltávolítja az összes IP leképezési információt.

-F Kiüríti a kapcsolatadatok gyorsítótárát.

-G Megjeleníti a szűrőszabályokat, amelyek beállíthatók úgy, hogy a forgalom belsőleg, a Megbízható tűzfal szolgáltatás használatával legyen továbbítva.

-I Megjeleníti az azonos központi feldolgozó komplexumokhoz tartozó, de különböző VLAN azonosítókkal társított logikai partíciók közötti kapcsolatadatokat.

-l Elindítja a Megbízható tűzfal naplózási szolgáltatást.

-L Leállítja a Megbízható tűzfal naplózási szolgáltatást, és átirányítja a nyomkövetési fájlok tartalmát a /home/padmin/svm/svm.log fájlba.

-m Engedélyezi a Megbízható tűzfal megfigyelést.

-M Letiltja a Megbízható tűzfal megfigyelést.

-q Lekérdezi a biztonságos virtuális gép állapotot.

-s Elindítja a Megbízható tűzfal szolgáltatást.

-t Leállítja a Megbízható tűzfal szolgáltatást.

Paraméterek

-N *egész_szám*
Megjeleníti a megadott egész számnak megfelelő szűrőszabályt.

Kilépési állapot

Ez a parancs a következő kilépési értékeket adja vissza:

0 Sikeres befejeződés.

>0 Hiba történt.

Példák

1. Az összes IP leképezés megjelenítéséhez adja ki a parancsot a következők szerint:
   ```
   vlantfw -d
   ```
2. Az összes IP leképezés eltávolításához adja ki a parancsot a következők szerint:
   ```
   vlantfw -f
   ```
3. A Megbízható tűzfal naplózási funkció elindításához adja ki a parancsot a következők szerint:
   ```
   vlantfw -l
   ```
4. Egy biztonságos virtuális gép állapotának ellenőrzéséhez adja ki a parancsot a következők szerint:
   ```
   vlantfw -q
   ```
5. A Megbízható tűzfal elindításához adja ki a parancsot a következők szerint:
   ```
   vlantfw -s
   ```
6. A Megbízható tűzfal leállításához adja ki a parancsot a következők szerint:
   ```
   vlantfw -t
   ```
7. A forgalmat a központi feldolgozó komplexumon belül továbbító szűrők előállításához használható megfelelő szabályok megjelenítéséhez adja ki a parancsot a következők szerint:
   ```
   vlantfw -G
   ```

Kapcsolódó hivatkozás:
“genvfilt parancs” oldalszám: 148

Nyilatkozatok

Ezek az információk az Egyesült Államokban forgalmazott termékekre és szolgáltatásokra vonatkoznak.

Elképzelhető, hogy a dokumentumban tárgyalt termékeket, szolgáltatásokat vagy lehetőségeket az IBM más országokban nem forgalmazza. Az adott országokban rendelkezésre álló termékekről és szolgáltatásokról a helyi IBM képviseletek szolgálnak felvilágosítással. Az IBM termékekre, programokra vagy szolgáltatásokra vonatkozó hivatkozások sem állítani, sem sugallni nem kívánják, hogy az adott helyzetben csak az IBM termékeit, programjait vagy szolgáltatásait lehet alkalmazni. Minden olyan működésében azonos termék, program vagy szolgáltatás alkalmazható, amely nem sérti az IBM szellemi tulajdonjogát. A nem IBM termékek, programok és szolgáltatások működésének megítélése és ellenőrzése természetesen a felhasználó felelőssége.

A dokumentum tartalmával kapcsolatban az IBM bejegyzett vagy bejegyzés alatt álló szabadalmakkal rendelkezhet. Ezen dokumentum nem ad semmiféle licencet ezen szabadalmakhoz. A licenckérelmeket írásban a következő címre küldheti:

IBM Director of Licensing
IBM Corporation
North Castle Drive, MD-NC119
Armonk, NY 10504-1785
US

Ha duplabyte-os karakterkészlet- (DBCS) információkra vonatkozóan van szüksége licencre, akkor lépjen kapcsolatba országában az IBM szellemi tulajdon osztályával, vagy írjon a következő címre:

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

AZ IBM A KIADVÁNYT "JELENLEGI FORMÁJÁBAN", BÁRMIFÉLE KIFEJEZETT VAGY VÉLELMEZETT GARANCIA NÉLKÜL ADJA KÖZRE, IDEÉRTVE, DE NEM KIZÁRÓLAG A JOGSÉRTÉS KIZÁRÁSÁRA, A KERESKEDELMI ÉRTÉKESÍTHETŐSÉGRE ÉS BIZONYOS CÉLRA VALÓ ALKALMASSÁGRA VONATKOZÓ VÉLELMEZETT GARANCIÁT. Egyes joghatóságok nem engedik meg a közvetett vagy közvetlen garanciavállalás visszautasítását bizonyos tranzakciókra, így a fenti állítás nem feltétlenül vonatkozik Önre.

Jelen dokumentum tartalmazhat technikai, illetve szerkesztési hibákat. A jelen információk időről időre megváltoznak; ezeket a változtatásokat a kiadvány újabb kiadásai tartalmazzák. Az IBM mindennemű értesítés nélkül fejlesztheti és/vagy módosíthatja a kiadványban tárgyalt termékeket és/vagy programokat.

A kiadványban a nem az IBM által üzemeltetett webhelyek megjelenése csak kényelmi célokat szolgál, és semmilyen módon nem jelenti e webhelyek előnyben részesítését másokhoz képest. Az ilyen webhelyeken található anyagok nem képezik az adott IBM termék dokumentációjának részét, így ezek felhasználása csak saját felelősségre történhet.

Az IBM belátása szerint bármilyen formában felhasználhatja és továbbadhatja a felhasználóktól származó adatokat anélkül, hogy ebből a felhasználók felé bármilyen kötelezettsége származna.

A programlicenc azon birtokosai, akik (i) a függetlenül létrehozott programok vagy más programok (beleértve ezt a programot is) közti információcsere, illetve (ii) a kicserélt információk kölcsönös használata céljából szeretnének információkhoz jutni, a következő címre írjanak:

IBM Director of Licensing
IBM Corporation
North Castle Drive, MD-NC119
Armonk, NY 10504-1785
US

Az ilyen információk bizonyos feltételek és kikötések mellett állnak rendelkezésre, ideértve azokat az eseteket is, amikor ez díjfizetéssel jár.

Az IBM a dokumentumban tárgyalt licencprogramokat és a hozzájuk tartozó licenc anyagokat IBM Vásárlói megállapodás, IBM Nemzetközi programlicenc szerződés vagy a felek azonos tartalmú megállapodása alapján biztosítja.

A megadott teljesítményadatok és ügyfélpéldák csak illusztrációs célokat szolgálnak. A tényleges teljesítményhez kapcsolódó eredmények a specifikus konfigurációktól és üzemeltetési helyzetektől függően eltérhetnek.

A nem IBM termékekre vonatkozó információk a termékek szállítóitól, illetve azok publikált dokumentációiból, valamint egyéb nyilvánosan hozzáférhető forrásokból származnak. Az IBM nem tesztelte ezeket a termékeket, így az IBM a nem IBM termékek esetében nem tudja megerősíteni a teljesítményre és kompatibilitásra vonatkozó, valamint az egyéb állítások pontosságát. A nem IBM termékek képességeivel kapcsolatos kérdésekkel forduljon azok terjesztőihez.

Az IBM jövőbeli tevékenységére vagy szándékaira vonatkozó állításokat az IBM mindennemű értesítés nélkül módosíthatja, azok csak célkitűzéseket jelentenek.

A feltüntetett árak az IBM által javasolt aktuális kiskereskedelmi árak, és ezek értesítés nélkül változhatnak. Az egyes viszonteladók árai eltérhetnek ettől.

Ezek az információk csak tervezési célokra használhatók. Az információk a tárgyalt termékek elérhetővé válása előtt megváltozhatnak.

Az információk között példaként napi üzleti tevékenységekhez kapcsolódó jelentések és adatok lehetnek. A tökéletes szemléltetés céljából a példák egyének, vállalatok, márkák és termékek neveit tartalmazzák. Minden ilyen név a képzelet szüleménye, és az esetleges hasonlóságuk a valódi személyekhez és üzleti vállalkozásokhoz teljes egészében a véletlen műve.

COPYRIGHT LICENSE:

A kiadvány forrásnyelvi alkalmazásokat tartalmaz, amelyek a programozási technikák bemutatására szolgálnak a különböző működési környezetekben. A példaprogramokat tetszőleges formában, az IBM-nek való díjfizetés nélkül másolhatja, módosíthatja és terjesztheti a példaprogram operációs rendszeréhez tartozó alkalmazásprogram-illesztőnek megfelelő alkalmazásprogram fejlesztésének, használatának, eladásának vagy terjesztésének céljából. Ezek a példák nem kerültek minden körülmények között tesztelésre. Ezért az IBM nem garantálja ezen programok megbízhatóságát, javíthatóságát és működését. A példaprogramok "JELENLEGI FORMÁJUKBAN", bármiféle garancia vállalása nélkül kerülnek közreadásra. Az IBM semmilyen felelősséget nem vállal a mintaprogramok használatából adódó káreseményekért.

A példaprogramok minden másolatának, bármely részletének, illetve az ezek felhasználásával készült minden származtatott munkának tartalmaznia kell az alábbi szerzői jogi feljegyzést:

© (cégnév) (évszám).

A kód bizonyos részei az IBM Corp. példaprogramjaiból származnak.

© Copyright IBM Corp. (évszám vagy évszámok)

Adatvédelmi irányelv szempontok

Az IBM szoftvertermékek, a szolgáltatási megoldásként használt szoftvereket (“Szoftver termékajánlatok”) is beleértve, cookie-k és más technológiák használatával begyűjthetik a termék használatával kapcsolatos információkat, aminek célja a végfelhasználói élmény tökéletesítése, a végfelhasználókkal folytatott együttműködés személyre szabása, stb. A szoftvertermék-ajánlatok sok esetben nem gyűjtenek személyes azonosításra alkalmas információkat. Néhány szoftvertermék-ajánlat segíthet személyesen azonosítható információk begyűjtésének engedélyezésében. Ha jelen szoftvertermék-ajánlat személyes azonosításra alkalmas információk gyűjtésére használ cookie-kat, akkor a cookie-knak az adott ajánlatban való használatáról az alábbiakban tájékozódhat.

Ez a szoftvertermék-ajánlat nem használ cookie-t vagy más technológiát a személyes azonosításra alkalmas információk gyűjtéséhez.

Ha a szoftvertermék-ajánlat telepített konfigurációi Önnek, mint ügyfélnek biztosítják azt a képességet, hogy személyesen azonosítható információkat gyűjtsön be a végfelhasználóktól cookie-kon és egyéb technológiákon keresztül, akkor Önnek kell az ilyen adatgyűjtésre vonatkozó törvényi szabályozással kapcsolatos információkat beszereznie, beleértve a nyilatkozatokkal és hozzájárulásokkal kapcsolatos követelményeket is.

A különféle technológiák (a cookie-kat is beleértve) ilyen célra való felhasználásával kapcsolatos további információkat a következő helyeken talál: IBM online adatvédelmi tájékoztató - kivonat (http://www.ibm.com/privacy) és IBM online adatvédelmi tájékoztató (http://www.ibm.com/privacy/details), valamint a “Cookies, Web Beacons and Other Technologies” és az “IBM Software Products and Software-as-a-Service Privacy Statement” részek a http://www.ibm.com/software/info/product-privacy webhelyen.

Védjegyek

IBM, az IBM logó és az ibm.com az International Business Machines Corporationnek a világ számos országában regisztrált védjegye. Más termék- és szolgáltatásnevek az IBM vagy más vállalatok védjegyei lehetnek. Az IBM védjegyek aktuális listája a Copyright and trademark information weboldalon érhető el az alábbi címen: www.ibm.com/legal/copytrade.shtml.

Linux Linus Torvalds bejegyzett védjegye az Egyesült Államokban és/vagy más országokban.

Java és minden Java alapú védjegy és logó az Oracle és/vagy társvállalatai védjegye vagy bejegyzett védjegye.

Tárgymutató

A, Á

B

C

D

E, É

F

G

H

I, Í

J

K

L

M

N

Ö, Ő

P

R

S

SZ

T

V

Nyomtatva Dániában