IBM PowerSC

Standard Edition

Verzia 1.1.6

PowerSC Standard Edition

IBM PowerSC

Standard Edition

Verzia 1.1.6

PowerSC Standard Edition

Poznámka

Pred použitím týchto informácií a produktu, ktoré podporujú, si prečítajte informácie v časti “Vyhlásenia” na strane 173.

Toto vydanie sa vzťahuje na produkt IBM PowerSC Standard Edition Verzia 1.1.6 a všetky následné vydania a modifikácie, pokiaľ v nových vydaniach nebude uvedené inak.

Obsah

O tomto dokumente v

Novinky v aplikácii PowerSC Standard Edition 1

Súbory PDF k produktu PowerSC Standard Edition 3

PowerSC Standard Edition - základné pojmy 5

Inštalácia PowerSC Standard Edition . . 7

Funkcia Security and Compliance Automation 9

Koncepty automatizácie bezpečnosti a súladu s nariadeniami 9
- Súlad s pokynmi STIG Ministerstva obrany USA . . 10
- Súlad s požiadavkami štandardu PCI - DSS (Payment Card Industry - Data Security Standard) 68
- Súlad s požiadavkami normy Sarbanes-Oxley Act a COBIT (SOX-COBIT) 81
- Health Insurance Portability and Accountability Act (HIPAA) 82
- Súlad s požiadavkami organizácie NERC (North American Electric Reliability Corporation) 87

Správa funkcie Security and Compliance Automation . . 89
- Vyhľadanie neúspešného pravidla 90
- Aktualizácia neúspešného pravidla 90
- Vytvorenie vlastného profilu konfigurácie zabezpečenia 90
- Testovanie aplikácií pomocou AIX Profile Manager . . 91
- Monitorovanie systémov pre trvalý súlad s požiadavkami pomocou programu AIX Profile Manager. 91

Konfigurácia funkcie Security and Compliance Automation softvéru PowerSC 91
- Konfigurácia nastavení volieb súladu s požiadavkami systému PowerSC 91
- Konfigurácia súladu s požiadavkami systému PowerSC z príkazového riadka 92
- Konfigurácia súladu s požiadavkami systému PowerSC pomocou programu AIX Profile Manager 93

PowerSC Real Time Compliance 95

Inštalácia PowerSC Real Time Compliance 95
Konfigurácia PowerSC Real Time Compliance 95
- Identifikácia súborov monitorovaných funkciou PowerSC Real Time Compliance 95
- Nastavenie výstrah pre PowerSC Real Time Compliance. 96

Funkcia Trusted Boot 97

Základné pojmy pre Trusted Boot 97
Plánovanie dôveryhodného spustenia 97
- Nevyhnutné podmienky pre Trusted Boot 97
- Príprava na nápravu 98
- Aspekty migrácie 98

Inštalácia funkcie Trusted Boot 99
- Inštalácia kolektora 99
- Inštalácia overovateľa. 99

Konfigurácia funkcie Trusted Boot 99
- Registrácia systému 99
- Atestácia systému 100

Správa funkcie Trusted Boot 100
- Interpretovanie výsledkov atestácie 100
- Odstraňovanie systémov 101

Riešenie problémov s funkciou Trusted Boot 101

Trusted Firewall 103

Základné pojmy pre Trusted Firewall 103
Inštalácia funkcie Trusted Firewall 105
Konfigurácia funkcie Trusted Firewall 106
- Trusted Firewall Advisor 106
- Protokolovanie funkcie Trusted Firewall 106
- Viaceré zdieľané ethernetové adaptéry 107
- Odstránenie zdieľaných ethernetových adaptérov . . 108
- Vytváranie pravidiel 108
- Deaktivovanie pravidiel. 109

Trusted Logging 111

Virtuálne protokoly 111
Zisťovanie virtuálnych protokolových zariadení . . . 111
Inštalácia funkcie Trusted Logging 112
Konfigurácia funkcie Trusted Logging 112
- Konfigurácia podsystému AIX Audit 112
- Konfigurácia súboru syslog. 113
- Zapisovanie údajov do virtuálnych protokolových zariadení 113

Trusted Network Connect (TNC) . . . 115

Základné pojmy pre Trusted Network Connect 115
- Komponenty rámca Trusted Network Connect . . . 115
- Bezpečná komunikácia IP Trusted Network Connect 116
- Protokol Trusted Network Connect 117
- Moduly IMC a IMV 117

Požiadavky TNC 117
Konfigurácia komponentov TNC 118
Konfigurácia volieb pre komponenty TNC 119
- Konfigurácia volieb pre server Trusted Network Connect (TNC) 119
- Konfigurácia ďalších volieb pre klienta TNC (Trusted Network Connect) 119
- Konfigurácia volieb pre server TNCPM 120
- Konfigurácia e-mailového oznámenia na serveri Trusted Network Connect 121
- Konfigurácia odkazujúceho servera IP na serveri VIOS 122

Správa komponentov Trusted Network Connect (TNC) 122

Prezeranie protokolov servera Trusted Network Connect 122
Vytváranie politík pre klienta Trusted Network Connect 123
Spustenie overovania pre klienta Trusted Network Connect 124
Prezeranie výsledkov overovania Trusted Network Connect 124
Aktualizácia klienta Trusted Network Connect . . . 124
Správa politík na správu opráv 125
Import certifikátov Trusted Network Connect . . . 125
Nahlasovanie servera TNC 126
Riešenie problémov s funkciou Trusted Network Connect a správou opráv 126

PowerSC GUI (grafické užívateľské rozhranie) 129

PowerSC GUI - základné pojmy 129
PowerSC GUI - bezpečnosť 129
Načítanie obsahu koncového bodu na stránke súladu s nariadeniami 130
Inštalácia PowerSC GUI 130
Agent PowerSC GUI 130
Server PowerSC GUI 131
Požiadavky PowerSC GUI 131
Distribúcia bezpečnostného certifikátu verejných kľúčov na koncové body 131
Manuálne kopírovanie súboru s verejnými kľúčmi na koncové body 132
Kopírovanie súboru s verejnými kľúčmi na koncové body pomocou manažéra virtualizácie 132
Nastavenie užívateľských kont 132
Spustenie skriptov a príkazov pre nastavenie skupín 133
Používanie PowerSC GUI 133
Určenie jazyka PowerSC GUI 134
Navigácia v PowerSC GUI 135
Administrácia komunikácie medzi koncovými bodmi a serverom 135
Overenie komunikácie medzi koncovými bodmi a serverom 135
Odstránenie koncových bodov z monitorovania PowerSC GUI 135
Požiadavky na overenie a generovanie skladu kľúčov 136
Usporiadanie a zoskupenie koncových bodov 137
Vytváranie vlastných skupín 137
Pridanie alebo odstránenie systémov priradených existujúcej skupine 137
Odstránenie skupiny 137
Premenovanie skupiny 138
Klonovanie skupiny 138
Práca s profilmi súladu 138
Zobrazenie profilov súladu s nariadeniami 138
Vytvorenie vlastného profilu 139
Kopírovanie profilov na členy skupiny 139
Odstránenie vlastného profilu 139
Administrácia profilov a úrovní súladu s nariadeniami 139
Použitie profilov a úrovní súladu s nariadeniami . . 140
Zrušenie použitých úrovní súladu s nariadeniami . . 141
Kontrola ostatného použitého profilu a úrovne súladu s nariadeniami 141
Kontrola zatiaľ nepoužitého profilu alebo úrovne súladu s nariadeniami 141
Odoslanie e-mailového oznámenia, keď dôjde k udalosti súladu s nariadeniami 142
Monitorovanie bezpečnosti koncových bodov 142
Konfigurácia produktu Real Time Compliance (RTC) 143
Obnovenie starších konfiguračných volieb RTC (Real Time Compliance) 143
Kopírovanie konfiguračných volieb súladu s nariadeniami v reálnom čase (RTC) na iné skupiny. . 143
Úprava zoznamu súborov Real Time Compliance (RTC) 143
Obnovenie starších konfiguračných volieb monitorovania súborov RTC (Real Time Compliance). 144
Kopírovanie volieb monitorovania zoznamu súborov Real Time Compliance (RTC) na iné skupiny . . . 144
Spustenie kontroly Real Time Compliance (RTC) . . 144
Konfigurácia produktu Trusted Execution 144
Kopírovanie volieb Trusted Execution (TE) na iné skupiny 145
Úprava zoznamu súborov Trusted Execution (TE) 145
Kopírovanie volieb monitorovania zoznamu súborov Trusted Execution (TE) na iné skupiny 145
Zobrazenie stavu ďalších funkcií PowerSC 146
Prepínanie monitorovania Trusted Execution . . . 146
Odoslanie e-mailového oznámenia, keď dôjde k bezpečnostnej udalosti 147
Práca so zostavami 147
Výber skupiny pre zostavu 147
Distribúcia zostáv prostredníctvom e-mailu 148

Príkazy PowerSC Standard Edition 149

príkaz chvfilt 149
príkaz genvfilt 150
príkaz lsvfilt 151
príkaz mkvfilt. 152
príkaz pmconf 153
Príkaz pscon 157
Príkaz pscuiserverctl. 164
Príkaz pscxpert 166
príkaz rmvfilt 169
Príkaz vlantfw 170

Vyhlásenia 173

Hľadiská politiky ochrany osobných údajov 175
Ochranné známky 175

Index 177

O tomto dokumente

Tento dokument poskytuje administrátorom systému komplexné informácie o zabezpečení súborov, systému a siete.

Zvýraznenie

V tomto dokumente sa používajú tieto konvencie zvýraznenia:

Tučné písmo	Identifikuje príkazy, podrutiny, kľúčové slová, súbory, štruktúry, adresáre a iné položky, ktorých názvy sú preddefinované systémom. Identifikuje aj grafické objekty, ako sú tlačidlá, štítky a ikony, ktoré užívateľ vyberie.
Kurzíva	Identifikuje parametre, ktorých skutočné názvy alebo hodnoty má poskytnúť užívateľ.
Písmo s rovnakými rozstupmi	Identifikuje príklady špecifických hodnôt údajov, príklady textu podobného tomu, ktorý by ste mohli vidieť zobrazený, príklady častí programového kódu podobného tomu, ktorý by ste mohli zapísať ako programátor, správy zo systému, alebo informácie, ktoré by ste v skutočnosti mali zadať.

Rozlišovanie veľkosti písma v AIX

Všetko v operačnom systéme AIX rozlišuje veľké a malé písmená. Napríklad môžete použiť príkaz **ls** na vypísanie súborov. Ak napíšete LS, systém bude reagovať tak, že príkaz je nenájdený. Podobne FILEA, FiLea a filea sú tri rozdielne názvy súborov, aj vtedy ak sa nachádzajú v rovnakom adresári. Ak sa chcete vyhnúť tomu, aby ste spôsobili vykonanie nežiaducich akcií, vždy sa uistite, že používate správnu veľkosť písma.

ISO 9000

Pri vývoji a výrobe tohto produktu boli využité systémy kvality v súlade s normou ISO 9000.

Novinky v aplikácii PowerSC Standard Edition

Prečítajte si, čo je nové alebo čo sa zmenilo v produkte PowerSC Standard Edition v tejto kolekcii tém.

V tomto súbore PDF môžete na ľavom okraji vidieť revízne značky (|), ktoré identifikujú nové a zmenené informácie.

September 2017

Do grafického užívateľského rozhrania PowerSC boli pridané nasledujúce funkcie:

- Bol pridaný riadiaci panel so súhrnnými informáciami o zabezpečení a súlade, ktorý poskytuje okamžitý prehľad o všetkých informáciách týkajúcich sa súladu s predpismi a stave integrity súborov.
- Bola pridaná integrácia s vizualizačnými manažérmi, ako napríklad PowerVC, prostredníctvom integrácie Open Stack, ktorá umožňuje automatizované a bezpečné zisťovanie koncových bodov. Navyše integrácia podporuje cloudové prostredie s prehľadom o zabezpečení od prvej chvíle po vytvorení virtuálneho stroja.
- Boli pridané funkcie tvorby zostáv na podporu auditov. K dispozícii sú súhrnné aj podrobné zostavy o súlade a integrite súborov vo formáte HTML aj CSV. Môžete naplánovať okamžitú alebo dennú distribúciu týchto zostáv.
- Vylepšený editor profilov uľahčuje prispôsobenie pravidiel súladu a profilov. Pravidlá môžete teraz spájať z rozličných zdrojov a upraviť ich v grafickom užívateľskom rozhraní.
- Bola pridaná integrácia s manažérmi informácií o bezpečnostných udalostiach, ako napríklad QRadar. Záznamy syslog ponúkajúce prehľadné informácie o udalostiach súladu a integrity súborov uľahčujú integráciu.
- Bola vylepšená funkcia zrušenia zmien. Táto funkcia zjednodušuje komplexnú úlohu zrušenia zmien vykonaných profilom. Vydanie PowerSC 1.1.6 výrazne zjednodušuje proces zrušenia zmien pri použití profilu PCI.
- Bola zlepšená rozšíriteľnosť grafického užívateľského rozhrania (GUI) pre súlad s nariadeniami. Server GUI je horizontálne škálovateľný, pričom každá nová inštancia môže podporovať až 1000 ďalších koncových bodov.

Boli pridané nasledujúce funkcie pre TNCPM (Trusted Network Connect Patch Management):

- Boli predstavený proxy server poskytujúci ďalšiu vrstvu zabezpečenia, keďže umožňuje izolovať TNCPM od internetu.
- Integrácia dočasných opráv (iFix) do TNCPM je teraz plne automatizovaná. TNCPM dokáže monitorovať a opravovať bezpečnostné nedostatky operačného systému bez manuálneho zásahu zo strany užívateľa.
- Sťahovanie balíkov Open Source je teraz integrované do TNCPM, čo zjednodušuje tok úloh pri práci s balíkmi Open Source.

Bola pridaná nasledujúca funkcia na zlepšenie podpory súladu s nariadeniami:

- Bola pridaná voľba zostavy poskytujúca podrobné informácie o pravidlách v profile pri uplatnení profilu.

Súbory PDF k produktu PowerSC Standard Edition

Dokumentácia k produktu PowerSC Standard Edition je k dispozícii aj vo formáte PDF.

- PowerSC Standard Edititon
- Poznámky k vydaniu produktu PowerSC Standard Edition

PowerSC Standard Edition - základné pojmy

Tento prehľad súčasti PowerSC Standard Edition vysvetľuje funkcie, komponenty a hardvérovú podporu týkajúcu sa súčasti PowerSC Standard Edition.

PowerSC Standard Edition zaisťuje zabezpečenie a kontrolu systémov pracujúcich v prostredí cloud alebo vo virtualizovaných údajových centrách a poskytuje prehľad v celej spoločnosti a schopnosti správy. PowerSC Standard Edition je súprava funkcií, ku ktorým patria Security and Compliance Automation, Trusted Boot, Trusted Firewall, Trusted Logging, a Trusted Network Connect a Patch Management. Bezpečnostná technológia, ktorá sa umiestni do virtualizačnej vrstvy, zaistí ďalšiu bezpečnosť pre samostatné systémy.

Nasledujúca tabuľka uvádza podrobné informácie o vydaniach, funkcie zahrnuté v týchto vydaniach, komponentoch a procesorovom hardvéri, na ktorom je každý komponent k dispozícii.

Tabuľka 1. Komponenty PowerSC Standard Edition, popis, podpora operačného systému a podpora hardvéru

Komponenty	Popis	Podporovaný operačný systém	Podporovaný hardvér
Security and Compliance Automation	Automatizuje nastavenie, monitorovanie a auditovanie a konfigurácie bezpečnosti a súladu s nariadeniami pre nasledujúce štandardy: • Payment Card Industry Data Security Standard (PCI DSS) • Sarbanes-Oxley Act a COBIT compliance (SOX/COBIT) • STIG Ministerstva obrany USA • Health Insurance Portability and Accountability Act (HIPAA)	• AIX 5.3 • AIX 6.1 • AIX 7.1 • AIX 7.2	• POWER5 • POWER6 • POWER7 • POWER8
Trusted Boot	Meria bootovací obraz, operačný systém a aplikácie a testuje ich dôveru s použitím technológie virtuálneho TPM.	• AIX 6 s úrovňou 6100-07 alebo novší • AIX 7 s úrovňou 7100-01 alebo novší	POWER7, firmvér eFW7.4 alebo novší
Trusted Firewall	Šetrí čas a prostriedky - umožňuje priame smerovanie po špecifikovaných virtuálnych LAN (VLAN), ktoré sú riadené tým istým systémom Virtual I/O Server.	• AIX 6.1 • AIX 7.1 • AIX 7.2 • VIOS, verzia 2.2.1.4 alebo novší	• POWER6 • POWER7 • POWER8 • Virtual I/O Server, verzia 6.1S alebo novší
Trusted Logging	Protokoly systému AIX sa v reálnom čase centrálne umiestňujú na virtuálnom I/O serveri (VIOS). Táto funkcia zabezpečuje nesfalšovateľné protokolovanie a pohodlné zálohovanie a správu záloh.	• AIX 5.3 • AIX 6.1 • AIX 7.1 • AIX 7.2	• POWER5 • POWER6 • POWER7 • POWER8
Trusted Network Connect a Patch Management	Overí, či všetky systémy AIX vo virtuálnom prostredí sú na špecifikovanej úrovni softvéru a úrovni opráv a poskytuje nástroje na správu, ktoré zabezpečia, že všetky systémy AIX sú na špecifikovanej úrovni softvéru. Umožňuje výstrahy, ak sa do siete pridá virtuálny systém na úrovni o jeden stupeň nižšej alebo ak sa vydá bezpečnostná oprava, ktorá má vplyv na systém.	• AIX 5.3 • AIX 6.1 • AIX 7.1 • AIX 7.2	• POWER5 • POWER6 • POWER7 • POWER8

Tabuľka 1. Komponenty PowerSC Standard Edition, popis, podpora operačného systému a podpora hardvéru (pokračovanie)

Komponenty	Popis	Podporovaný operačný systém	Podporovaný hardvér
Klient Trusted Network Connect	Klient Trusted Network Connect vyžaduje niektorý z komponentov uvedených s operačným systémom.	• AIX 6.1 s úrovňou 6100-06 alebo novší • Systém konzoly AIX, verzia 7.1 Service Update Management Assistant (SUMA) v prostredí SUMA na správu opráv • Konzolový systém Service Update Management Assistant (SUMA) systému AIX verzie 7.2.1 v rámci prostredia SUMA na správu opráv	

Inštalácia PowerSC Standard Edition

Pre každú špecifickú funkciu PowerSC Standard Edition musíte nainštalovať sadu súborov.

K dispozícii sú nasledujúce sady súborov pre softvér PowerSC Standard Edition a PowerSC GUI (grafické užívateľské rozhranie):

- powerscStd.ice: Inštaluje sa v systémoch AIX, v ktorých sa vyžaduje funkcia Security and Compliance Automation softvéru PowerSC Standard Edition. Tento program vyžaduje aspoň 5 MB voľného miesta na disku v súborovom systéme "/".
- powerscStd.vtpm: Nainštalovaná v systémoch AIX, ktoré vyžadujú funkciu Trusted Boot v PowerSC Standard Edition. Sadu súborov powerscStd.vtpm nájdete na disku so základným operačným systémom AIX alebo na stránke from https://www-01.ibm.com/marketing/iwm/iwm/web/preLogin.do?source=aixbp&S_PKG=vtpm.
- powerscStd.vlog: Nainštalovaná v systémoch AIX, ktoré vyžadujú funkciu Trusted Logging v PowerSC Standard Edition.
- powerscStd.tnc_pm: Inštaluje sa v systémoch AIX, verzia 7.1 TL4 a novších s konzolovým systémom Service Update Management Assistant (SUMA) v rámci prostredia SUMA na účely správy opráv 7.2.1.0. Do systému TNC Patch Manager by ste mali nainštalovať softvér Curl 7.52.1-1 pre bezpečný prenos opráv ifix z lokality IBM Security.
- powerscStd.svm: Inštaluje sa v systémoch AIX, ktoré by mohli profitovať z funkcie smerovania v PowerSC Standard Edition.
- powerscStd.rtc: Inštaluje sa v systémoch AIX vyžadujúcich funkciu Real Time Compliance softvéru PowerSC Standard Edition.
- powerscStd.uiAgent.rte: Inštaluje sa v systémoch AIX, ktoré budú spravované prostredníctvom softvéru PowerSC GUI (grafické užívateľské rozhranie). Aby bolo možné nainštalovať sadu súborov powerscStd.uiAgent.rte verzie 116, musíte mať k dispozícii balík powerscStd.ice verzie 115 alebo novší.
- powerscStd.uiServer.rte: Inštaluje sa v systéme AIX, ktorý bol nakonfigurovaný špecificky na účely spúšťania servera PowerSC GUI (grafické užívateľské rozhranie).

Softvér PowerSC Standard Edition a PowerSC GUI (grafické užívateľské rozhranie) môžete nainštalovať prostredníctvom nasledujúcich rozhraní:

- Príkaz **installp** z rozhrania príkazového riadka
- Rozhranie SMIT

Ak chcete inštalovať PowerSC Standard Edition prostredníctvom rozhrania SMIT, postupujte podľa týchto krokov:

1. Spustite tento príkaz:
   ```
   % smitty installp
   ```
2. Vyberte voľbu **Inštalovať softvér**.
3. Vyberte vstupné zariadenie alebo adresár pre softvér, ktorým zadáte umiestnenie a inštalačný súbor inštalačného obrazu IBM Compliance Expert. Ak má napríklad inštalačný obraz cestu k adresáru a názov súboru /usr/sys/inst.images/powerscStd.vtpm, musíte zadať cestu k súboru v poli**INPUT**.
4. Zobrazte a akceptujte licenčnú zmluvu. Akceptujte licenčnú zmluvu pomocou šípky nadol, ktorou vyberiete možnosť **AKCEPTOVAŤ nové licenčné zmluvy**, a stlačte kláves tabulátora, čím zmeníte hodnotu na **Áno**.
5. Stlačte kláves **Enter** pre spustenie inštalácie.
6. Po dokončení inštalácie skontrolujte, či je stav príkazu **OK**.

V téme “Inštalácia PowerSC GUI” na strane 130 nájdete bližšie informácie o inštalácii softvéru PowerSC GUI (grafické užívateľské rozhranie)

Zobrazenie softvérovej licencie

Softvérovú licenciu možno zobraziť v rozhraní príkazového riadka pomocou tohto príkazu:

```
% installp –lE –d cesta/názov súboru
```

cesta/názov súboru určuje inštalačný obraz PowerSC Standard Edition.

Tento príkaz môžete zadať napríklad pomocou rozhrania príkazového riadka, čím určíte licenčné informácie súvisiace s PowerSC Standard Edition:

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

Súvisiace koncepty:

“PowerSC Standard Edition - základné pojmy” na strane 5
Tento prehľad súčasti PowerSC Standard Edition vysvetľuje funkcie, komponenty a hardvérovú podporu týkajúcu sa súčasti PowerSC Standard Edition.

“Inštalácia funkcie Trusted Boot” na strane 99
Existujú určité vyžadované hardvérové a softvérové konfigurácie, ktoré sú potrebné na inštaláciu funkcie Trusted Boot.

Súvisiace úlohy:

“Inštalácia funkcie Trusted Firewall” na strane 105
Inštalácia funkcie PowerSC Trusted Firewall je podobná ako inštalácia funkcií PowerSC.

“Inštalácia funkcie Trusted Logging” na strane 112
Funkciu PowerSC Trusted Logging môžete nainštalovať pomocou rozhrania príkazového riadka alebo nástroja SMIT.

“Konfigurácia komponentov TNC” na strane 118
Každý komponent Trusted Network Connect (TNC) vyžaduje isté nastavenie, aby ste ho mohli používať vo vašom prostredí.

Funkcia Security and Compliance Automation

AIX Profile Manager spravuje vopred definované profily v záujme zabezpečenia a súladu s požiadavkami. Softvér PowerSC Real Time Compliance neustále monitoruje aktivované systémy AIX, aby sa zabezpečila ich konzistentná a bezpečná konfigurácia.

Profily XML automatizujú uplatňovanie odporúčanej konfigurácie systémov AIX od IBM, aby bola v súlade s požiadavkami noriem Payment Card Data Security Standard, Sarbanes-Oxley Act, STIGA Ministerstva obrany USA pre systémy UNIX a Health Insurance Portability and Accountability Act (HIPAA). Organizácie, ktoré chcú dodržiavať tieto bezpečnostné normy, musia používať vopred definované nastavenia zabezpečenia systému.

AIX Profile Manager funguje ako modul plug-in softvéru IBM® Systems Director, ktorý zjednodušuje uplatňovanie nastavení zabezpečenia, monitorovanie nastavení zabezpečenia a auditovanie nastavení zabezpečenia, pre operačný systém AIX aj systémy Virtual I/O Server (VIOS). Aby ste mohli používať funkciu automatizácie zabezpečenia a súladu, aplikácia PowerSC musí byť nainštalovaná na riadených systémoch AIX, ktoré sú v súlade s príslušnými bezpečnostnými normami. Funkcia Security and Compliance Automation je súčasťou produktu PowerSC Standard Edition.

Inštalačný balík PowerSC Standard Edition (5765-PSE) musíte nainštalovať v riadených systémoch AIX. Tento inštalačný balík nainštaluje sadu súborov powerscStd.ice, ktorú môžete implementovať v systéme pomocou príkazu AIX Profile Manager alebo **pscxpert**. Funkcia PowerSC with IBM Compliance Expert Express (ICEE) uľahčuje správu a vylepšovanie profilov XML. Profily XML sú spravované softvérom AIX Profile Manager.

Poznámka: Pred uplatnením bezpečnostného profilu nainštaluje do systému všetky požadované aplikácie.

Koncepty automatizácie bezpečnosti a súladu s nariadeniami

Funkcia bezpečnosti a súladu s nariadeniami PowerSC je automatizovaná metóda, ktorou sú systémy AIX konfigurované a auditované v súlade s nariadeniami a štandardmi DoD STIG (U.S. Department of Defense (DoD) Security Technical Implementation Guide), PCI DSS (Payment Card Industry Data Security Standard), zákona Sarbanes-Oxley, súladu s nariadeniami COBIT (SOX/COBIT) a HIPA (Health Insurance Portability and Accountability Act).

PowerSC pomáha automatizovať konfiguráciu a monitorovanie systémov, ktoré musia byť v súlade so štandardom zabezpečenia údajov PCI verzia 1.2, 2.0 alebo 3.0. Z toho dôvodu je funkcia bezpečnosti a monitorovania PowerSC presnou a úplnou metódou automatizácie bezpečnostnej konfigurácie, ktorá umožňuje v oblasti IT naplniť požiadavky súladu s nariadeniami DoD UNIX STIG, PCI DSS, zákona Sarbanes-Oxley, súladu s nariadeniami COBIT (SOX/COBIT) a HIPPA (Health Insurance Portability and Accountability Act).

Poznámka: Funkcia bezpečnosti a súladu s nariadeniami PowerSC aktualizuje existujúce profily XML použité vo vydaní IBM Compliance Expert Express (ICEE). Profily XML v PowerSC Standard Edition môžete použiť príkazom **pscxpert**, podobne ako v ICEE.

Vopred nakonfigurované profily súladu s nariadeniami v PowerSC Standard Edition znižujú administratívne zaťaženie pri interpretácii dokumentácie súladu s nariadeniami a pri implementácii štandardov vo forme špecifických systémových konfiguračných parametrov. Táto technológia svojimi automatizovanými procesmi znižuje náklady na konfiguráciu a auditovanie súladu s nariadeniami. Produkt IBMPowerSC Standard Edition je vytvorený tak, aby pomohol účinne spravovať systémové požiadavky súvisiace s napĺňaním súladu s externými štandardmi, čo môže viesť k zníženiu nákladov a zároveň k zvýšeniu súladu.

Súlad s pokynmi STIG Ministerstva obrany USA

Ministerstvo obrany USA (ďalej aj „DoD“) vyžaduje vysoko zabezpečené počítačové systémy. Táto úroveň zabezpečenia a kvality definovaná Ministerstvom obrany USA splňuje požiadavky na kvalitu a užívateľskú bázu systému AIX na serveroch Power Systems.

Bezpečné operačné systémy, akým je aj systém AIX, musia byť nakonfigurované presne, aby boli dosiahnuté definované ciele v oblasti zabezpečenia. Ministerstvo obrany USA uznalo potrebu konfigurácií zabezpečenia všetkých operačných systémov v nariadení 8500.1. Toto nariadenie stanovuje zásady a uložilo agentúre US Defense Information Security Agency (DISA) povinnosť poskytovať súčinnosti pri konfigurácii zabezpečenia.

Agentúra DISA zdokumentovala hlavné zásady a pravidlá v príručke UNIX Security Technical Implementation Guide (STIG), ktorá definuje prostredie splňujúce alebo prekračujúce požiadavky na zabezpečenie systémov Ministerstva obrany USA, ktoré sa prevádzkujú na úrovni kategórie zabezpečenia úloh (MAC) citlivosti IT zahrňujúcej citlivé informácie. Ministerstvo obrany USA má prísne požiadavky na zabezpečenie IT a definovalo podrobné požiadavky na konfiguračné nastavenia s cieľom zabezpečiť bezpečnú prevádzku systémov. Môžete využiť odborné poradenstvo. PowerSC Standard Edition pomáha zautomatizovať proces konfigurácie nastavení podľa požiadaviek Ministerstva obrany USA.

Poznámka: Všetky súbory vlastných skriptov na zabezpečenie súladu s požiadavkami Ministerstva obrany USA sú uložené v adresári /etc/security/pscexpert/dodv2.

PowerSC Standard Edition podporuje požiadavky verzie 1, vydanie 2 dokumentu AIX DoD STIG. V nasledujúcich tabuľkách nájdete súhrn požiadaviek a informácie o tom, ako môžete zabezpečiť súlad s nimi.

Tabuľka 2. Všeobecné požiadavky Ministerstva obrany USA

ID kontrolného bodu STIG Ministerstva obrany USA	Kategória pravidla STIG	Popis	Umiestnenie skriptu, v ktorom je definovaná akcia, a výsledky akcie zabezpečujúcej súlad
AIX00020	2	Musí byť implementovaný softvér AIX Trusted Computing Base.	**Umiestnenie** /etc/security/pscexpert/dodv2/trust **Akcia na zabezpečenie súladu** Zabezpečuje, že systém bude spĺňať definované požiadavky.
AIX00040	2	Musí byť použitý príkaz **securetcpip**.	**Umiestnenie** /etc/security/pscexpert/dodv2/dodsecuretcpip **Akcia na zabezpečenie súladu** Zabezpečuje, že systém bude spĺňať definované požiadavky.
AIX00060	2	Systém musí byť týždenne kontrolovaný, či neobsahuje neoprávnené súbory setuid alebo či nedošlo k neoprávnenej úprave oprávnených súborov setuid.	**Umiestnenie** /etc/security/pscexpert/dodv2/trust **Akcia na zabezpečenie súladu** Týždenne skontroluje, či nedošlo k zmenám v určených súboroch.
AIX00080	1	Atribút SYSTEM nesmie mať hodnotu *none* pri žiadnom konte.	**Umiestnenie** /etc/security/pscexpert/dodv2/SYSattr **Akcia na zabezpečenie súladu** Zabezpečuje, že určený atribút bude mať inú hodnotu ako *none*. **Poznámka:** Toto nastavenie nebude automaticky zmenené pri obnovení predvolenej politiky systému AIX prostredníctvom súboru DoDv2_to_ AIXDefault.xml. Toto nastavenie je potrebné manuálne zmeniť.

Tabuľka 2. Všeobecné požiadavky Ministerstva obrany USA (pokračovanie)

ID kontrolného bodu STIG Ministerstva obrany USA	Kategória pravidla STIG	Popis	Umiestnenie skriptu, v ktorom je definovaná akcia, a výsledky akcie zabezpečujúcej súlad
AIX00200	2	Systém nesmie povoľovať prechod smerovaného vysielania cez bránu.	**Umiestnenie** /etc/security/pscexpert/dodv2/ntwkoptsdod **Akcia na zabezpečenie súladu** Pre voľbu siete direct_broadcast nastaví hodnotu *0*.
AIX00210	2	Systém musí poskytovať ochranu pred útokmi cez ICMP (Internet Control Message Protocol) pri pripojeniach TCP.	**Umiestnenie** /etc/security/pscexpert/dodv2/ntwkoptsdod **Akcia na zabezpečenie súladu** Pre voľbu siete tcp_icmpsecure nastaví hodnotu *1*.
AIX00220	2	Systém musí poskytovať ochranu zásobníka TCP pred útokmi vynulovaním pripojenia, synchronizovaním (SYN) a vkladaním údajov (injection).	**Umiestnenie** /etc/security/pscexpert/dodv2/ntwkoptsdod **Akcia na zabezpečenie súladu** Zabezpečí, že voľba siete tcp_tcpsecure bude mať hodnotu *7*.
AIX00230	2	Systém musí poskytovať ochranu pred útokmi fragmentáciou IP.	**Umiestnenie** /etc/security/pscexpert/dodv2/ntwkoptsdod **Akcia na zabezpečenie súladu** Nastaví voľbu siete ip_nfrag na hodnotu *200*.
AIX00300	1,2,3	V systéme nesmie byť aktívna služba bootp.	**Umiestnenie** /etc/security/pscexpert/dodv2/inetdservices **Akcia na zabezpečenie súladu** Zakazuje určenú službu.
AIX00310	2	Musia existovať súbory /etc/ftpaccess.ctl.	**Umiestnenie** /etc/security/pscexpert/dodv2/dodv2loginherald **Akcia na zabezpečenie súladu** Zabezpečí, že existuje súbor.
GEN000020	2	Systém musí vyžadovať overenie pri spustení v režime s jedným užívateľom.	**Umiestnenie** /etc/security/pscexpert/dodv2/rootpasswd_home **Akcia na zabezpečenie súladu** Zabezpečí, že konto užívateľa root pre spúšťacie oddiely bude zabezpečené heslom v súbore /etc/security/passwd. **Poznámka:** Toto nastavenie nebude automaticky zmenené pri obnovení predvolenej politiky systému AIX prostredníctvom súboru DoDv2_to_ AIXDefault.xml. Toto nastavenie je potrebné manuálne zmeniť.
GEN000100	1	Operačný systém musí mať podporované vydanie.	**Umiestnenie** /etc/security/pscexpert/dodv2/dodv2cat1 **Akcia na zabezpečenie súladu** Zobrazí výsledky určených testov pravidiel.
GEN000120	2	Musia byť nainštalované najnovšie opravy zabezpečenia systému.	**Umiestnenie** /usr/sbin/instfix -i /etc/security/pscexpert/dodv2/dodv2cat1 **Akcia na zabezpečenie súladu** Nakonfigurujte prostredníctvom funkcie Trusted Network Connect.

Tabuľka 2. Všeobecné požiadavky Ministerstva obrany USA (pokračovanie)

ID kontrolného bodu STIG Ministerstva obrany USA	Kategória pravidla STIG	Popis	Umiestnenie skriptu, v ktorom je definovaná akcia, a výsledky akcie zabezpečujúcej súlad
GEN000140	2	Systém musí byť týždenne kontrolovaný, či neobsahuje neoprávnené súbory setuid alebo či nedošlo k neoprávnenej úprave oprávnených súborov setuid.	**Umiestnenie** /etc/security/pscexpert/dodv2/trust **Akcia na zabezpečenie súladu** Týždenne skontroluje, či nedošlo k zmenám v určených súboroch.
GEN000220	2	Systém musí byť týždenne kontrolovaný, či neobsahuje neoprávnené súbory setuid alebo či nedošlo k neoprávnenej úprave oprávnených súborov setuid.	**Umiestnenie** /etc/security/pscexpert/dodv2/trust **Akcia na zabezpečenie súladu** Týždenne skontroluje, či nedošlo k zmenám v určených súboroch.
GEN000240	2	Systémové hodiny musia byť synchronizované so zdrojom času schváleným Ministerstvom obrany USA.	**Umiestnenie** /etc/security/pscexpert/dodv2/dodv2cmntrows **Akcia na zabezpečenie súladu** Zabezpečuje, že systémové hodiny budú v súlade s požiadavkami.
GEN000241	2	Systémové hodiny musia byť neustále - alebo aspoň denne - synchronizované.	**Umiestnenie** /etc/security/pscexpert/dodv2/dodv2cmntrows **Akcia na zabezpečenie súladu** Zabezpečuje, že systémové hodiny budú v súlade s požiadavkami.
GEN000242	2	Systém musí používať aspoň dva zdroje času pre synchronizáciu hodín.	**Umiestnenie** /etc/security/pscexpert/dodv2/dodv2netrules **Akcia na zabezpečenie súladu** Zabezpečuje, že sa bude používať viac ako jeden zdroj času na synchronizáciu hodín.
GEN000280	2	Nesmú byť povolené priame prihlásenia do nasledujúcich typov kont: • application • default • shared • utility	**Umiestnenie** /etc/security/pscexpert/dodv2/lockacc_rlogin **Akcia na zabezpečenie súladu** Zabráni priamym prihláseniam do určených kont.
GEN000290	2	V systéme sa nesmú nachádzať nepotrebné kontá.	**Umiestnenie** /etc/security/pscexpert/dodv2/lockacc_rlogin **Akcia na zabezpečenie súladu** Zabezpečuje, že nebudú existovať žiadne nepoužívané kontá.

Tabuľka 2. Všeobecné požiadavky Ministerstva obrany USA (pokračovanie)

ID kontrolného bodu STIG Ministerstva obrany USA	Kategória pravidla STIG	Popis	Umiestnenie skriptu, v ktorom je definovaná akcia, a výsledky akcie zabezpečujúcej súlad
GEN000300 (súvisí s GEN000320, GEN000380 a GEN000880)	2	Všetky kontá v systéme musia mať jedinečné meno užívateľa alebo konta a jedinečné heslo užívateľa alebo konta.	**Umiestnenie** /etc/security/pscexpert/dodv2/grpusrpass_chk **Akcia na zabezpečenie súladu** Zabezpečuje, že všetky kontá budú spĺňať definované požiadavky. **Poznámka:** Toto nastavenie nebude automaticky zmenené pri obnovení predvolenej politiky systému AIX prostredníctvom súboru DoDv2_to_ AIXDefault.xml. Toto nastavenie je potrebné manuálne zmeniť.
GEN000320 (súvisí s GEN000300, GEN000380 a GEN000880)	2	Všetky kontá v systéme musia mať jedinečné meno užívateľa alebo konta a jedinečné heslo užívateľa alebo konta.	**Umiestnenie** /etc/security/pscexpert/dodv2/grpusrpass_chk **Akcia na zabezpečenie súladu** Zabezpečuje, že všetky kontá budú spĺňať definované požiadavky. **Poznámka:** Toto nastavenie nebude automaticky zmenené pri obnovení predvolenej politiky systému AIX prostredníctvom súboru DoDv2_to_ AIXDefault.xml. Toto nastavenie je potrebné manuálne zmeniť.
GEN000340	2	Identifikátory užívateľov (UID) a identifikátory skupín (GID), ktoré sú rezervované pre systémové kontá, nesmú byť priradené k nesystémovým kontám alebo nesystémovým skupinám.	**Umiestnenie** /etc/security/pscexpert/dodv2/account **Akcia na zabezpečenie súladu** Toto nastavenie je automaticky povolené, aby sa uplatňovalo pravidlo.
GEN000360	2	Identifikátory UID a GID, ktoré sú rezervované pre systémové kontá, nesmú byť priradené k nesystémovým kontám alebo nesystémovým skupinám.	**Umiestnenie** /etc/security/pscexpert/dodv2/account **Akcia na zabezpečenie súladu** Toto nastavenie je automaticky povolené, aby sa uplatňovalo pravidlo.
GEN000380 (súvisí s GEN000300, GEN000320 a GEN000880)	2	Všetky kontá v systéme musia mať jedinečné meno užívateľa alebo konta a jedinečné heslo užívateľa alebo konta.	**Umiestnenie** /etc/security/pscexpert/dodv2/grpusrpass_chk **Akcia na zabezpečenie súladu** Zabezpečuje, že všetky kontá budú spĺňať definované požiadavky.
GEN000400	2	Prihlasovací pruh Ministerstva obrany USA (DoD) sa musí zobraziť okamžite pred prihlasovacími výzvami v konzole alebo v rámci nich.	**Umiestnenie** /etc/security/pscexpert/dodv2/dodv2loginherald **Akcia na zabezpečenie súladu** Zobrazí požadovaný pruh.
GEN000402	2	Prihlasovací pruh DoD sa musí zobraziť okamžite pred prihlasovacími výzvami v grafickom rozhraní alebo v rámci nich.	**Umiestnenie** /etc/security/pscexpert/dodv2/dodv2loginherald **Akcia na zabezpečenie súladu** Ako prihlasovací pruh je nastavený pruh DoD.

Tabuľka 2. Všeobecné požiadavky Ministerstva obrany USA (pokračovanie)

ID kontrolného bodu STIG Ministerstva obrany USA	Kategória pravidla STIG	Popis	Umiestnenie skriptu, v ktorom je definovaná akcia, a výsledky akcie zabezpečujúcej súlad
GEN000410	2	Služba FTPS (File Transfer Protocol over SSL) alebo FTP (File Transfer Protocol) musí byť v systéme nakonfigurovaná s prihlasovacím pruhom DoD.	**Umiestnenie** /etc/security/pscexpert/dodv2/dodv2loginherald **Akcia na zabezpečenie súladu** Zobrazí pruh pri použití protokolu FTP.
GEN000440	2	Úspešné a neúspešné pokusy o prihlásenie a odhlásenie musia byť zaznamenané.	**Umiestnenie** /etc/security/pscexpert/dodv2/loginout **Akcia na zabezpečenie súladu** Povolí vyžadované protokolovanie.
GEN000452	2	Systém musí zobraziť dátum a čas posledného prihlásenia do konta pri každom prihlásení.	**Umiestnenie** /etc/security/pscexpert/dodv2/sshDoDconfig **Akcia na zabezpečenie súladu** Zobrazí požadované informácie.
GEN000460	2	Toto pravidlo zakáže konto po 3 po sebe nasledujúcich neúspešných pokusoch o prihlásenie.	**Umiestnenie** /etc/security/pscexpert/dodv2/chusrattrdod **Akcia na zabezpečenie súladu** Nastaví limit pokusov o prihlásenie na určenú hodnotu.
GEN000480	2	Toto pravidlo nastaví dobu oneskorenia prihlásenia na 4 sekundy.	**Umiestnenie** /etc/security/pscexpert/dodv2/chdefstanzadod **Akcia na zabezpečenie súladu** Nastaví dobu oneskorenia prihlásenia na požadovanú hodnotu.
GEN000540	2	Toto pravidlo zabezpečí, že globálne konfiguračné súbory hesiel v systéme budú nakonfigurované v súlade s požiadavkami na heslá.	**Umiestnenie** /etc/security/pscexpert/dodv2/chusrattrdod **Akcia na zabezpečenie súladu** Nastaví vyžadované nastavenia hesiel.
GEN000560	1	Všetky kontá v systéme musia mať platné heslá.	**Umiestnenie** /etc/security/pscexpert/dodv2/grpusrpass_chk **Akcia na zabezpečenie súladu** Zabezpečí, že všetky kontá budú mať heslá.
GEN000580	2	Toto pravidlo zabezpečí, že všetky heslá budú obsahovať aspoň 14 znakov.	**Umiestnenie** /etc/security/pscexpert/dodv2/chusrattrdod **Akcia na zabezpečenie súladu** Nastaví minimálnu dĺžku hesla na 14 znakov.
GEN000585	2	Systém musí používať šifrovací hashovací algoritmus schválený na základe štandardu FIPS (Federal Information Processing Standards) 140-2 pri generovaní hodnôt hash hesiel pre kontá.	**Umiestnenie** /etc/security/pscexpert/dodv2/fipspasswd **Akcia na zabezpečenie súladu** Zabezpečuje, že hodnoty hash hesiel používajú schválený hashovací algoritmus.

Tabuľka 2. Všeobecné požiadavky Ministerstva obrany USA (pokračovanie)

ID kontrolného bodu STIG Ministerstva obrany USA	Kategória pravidla STIG	Popis	Umiestnenie skriptu, v ktorom je definovaná akcia, a výsledky akcie zabezpečujúcej súlad
GEN000590	2	Systém musí používať šifrovací hashovací algoritmus schválený na základe štandardu FIPS 140-2 pri generovaní hodnôt hash hesiel pre kontá.	**Umiestnenie** /etc/security/pscexpert/dodv2/fipspasswd **Akcia na zabezpečenie súladu** Zabezpečuje, že hodnoty hash hesiel používajú schválený hashovací algoritmus.
GEN000595	2	Používať schválený šifrovací hashovací algoritmus pri generovaní hodnôt hash hesiel pre kontá.	**Umiestnenie** /etc/security/pscexpert/dodv2/fipspasswd **Akcia na zabezpečenie súladu** Zabezpečuje, že hodnoty hash hesiel používajú schválený hashovací algoritmus.
GEN000640	2	Toto pravidlo vyžaduje, aby heslo obsahovalo aspoň jeden neabecedný znak.	**Umiestnenie** /etc/security/pscexpert/dodv2/chusrattrdod **Akcia na zabezpečenie súladu** Nastaví minimálny počet neabecedných znakov v hesle na 1.
GEN000680	2	Toto pravidlo zabezpečuje, že heslo nebude obsahovať viac ako tri po sebe sa opakujúce znaky.	**Umiestnenie** /etc/security/pscexpert/dodv2/chusrattrdod **Akcia na zabezpečenie súladu** Nastaví maximálny počet opakujúcich sa znakov v hesle na 3.
GEN000700	2	Toto pravidlo zabezpečí, že globálne konfiguračné súbory hesiel v systéme budú nakonfigurované v súlade s požiadavkami na heslá.	**Umiestnenie** /etc/security/pscexpert/dodv2/chusrattrdod **Akcia na zabezpečenie súladu** Zabezpečuje, že konfiguračné súbory hesiel splňujú požiadavky.
GEN000740	2	Všetky heslá kont neinteraktívneho a automatizovaného spracovania musia byť uzamknuté (GEN000280). Nesmie byť povolené priame prihlásenie do zdieľaných, predvolených, aplikačných ani pomocných kont. (GEN002640) Predvolené systémové kontá musia byť zakázané alebo odstránené.	**Umiestnenie** /etc/security/pscexpert/dodv2/loginout /etc/security/pscexpert/dodv2/lockacc_rlogin **Akcia na zabezpečenie súladu** Toto nastavenie je automaticky povolené.
GEN000740	2	Všetky heslá kont neinteraktívneho a automatizovaného spracovania musia byť zmenené aspoň raz za rok alebo uzamknuté.	**Umiestnenie** /etc/security/pscexpert/dodv2/lockacc_rlogin **Akcia na zabezpečenie súladu** Zabezpečuje, že určené heslá budú zmenené aspoň raz za rok alebo uzamknuté.

Tabuľka 2. Všeobecné požiadavky Ministerstva obrany USA (pokračovanie)

ID kontrolného bodu STIG Ministerstva obrany USA	Kategória pravidla STIG	Popis	Umiestnenie skriptu, v ktorom je definovaná akcia, a výsledky akcie zabezpečujúcej súlad
GEN000750	2	Toto pravidlo vyžaduje, aby nové heslá obsahovali minimálne 4 znaky, ktoré neboli súčasťou starého hesla.	**Umiestnenie** /etc/security/pscexpert/dodv2/chusrattrdod **Akcia na zabezpečenie súladu** Nastaví minimálny vyžadovaný počet nových znakov v novom hesle na 4.
GEN000760	2	Kontá musia byť uzamknuté po 35 dňoch nečinnosti.	**Umiestnenie** /etc/security/pscexpert/dodv2/disableacctdod **Akcia na zabezpečenie súladu** Uzamkne kontá po 35 dňoch nečinnosti.
GEN000790	2	Systém nesmie povoľovať používanie slovníkových slov ako hesiel.	**Umiestnenie** /etc/security/pscexpert/dodv2/chuserstanzadod **Akcia na zabezpečenie súladu** Zabezpečuje, že predvolene nastavené heslo nebude slabé.
GEN000800	2	Toto pravidlo zabezpečuje, že nebude možné znova použiť posledných päť hesiel.	**Umiestnenie** /etc/security/pscexpert/dodv2/chusrattrdod **Akcia na zabezpečenie súladu** Zabezpečuje, že nové heslo nebude rovnaké ako žiadne z posledných 5 hesiel.
GEN000880 (súvisí s GEN000300, GEN000320 a GEN000380)	2	Všetky kontá v systéme musia mať jedinečné meno užívateľa alebo konta a jedinečné heslo užívateľa alebo konta.	**Umiestnenie** /etc/security/pscexpert/dodv2/grpusrpass_chk **Akcia na zabezpečenie súladu** Zabezpečuje, že všetky kontá budú spĺňať definované požiadavky.
GEN000900	3	Domovský adresár užívateľa root nesmie byť koreňový adresár (/).	**Umiestnenie** /etc/security/pscexpert/dodv2/rootpasswd_home **Akcia na zabezpečenie súladu** Zabezpečuje, že systém bude spĺňať definovanú požiadavku. **Poznámka:** Toto nastavenie nebude automaticky zmenené pri obnovení predvolenej politiky systému AIX prostredníctvom súboru DoDv2_to_ AIXDefault.xml. Toto nastavenie je potrebné manuálne zmeniť.
GEN000940	2	Cesta vyhľadávania pre spustiteľné súbory v konte užívateľa root musí byť predvolená cesta a môže obsahovať iba absolútne cesty.	**Umiestnenie** /etc/security/pscexpert/dodv2/fixpathvars **Akcia na zabezpečenie súladu** Zabezpečuje, že systém bude spĺňať definované požiadavky. **Poznámka:** Toto nastavenie nebude automaticky zmenené pri obnovení predvolenej politiky systému AIX prostredníctvom súboru DoDv2_to_ AIXDefault.xml. Toto nastavenie je potrebné manuálne zmeniť.
GEN000945	2	Cesta vyhľadávania pre knižnice v konte užívateľa root musí byť predvolená cesta systému a môže obsahovať iba absolútne cesty.	**Umiestnenie** /etc/security/pscexpert/dodv2/fixpathvars **Akcia na zabezpečenie súladu** Zabezpečuje, že systém bude spĺňať definované požiadavky. **Poznámka:** Toto nastavenie nebude automaticky zmenené pri obnovení predvolenej politiky systému AIX prostredníctvom súboru DoDv2_to_ AIXDefault.xml. Toto nastavenie je potrebné manuálne zmeniť.

Tabuľka 2. Všeobecné požiadavky Ministerstva obrany USA (pokračovanie)

ID kontrolného bodu STIG Ministerstva obrany USA	Kategória pravidla STIG	Popis	Umiestnenie skriptu, v ktorom je definovaná akcia, a výsledky akcie zabezpečujúcej súlad
GEN000950	2	Zoznam vopred načítaných knižníc konta užívateľa root musí byť prázdny.	**Umiestnenie** /etc/security/pscexpert/dodv2/fixpathvars **Akcia na zabezpečenie súladu** Zabezpečuje, že systém bude spĺňať definované požiadavky. **Poznámka:** Toto nastavenie nebude automaticky zmenené pri obnovení predvolenej politiky systému AIX prostredníctvom súboru DoDv2_to_ AIXDefault.xml. Toto nastavenie je potrebné manuálne zmeniť.
GEN000960 (súvisí s GEN003000, GEN003020, GEN003160, GEN003360 a GEN003380)	2	Konto užívateľa root nesmie obsahovať globálne zapisovateľné adresáre v ceste vyhľadávania spustiteľných súborov.	**Umiestnenie** /etc/security/pscexpert/dodv2/rmwwpaths **Akcia na zabezpečenie súladu** Zabezpečuje, že systém bude spĺňať definované požiadavky. **Poznámka:** Toto nastavenie nebude automaticky zmenené pri obnovení predvolenej politiky systému AIX prostredníctvom súboru DoDv2_to_ AIXDefault.xml. Toto nastavenie je potrebné manuálne zmeniť.
GEN000980	2	Systém nesmie povoľovať kontu užívateľa root priame prihlásenie okrem systémovej konzoly.	**Umiestnenie** /etc/security/pscexpert/dodv2/chuserstanzadod **Akcia na zabezpečenie súladu** Zabezpečuje, že systém bude spĺňať definované požiadavky.
GEN001000	2	Vzdialené konzoly musia byť zakázané a chránené pred neoprávneným prístupom.	**Umiestnenie** /etc/security/pscexpert/dodv2/remoteconsole **Akcia na zabezpečenie súladu** Zabezpečuje, že určené konzoly budú zakázané.
GEN001020	2	Konto užívateľa root sa nesmie používať na priame prihlásenie.	**Umiestnenie** /etc/security/pscexpert/dodv2/sshDoDconfig **Akcia na zabezpečenie súladu** Zakáže priame prihlásenie pre konto užívateľa root.
GEN001060	2	Systém musí zaznamenávať do protokolu úspešné aj neúspešné pokusy o prístup ku kontu užívateľa root.	**Umiestnenie** /etc/security/pscexpert/dodv2/loginout **Akcia na zabezpečenie súladu** Zabezpečuje, že systém bude spĺňať definované požiadavky.
GEN001100	1	Heslá užívateľa root nesmú byť nikdy odosielané v rámci siete v textovej podobe.	**Umiestnenie** /etc/security/pscexpert/dodv2/chuserstanzadod **Akcia na zabezpečenie súladu** Zabezpečuje, že systém bude spĺňať definované požiadavky.
GEN001120	2	Systém nesmie povoľovať prihlásenie užívateľa root cez protokol SSH.	**Umiestnenie** /etc/security/pscexpert/dodv2/sshDoDconfig **Akcia na zabezpečenie súladu** Zakáže prihlásenie užívateľa root cez SSH.
GEN001440	3	K všetkým interaktívnym užívateľom musí byť priradený domovský adresár v súbore /etc/passwd.	**Umiestnenie** /etc/security/pscexpert/dodv2/grpusrpass_chk **Akcia na zabezpečenie súladu** Zabezpečuje, že všetci interaktívni užívatelia budú mať určený adresár.

Tabuľka 2. Všeobecné požiadavky Ministerstva obrany USA (pokračovanie)

ID kontrolného bodu STIG Ministerstva obrany USA	Kategória pravidla STIG	Popis	Umiestnenie skriptu, v ktorom je definovaná akcia, a výsledky akcie zabezpečujúcej súlad
GEN001475	2	Súbor /etc/group nesmie obsahovať žiadne hodnoty hash skupinových hesiel.	**Umiestnenie** /etc/security/pscexpert/dodv2/passwdhash **Akcia na zabezpečenie súladu** Zabezpečuje, že v určenom súbore nebudú uložené žiadne hodnoty hash skupinových hesiel. **Poznámka:** Toto nastavenie nebude automaticky zmenené pri obnovení predvolenej politiky systému AIX prostredníctvom súboru DoDv2_to_ AIXDefault.xml. Toto nastavenie je potrebné manuálne zmeniť.
GEN001600	2	Cesty vyhľadávania spustiteľných súborov riadiacich skriptov spustenia môžu obsahovať iba absolútne cesty.	**Umiestnenie** /etc/security/pscexpert/dodv2/fixpathvars **Akcia na zabezpečenie súladu** Zabezpečuje, že systém bude spĺňať definované požiadavky. **Poznámka:** Toto nastavenie nebude automaticky zmenené pri obnovení predvolenej politiky systému AIX prostredníctvom súboru DoDv2_to_ AIXDefault.xml. Toto nastavenie je potrebné manuálne zmeniť.
GEN001605	2	Cesty vyhľadávania knižníc riadiacich skriptov spustenia môžu obsahovať iba absolútne cesty.	**Umiestnenie** /etc/security/pscexpert/dodv2/fixpathvars **Akcia na zabezpečenie súladu** Zabezpečuje, že systém bude spĺňať definované požiadavky. **Poznámka:** Toto nastavenie nebude automaticky zmenené pri obnovení predvolenej politiky systému AIX prostredníctvom súboru DoDv2_to_ AIXDefault.xml. Toto nastavenie je potrebné manuálne zmeniť.
GEN001610	2	Zoznamy vopred načítaných knižníc riadiacich skriptov spustenia môžu obsahovať iba absolútne cesty.	**Umiestnenie** /etc/security/pscexpert/dodv2/fixpathvars **Akcia na zabezpečenie súladu** Zabezpečuje, že systém bude spĺňať definované požiadavky. **Poznámka:** Toto nastavenie nebude automaticky zmenené pri obnovení predvolenej politiky systému AIX prostredníctvom súboru DoDv2_to_ AIXDefault.xml. Toto nastavenie je potrebné manuálne zmeniť.
GEN001840	2	Cesty vyhľadávania spustiteľných súborov všetkých globálnych inicializačných súborov môžu obsahovať iba absolútne cesty.	**Umiestnenie** /etc/security/pscexpert/dodv2/fixpathvars **Akcia na zabezpečenie súladu** Zabezpečuje, že systém bude spĺňať definované požiadavky. **Poznámka:** Toto nastavenie nebude automaticky zmenené pri obnovení predvolenej politiky systému AIX prostredníctvom súboru DoDv2_to_ AIXDefault.xml. Toto nastavenie je potrebné manuálne zmeniť.
GEN001845	2	Cesty vyhľadávania knižníc všetkých globálnych inicializačných súborov môžu obsahovať iba absolútne cesty.	**Umiestnenie** /etc/security/pscexpert/dodv2/fixpathvars **Akcia na zabezpečenie súladu** Zabezpečuje, že systém bude spĺňať definované požiadavky. **Poznámka:** Toto nastavenie nebude automaticky zmenené pri obnovení predvolenej politiky systému AIX prostredníctvom súboru DoDv2_to_ AIXDefault.xml. Toto nastavenie je potrebné manuálne zmeniť.

Tabuľka 2. Všeobecné požiadavky Ministerstva obrany USA (pokračovanie)

ID kontrolného bodu STIG Ministerstva obrany USA	Kategória pravidla STIG	Popis	Umiestnenie skriptu, v ktorom je definovaná akcia, a výsledky akcie zabezpečujúcej súlad
GEN001850	2	Zoznamy vopred načítaných knižníc všetkých globálnych inicializačných súborov môžu obsahovať iba absolútne cesty.	**Umiestnenie** /etc/security/pscexpert/dodv2/fixpathvars **Akcia na zabezpečenie súladu** Zabezpečuje, že systém bude spĺňať definované požiadavky. **Poznámka:** Toto nastavenie nebude automaticky zmenené pri obnovení predvolenej politiky systému AIX prostredníctvom súboru DoDv2_to_ AIXDefault.xml. Toto nastavenie je potrebné manuálne zmeniť.
GEN001900	2	Cesty vyhľadávania spustiteľných súborov všetkých lokálnych inicializačných súborov môžu obsahovať iba absolútne cesty.	**Umiestnenie** /etc/security/pscexpert/dodv2/fixpathvars **Akcia na zabezpečenie súladu** Zabezpečuje, že systém bude spĺňať definované požiadavky. **Poznámka:** Toto nastavenie nebude automaticky zmenené pri obnovení predvolenej politiky systému AIX prostredníctvom súboru DoDv2_to_ AIXDefault.xml. Toto nastavenie je potrebné manuálne zmeniť.
GEN001901	2	Cesty vyhľadávania knižníc všetkých lokálnych inicializačných súborov môžu obsahovať iba absolútne cesty.	**Umiestnenie** /etc/security/pscexpert/dodv2/fixpathvars **Akcia na zabezpečenie súladu** Zabezpečuje, že systém bude spĺňať definované požiadavky. **Poznámka:** Toto nastavenie nebude automaticky zmenené pri obnovení predvolenej politiky systému AIX prostredníctvom súboru DoDv2_to_ AIXDefault.xml. Toto nastavenie je potrebné manuálne zmeniť.
GEN001902	2	Zoznamy vopred načítaných knižníc všetkých lokálnych inicializačných súborov môžu obsahovať iba absolútne cesty.	**Umiestnenie** /etc/security/pscexpert/dodv2/fixpathvars **Akcia na zabezpečenie súladu** Zabezpečuje, že systém bude spĺňať definované požiadavky. **Poznámka:** Toto nastavenie nebude automaticky zmenené pri obnovení predvolenej politiky systému AIX prostredníctvom súboru DoDv2_to_ AIXDefault.xml. Toto nastavenie je potrebné manuálne zmeniť.
GEN001940	2	Užívateľské inicializačné súbory sa nesmú spúšťať v globálne zapisovateľných programoch.	**Umiestnenie** /etc/security/pscexpert/dodv2/rmwwpaths **Akcia na zabezpečenie súladu** Zabezpečuje, že systém bude spĺňať definované požiadavky.
GEN001980	2	Súbory .rhosts, .shosts, hosts.equiv, shosts.equiv, /etc/passwd, /etc/shadow a /etc/group nesmú obsahovať znamienko plus (+) bez definovania položiek v skupinách sietí NIS+.	**Umiestnenie** /etc/security/pscexpert/dodv2/dodv2netrules **Akcia na zabezpečenie súladu** Zabezpečuje, že určené súbory splňujú určené požiadavky.

Tabuľka 2. Všeobecné požiadavky Ministerstva obrany USA (pokračovanie)

ID kontrolného bodu STIG Ministerstva obrany USA	Kategória pravidla STIG	Popis	Umiestnenie skriptu, v ktorom je definovaná akcia, a výsledky akcie zabezpečujúcej súlad
GEN002000	2	V systéme sa nesmú nachádzať žiadne súbory .netrc.	**Umiestnenie** /etc/security/pscexpert/dodv2/dodv2netrules **Akcia na zabezpečenie súladu** Zabezpečuje, že v systéme sa nenachádzajú žiadne takéto súbory. **Poznámka:** Toto nastavenie nebude automaticky zmenené pri obnovení predvolenej politiky systému AIX prostredníctvom súboru DoDv2_to_ AIXDefault.xml. Toto nastavenie je potrebné manuálne zmeniť.
GEN002020	2	Všetky súbory .rhosts, .shosts a hosts.equiv môžu obsahovať iba dvojice dôveryhodných hostiteľov a užívateľov.	**Umiestnenie** /etc/security/pscexpert/dodv2/dodv2netrules **Akcia na zabezpečenie súladu** Zabezpečuje, že určené súbory spĺňajú túto požiadavku.
GEN002040	1	Toto pravidlo zakazuje súbory .rhosts, .shosts a hosts.equiv alebo súbory shosts.equiv.	**Umiestnenie** /etc/security/pscexpert/dodv2/mvhostsfilesdod **Akcia na zabezpečenie súladu** Zakáže určené súbory.
GEN002120	1,2	Toto pravidlo skontroluje a nakonfiguruje užívateľské prostredia shell.	**Umiestnenie** /etc/security/pscexpert/dodv2/usershells **Akcia na zabezpečenie súladu** Vytvorí vyžadované prostredia shell. **Poznámka:** Toto nastavenie nebude automaticky zmenené pri obnovení predvolenej politiky systému AIX prostredníctvom súboru DoDv2_to_ AIXDefault.xml. Toto nastavenie je potrebné manuálne zmeniť.
GEN002140	1,2	Všetky prostredia shell, na ktoré sa odkazuje zoznam v súbore /etc/passwd, musia byť uvedené v súbore /etc/shells, okrem prostredí shell, ktoré sú určené za účelom zabránenia v prihlásení.	**Umiestnenie** /etc/security/pscexpert/dodv2/usershells **Akcia na zabezpečenie súladu** Zabezpečuje, že všetky prostredia shell budú uvedené v správnych súboroch. **Poznámka:** Toto nastavenie nebude automaticky zmenené pri obnovení predvolenej politiky systému AIX prostredníctvom súboru DoDv2_to_ AIXDefault.xml. Toto nastavenie je potrebné manuálne zmeniť.
GEN002280	2	Súbory a adresáre zariadení musia byť zapisovateľné iba pre užívateľov so systémovým kontom alebo podľa konfigurácie systému dodávateľom.	**Umiestnenie** /etc/security/pscexpert/dodv2/wwdevfiles **Akcia na zabezpečenie súladu** Zobrazí globálne zapisovateľné súbory a adresáre a všetky ďalšie súbory v systéme, ktoré sa nachádzajú v neverejných adresároch.
GEN002300	2	Súbory zariadení, ktoré sa používajú na zálohovanie, musia byť čitateľné alebo zapisovateľné (alebo aj čitateľné, aj zapisovateľné) iba pre užívateľa root alebo záložného užívateľa.	**Umiestnenie** /etc/security/pscexpert/dodv2/wwdevfiles **Akcia na zabezpečenie súladu** Zobrazí globálne zapisovateľné súbory a adresáre a všetky ďalšie súbory v systéme, ktoré sa nachádzajú v neverejných adresároch.

Tabuľka 2. Všeobecné požiadavky Ministerstva obrany USA (pokračovanie)

ID kontrolného bodu STIG Ministerstva obrany USA	Kategória pravidla STIG	Popis	Umiestnenie skriptu, v ktorom je definovaná akcia, a výsledky akcie zabezpečujúcej súlad
GEN002400	2	Systém musí byť týždenne kontrolovaný, či neobsahuje neoprávnené súbory setuid alebo či nedošlo k neoprávnenej úprave oprávnených súborov setuid.	**Umiestnenie** /etc/security/pscexpert/dodv2/trust **Akcia na zabezpečenie súladu** Týždenne skontroluje, či nedošlo k zmenám v určených súboroch. **Poznámka:** Porovnajú sa dva najnovšie týždenné protokoly vytvorené v adresári /var/security/pscexpert s cieľom overiť, či nedošlo k neoprávnenej aktivite.
GEN002420	2	Vymeniteľné médiá, vzdialené súborové systémy a všetky súborové systémy, ktoré neobsahujú schválené súbory setuid, musia byť pripojené s použitím voľby *nosuid*.	**Umiestnenie** /etc/security/pscexpert/dodv2/fsmntoptions **Akcia na zabezpečenie súladu** Zabezpečuje, že pre vzdialene pripojené súborové systémy sú nastavené určené voľby. **Poznámka:** Toto nastavenie nebude automaticky zmenené pri obnovení predvolenej politiky systému AIX prostredníctvom súboru DoDv2_to_ AIXDefault.xml. Toto nastavenie je potrebné manuálne zmeniť.
GEN002430	2	Vymeniteľné médiá, vzdialené súborové systémy a všetky súborové systémy, ktoré neobsahujú schválené súbory zariadení, musia byť pripojené s použitím voľby *nodev*.	**Umiestnenie** /etc/security/pscexpert/dodv2/fsmntoptions **Akcia na zabezpečenie súladu** Zabezpečuje, že pre vzdialene pripojené súborové systémy sú nastavené určené voľby. **Poznámka:** Toto nastavenie nebude automaticky zmenené pri obnovení predvolenej politiky systému AIX prostredníctvom súboru DoDv2_to_ AIXDefault.xml. Toto nastavenie je potrebné manuálne zmeniť.
GEN002480	2	Verejné adresáre musia byť jediné globálne zapisovateľné adresáre a globálne zapisovateľné súbory sa môžu nachádzať iba vo verejných adresároch.	**Umiestnenie** /etc/security/pscexpert/dodv2/wwdevfiles /etc/security/pscexpert/dodv2/fpmdodfiles **Akcia na zabezpečenie súladu** Nahlási, keď globálne zapisovateľné súbory sa nenachádzajú vo verejných adresároch.
GEN002640	2	Predvolené systémové kontá musia byť zakázané alebo odstránené.	**Umiestnenie** /etc/security/pscexpert/dodv2/lockacc_rlogin /etc/security/pscexpert/dodv2/loginout **Akcia na zabezpečenie súladu** Zakáže predvolené systémové kontá.
GEN002660	2	Auditovanie musí byť povolené.	**Umiestnenie** /etc/security/pscexpert/dodv2/dodaudit **Akcia na zabezpečenie súladu** Povolí príkaz dodaudit povoľujúci auditovanie.
GEN002720	2	Systém auditovania musí byť nakonfigurovaný tak, by auditoval neúspešné pokusy o prístup k súborom a programom.	**Umiestnenie** /etc/security/pscexpert/dodv2/dodaudit **Akcia na zabezpečenie súladu** Automaticky povolí určené auditovanie.

Tabuľka 2. Všeobecné požiadavky Ministerstva obrany USA (pokračovanie)

ID kontrolného bodu STIG Ministerstva obrany USA	Kategória pravidla STIG	Popis	Umiestnenie skriptu, v ktorom je definovaná akcia, a výsledky akcie zabezpečujúcej súlad
GEN002740	2	Systém auditovania musí byť nakonfigurovaný tak, by auditoval odstránenia súborov.	**Umiestnenie** /etc/security/pscexpert/dodv2/dodaudit **Akcia na zabezpečenie súladu** Automaticky povolí určené auditovanie.
GEN002750	3	Systém auditovania musí byť nakonfigurovaný tak, by auditoval vytvorenie kont.	**Umiestnenie** /etc/security/pscexpert/dodv2/dodaudit **Akcia na zabezpečenie súladu** Automaticky povolí určené auditovanie.
GEN002751	3	Systém auditovania musí byť nakonfigurovaný tak, by auditoval úpravu kont.	**Umiestnenie** /etc/security/pscexpert/dodv2/dodaudit **Akcia na zabezpečenie súladu** Automaticky povolí určené auditovanie.
GEN002752	3	Systém auditovania musí byť nakonfigurovaný tak, by auditoval zakázané kontá.	**Umiestnenie** /etc/security/pscexpert/dodv2/dodaudit **Akcia na zabezpečenie súladu** Automaticky povolí určené auditovanie.
GEN002753	3	Systém auditovania musí byť nakonfigurovaný tak, by auditoval ukončenie kont.	**Umiestnenie** /etc/security/pscexpert/dodv2/dodaudit **Akcia na zabezpečenie súladu** Automaticky povolí určené auditovanie.
GEN002760	2	Systém auditovania musí byť nakonfigurovaný tak, by auditoval všetky administračné, privilegované alebo bezpečnostné úkony.	**Umiestnenie** /etc/security/pscexpert/dodv2/dodaudit **Akcia na zabezpečenie súladu** Automaticky povolí určené auditovanie.
GEN002800	2	Systém auditovania musí byť nakonfigurovaný tak, by auditoval prihlásenie, odhlásenie a spustenie relácie.	**Umiestnenie** /etc/security/pscexpert/dodv2/dodaudit **Akcia na zabezpečenie súladu** Automaticky povolí určené auditovanie.
GEN002820	2	Systém auditovania musí byť nakonfigurovaný tak, by auditoval všetky jednotlivé zmeny oprávnení v riadení prístupu.	**Umiestnenie** /etc/security/pscexpert/dodv2/dodaudit **Akcia na zabezpečenie súladu** Automaticky povolí určené auditovanie.
GEN002825	2	Systém auditovania musí byť nakonfigurovaný tak, by auditoval načítanie a uvoľnenie dynamických modulov jadra.	**Umiestnenie** /etc/security/pscexpert/dodv2/dodaudit **Akcia na zabezpečenie súladu** Automaticky povolí určené auditovanie.
GEN002860	2	Protokoly z auditu musia byť denne rotované.	**Umiestnenie** /etc/security/pscexpert/dodv2/rotateauditdod **Akcia na zabezpečenie súladu** Zabezpečuje rotáciu protokolov z auditu.

Tabuľka 2. Všeobecné požiadavky Ministerstva obrany USA (pokračovanie)

ID kontrolného bodu STIG Ministerstva obrany USA	Kategória pravidla STIG	Popis	Umiestnenie skriptu, v ktorom je definovaná akcia, a výsledky akcie zabezpečujúcej súlad
GEN002960	2	Prístup k pomocnému programu cron musí byť riadený prostredníctvom súboru cron.allow alebo cron.deny alebo oboch týchto súborov.	**Umiestnenie** /etc/security/pscexpert/dodv2/limitsysacc **Akcia na zabezpečenie súladu** Zabezpečuje, že budú povolené príslušné obmedzenia.
GEN003000 (súvisí s GEN000960, GEN003020, GEN003160, GEN003360 a GEN003380)	2	Program cron nesmie spúšťať skupinovo alebo globálne zapisovateľné programy.	**Umiestnenie** /etc/security/pscexpert/dodv2/rmwwpaths **Akcia na zabezpečenie súladu** Zabezpečuje, že budú povolené príslušné obmedzenia. **Poznámka:** Toto nastavenie nebude automaticky zmenené pri obnovení predvolenej politiky systému AIX prostredníctvom súboru DoDv2_to_ AIXDefault.xml. Toto nastavenie je potrebné manuálne zmeniť.
GEN003020 (súvisí s GEN000960, GEN003000, GEN003160, GEN003360 a GEN003380)	2	Program cron nesmie spúšťať programy v globálne zapisovateľných adresároch alebo pod nimi.	**Umiestnenie** /etc/security/pscexpert/dodv2/rmwwpaths **Akcia na zabezpečenie súladu** Odstráni oprávnenie na globálny zápis s adresárov programu cron. **Poznámka:** Toto nastavenie nebude automaticky zmenené pri obnovení predvolenej politiky systému AIX prostredníctvom súboru DoDv2_to_ AIXDefault.xml. Toto nastavenie je potrebné manuálne zmeniť.
GEN003060	2	Predvolené systémové kontá (okrem konta užívateľa root) nesmú byť uvedené v súbore cron.allow alebo musia byť uvedené v súbore cron.deny, ak súbor cron.allow neexistuje.	**Umiestnenie** cron.allow alebo cron.deny **Akcia na zabezpečenie súladu** Zabezpečuje, že systém bude spĺňať definované požiadavky.
GEN003160 (súvisí s GEN000960, GEN003000, GEN003020, GEN003360 a GEN003380)	2	Musí byť spustené protokolovanie pre program cron.	**Umiestnenie** /etc/security/pscexpert/dodv2/rmwwpaths **Akcia na zabezpečenie súladu** Zabezpečuje, že systém bude spĺňať definované požiadavky.
GEN003280	2	Prístup k pomocnému programu at musí byť riadený prostredníctvom súborov at.allow a at.deny.	**Umiestnenie** /etc/security/pscexpert/dodv2/chcronfilesdod **Akcia na zabezpečenie súladu** Zabezpečuje, že systém bude spĺňať definované požiadavky.
GEN003300	2	Súbor at.deny nesmie byť prázdny, ak existuje.	**Umiestnenie** /etc/security/pscexpert/dodv2/chcronfilesdod **Akcia na zabezpečenie súladu** Zabezpečuje, že systém bude spĺňať definované požiadavky.
GEN003320	2	Predvolené systémové kontá (okrem konta užívateľa root) nesmú byť uvedené v súbore at.allow alebo musia byť uvedené v súbore at.deny, ak súbor at.allow neexistuje.	**Umiestnenie** /etc/security/pscexpert/dodv2/chcronfilesdod **Akcia na zabezpečenie súladu** Zabezpečuje, že systém bude spĺňať definované požiadavky.

Tabuľka 2. Všeobecné požiadavky Ministerstva obrany USA (pokračovanie)

ID kontrolného bodu STIG Ministerstva obrany USA	Kategória pravidla STIG	Popis	Umiestnenie skriptu, v ktorom je definovaná akcia, a výsledky akcie zabezpečujúcej súlad
GEN003360 (súvisí s GEN000960, GEN003000, GEN003020, GEN003160 a GEN003380)	2	Démon at nesmie spúšťať skupinovo alebo globálne zapisovateľné programy.	**Umiestnenie** /etc/security/pscexpert/dodv2/rmwwpaths **Akcia na zabezpečenie súladu** Zabezpečuje, že systém bude spĺňať definované požiadavky. **Poznámka:** Toto nastavenie nebude automaticky zmenené pri obnovení predvolenej politiky systému AIX prostredníctvom súboru DoDv2_to_ AIXDefault.xml. Toto nastavenie je potrebné manuálne zmeniť.
GEN003380 (súvisí s GEN000960, GEN003000, GEN003020, GEN003160 a GEN003360)	2	Démon at nesmie spúšťať programy v globálne zapisovateľných adresároch alebo pod nimi.	**Umiestnenie** /etc/security/pscexpert/dodv2/rmwwpaths **Akcia na zabezpečenie súladu** Zabezpečuje, že systém bude spĺňať definované požiadavky. **Poznámka:** Toto nastavenie nebude automaticky zmenené pri obnovení predvolenej politiky systému AIX prostredníctvom súboru DoDv2_to_ AIXDefault.xml. Toto nastavenie je potrebné manuálne zmeniť.
GEN003510	2	Výpisy pamäte jadra musia byť zakázané, pokiaľ nie sú potrebné.	**Umiestnenie** /etc/security/pscexpert/dodv2/coredumpdev **Akcia na zabezpečenie súladu** Zakáže výpisy pamäte jadra.
GEN003540	2	Systém musí používať nespustiteľné zásobníky programov.	**Umiestnenie** /etc/security/pscexpert/dodv2/sedconfigdod **Akcia na zabezpečenie súladu** Vynucuje používanie nespustiteľných zásobníkov programov.
GEN003600	2	Systém nesmie preposielať pakety IPv4 smerované zo zdroja.	**Umiestnenie** /etc/security/pscexpert/dodv2/ntwkoptsdod **Akcia na zabezpečenie súladu** Nastavuje hodnotu voľby siete ipsrcforward na *0*.
GEN003601	2	Veľkosti rezervných frontov TCP musia byť nastavené správne.	**Umiestnenie** /etc/security/pscexpert/dodv2/ntwkoptsdod **Akcia na zabezpečenie súladu** Nastaví hodnotu voľby siete clean_partial_ conns na *1*.
GEN003603	2	Systém nesmie reagovať na správy echo odoslané na adresu vysielania cez protokol ICMPv4 (Internet Control Message Protocol verzie 4).	**Umiestnenie** /etc/security/pscexpert/dodv2/ntwkoptsdod **Akcia na zabezpečenie súladu** Nastaví hodnotu voľby siete bcastping na *0*.
GEN003604	2	Systém nesmie reagovať na požiadavky na časovú značku ICMP odoslané na adresu vysielania.	**Umiestnenie** /etc/security/pscexpert/dodv2/ntwkoptsdod **Akcia na zabezpečenie súladu** Nastaví hodnotu voľby siete bcastping na *0*.
GEN003605	2	Systém nesmie použiť rezervované smerovanie zo zdroja pri odpovediach cez TCP.	**Umiestnenie** /etc/security/pscexpert/dodv2/ntwkoptsdod **Akcia na zabezpečenie súladu** Nastaví hodnotu voľby siete nonlocsrcroute na *0*.

Tabuľka 2. Všeobecné požiadavky Ministerstva obrany USA (pokračovanie)

ID kontrolného bodu STIG Ministerstva obrany USA	Kategória pravidla STIG	Popis	Umiestnenie skriptu, v ktorom je definovaná akcia, a výsledky akcie zabezpečujúcej súlad
GEN003606	2	Systém nesmie dovoliť lokálnym aplikáciám generovať pakety smerované zo zdroja.	**Umiestnenie** /etc/security/pscexpert/dodv2/ntwkoptsdod **Akcia na zabezpečenie súladu** Nastaví hodnotu voľby siete ipsrcroutesend na *0*.
GEN003607	2	Systém nesmie akceptovať pakety IPv4 smerované zo zdroja.	**Umiestnenie** /etc/security/pscexpert/dodv2/ntwkoptsdod **Akcia na zabezpečenie súladu** Zakáže schopnosť akceptovať pakety IPv4 smerované zo zdroja.
GEN003609	2	Systé musí ignorovať správy o presmerovaní IPv4 ICMP.	**Umiestnenie** /etc/security/pscexpert/dodv2/ntwkoptsdod **Akcia na zabezpečenie súladu** Nastaví hodnotu voľby siete ipignoreredirects na *1*.
GEN003610	2	Systém nesmie posielať správy o presmerovaní IPv4 ICMP.	**Umiestnenie** /etc/security/pscexpert/dodv2/ntwkoptsdod **Akcia na zabezpečenie súladu** Nastaví hodnotu voľby siete ipsendredirects na *0*.
GEN003612	2	Systém musí byť nakonfigurovaný tak, aby používal objekty TCP syncookie pri zaplavení TCP SYN.	**Umiestnenie** /etc/security/pscexpert/dodv2/ntwkoptsdod **Akcia na zabezpečenie súladu** Nastaví hodnotu voľby siete clean_partial _conns na *1*.
GEN003640	2	Koreňový súborový systém musí používať žurnálovanie alebo iný spôsob na zabezpečenie konzistentnosti súborového systému.	**Umiestnenie** /etc/security/pscexpert/dodv2/chkjournal **Akcia na zabezpečenie súladu** Povolí žurnálovanie pre koreňový súborový systém.
GEN003660	2	Systém musí zaznamenávať údaje autentifikačných údajov do protokolu.	**Umiestnenie** /etc/security/pscexpert/dodv2/chsyslogdod **Akcia na zabezpečenie súladu** Povolí zaznamenávanie údajov auth a info do protokolu.
GEN003700	2	Služby inetd a xinetd musia byť zakázané alebo odstránené, ak ich nepoužívajú žiadne sieťové služby.	**Umiestnenie** /etc/security/pscexpert/dodv2/dodv2services **Akcia na zabezpečenie súladu** Zabezpečuje, že systém bude spĺňať definované požiadavky.
GEN003810	2	Služby portmap a rpcbind nesmú byť spustené, pokiaľ nie sú potrebné.	**Umiestnenie** /etc/security/pscexpert/dodv2/dodv2services **Akcia na zabezpečenie súladu** Zabezpečuje, že systém bude spĺňať definované požiadavky.
GEN003815	2	Služby portmap a rpcbind nesmú byť nainštalované, pokiaľ nie sú používané.	**Umiestnenie** /etc/security/pscexpert/dodv2/dodv2services **Akcia na zabezpečenie súladu** Zabezpečuje, že systém bude spĺňať definované požiadavky.

Tabuľka 2. Všeobecné požiadavky Ministerstva obrany USA (pokračovanie)

ID kontrolného bodu STIG Ministerstva obrany USA	Kategória pravidla STIG	Popis	Umiestnenie skriptu, v ktorom je definovaná akcia, a výsledky akcie zabezpečujúcej súlad
GEN003820-3860	1,2,3	Démoni rsh, rexexec a telnet a služba rlogind nesmú bežať.	**Umiestnenie** /etc/security/pscexpert/dodv2/inetdservices **Akcia na zabezpečenie súladu** Zakáže vyžadovaných démonov a služby označením položiek v súbore /etc/inetd.conf znakom komentára.
GEN003865	2	Nesmú byť nainštalované nástroje na analýzu siete.	**Umiestnenie** /etc/security/pscexpert/dodv2/dodv2services **Akcia na zabezpečenie súladu** Zabezpečuje, že systém bude spĺňať definované požiadavky.
GEN003900	2	Súbor hosts.lpd (alebo ekvivalentný) nesmie obsahovať znamienko plus (+).	**Umiestnenie** /etc/security/pscexpert/dodv2/printers **Akcia na zabezpečenie súladu** Zabezpečuje, že systém bude spĺňať definované požiadavky.
GEN004220	1	Z administračných kont sa nesmie otvárať webový prehliadač, pokiaľ nie je potrebný na správu lokálnych služieb.	**Umiestnenie** /etc/security/pscexpert/dodv2/dodv2cat1 **Akcia na zabezpečenie súladu** Zobrazí výsledky určených testov pravidiel.
GEN004460	2	Toto pravidlo zaznamenáva údaje auth a info do protokolu.	**Umiestnenie** /etc/security/pscexpert/dodv2/chsyslogdod **Akcia na zabezpečenie súladu** Povolí zaznamenávanie údajov auth a info do protokolu.
GEN004540	2	Toto pravidlo zakáže pomoc k príkazu sendmail.	**Umiestnenie** /etc/security/pscexpert/dodv2/sendmailhelp /etc/security/pscexpert/dodv2/dodv2cmntrows **Akcia na zabezpečenie súladu** Zakáže určený príkaz.
GEN004580	2	Systém nesmie používať súbory .forward.	**Umiestnenie** /etc/security/pscexpert/dodv2/forward **Akcia na zabezpečenie súladu** Zakáže určené súbory. **Poznámka:** Toto nastavenie nebude automaticky zmenené pri obnovení predvolenej politiky systému AIX prostredníctvom súboru DoDv2_to_ AIXDefault.xml. Toto nastavenie je potrebné manuálne zmeniť.
GEN004600	1	Služba SMTP musí mať najnovšiu verziu.	**Umiestnenie** /etc/security/pscexpert/dodv2/SMTP_ver **Akcia na zabezpečenie súladu** Zabezpečuje, že bude spustená najnovšia verzia určenej služby. **Poznámka:** Toto nastavenie nebude automaticky zmenené pri obnovení predvolenej politiky systému AIX prostredníctvom súboru DoDv2_to_ AIXDefault.xml. Toto nastavenie je potrebné manuálne zmeniť.

Tabuľka 2. Všeobecné požiadavky Ministerstva obrany USA (pokračovanie)

ID kontrolného bodu STIG Ministerstva obrany USA	Kategória pravidla STIG	Popis	Umiestnenie skriptu, v ktorom je definovaná akcia, a výsledky akcie zabezpečujúcej súlad
GEN004620	2	Funkcia ladenia servera sendmail musí byť zakázaná.	**Umiestnenie** /etc/security/pscexpert/dodv2/SMTP_ver **Akcia na zabezpečenie súladu** Zakáže funkciu ladenia programu sendmail.
GEN004640	1	Služba SMTP nesmie mať aktívny alias uudecode.	**Umiestnenie** /etc/security/pscexpert/dodv2/SMTPuucode **Akcia na zabezpečenie súladu** Zakáže alias uudecode.
GEN004710	2	Odosielanie e-mailov z cudzej adresy musí byť zakázané.	**Umiestnenie** /etc/security/pscexpert/dodv2/sendmaildod **Akcia na zabezpečenie súladu** Zakáže odosielanie e-mailov z cudzej adresy.
GEN004800	1,2,3	V systéme sa nesmie používať nešifrovaný prenos FTP.	**Umiestnenie** /etc/security/pscexpert/dodv2/inetdservices **Akcia na zabezpečenie súladu** Zakáže vyžadovaných démonov a služby označením položiek v súbore /etc/inetd.conf znakom komentára.
GEN004820	2	Anonymné pripojenia cez FTP nesmú byť aktívne v systéme, pokiaľ nie sú autorizované.	**Umiestnenie** /etc/security/pscexpert/dodv2/anonuser **Akcia na zabezpečenie súladu** Zakáže anonymné pripojenia FTP v systéme. **Poznámka:** Toto nastavenie nebude automaticky zmenené pri obnovení predvolenej politiky systému AIX prostredníctvom súboru DoDv2_to_ AIXDefault.xml. Toto nastavenie je potrebné manuálne zmeniť.
GEN004840	2	Ak systém je anonymný server FTP, musí byť izolovaný v sieti demilitarizovanej zóny (DMZ).	**Umiestnenie** /etc/security/pscexpert/dodv2/anonuser **Akcia na zabezpečenie súladu** Zabezpečí, že anonymné pripojenia FTP v systéme budú v sieti DMZ.
GEN004880	2	Musí existovať súbor ftpusers.	**Umiestnenie** /etc/security/pscexpert/dodv2/chdodftpusers **Akcia na zabezpečenie súladu** Zabezpečí, že určený súbor bude existovať v systéme.
GEN004900	2	Súbor ftpusers musí obsahovať názvy kont, ktoré nemôžu používať protokol FTP.	**Umiestnenie** /etc/security/pscexpert/dodv2/chdodftpusers **Akcia na zabezpečenie súladu** Zabezpečuje, že súbor bude obsahovať vyžadované názvy kont.

Tabuľka 2. Všeobecné požiadavky Ministerstva obrany USA (pokračovanie)

ID kontrolného bodu STIG Ministerstva obrany USA	Kategória pravidla STIG	Popis	Umiestnenie skriptu, v ktorom je definovaná akcia, a výsledky akcie zabezpečujúcej súlad
GEN005000	1	Anonymné kontá FTP nesmú mať funkčné prostredie shell.	**Umiestnenie** /etc/security/pscexpert/dodv2/usershells **Akcia na zabezpečenie súladu** Odstráni prostredia shell z anonymných kont FTP. **Poznámka:** Toto nastavenie nebude automaticky zmenené pri obnovení predvolenej politiky systému AIX prostredníctvom súboru DoDv2_to_ AIXDefault.xml. Toto nastavenie je potrebné manuálne zmeniť.
GEN005080	1	Démon TFTP musí fungovať v bezpečnom režime, ktorý umožňuje prístup iba k jednému adresáru v hostiteľskom súborovom systéme.	**Umiestnenie** /etc/security/pscexpert/dodv2/tftpdod **Akcia na zabezpečenie súladu** Zabezpečuje, že démon bude spĺňať určené požiadavky.
GEN005120	2	Démon TFTP musí byť nakonfigurovaný v súlade so špecifikáciami dodávateľa vrátane vyhradeného užívateľského konta TFTP, neprihlasovacieho prostredia shell, ako je napríklad /bin/false, a domovského adresára vlastneného užívateľom TFTP.	**Umiestnenie** /etc/security/pscexpert/dodv2/tftpdod **Akcia na zabezpečenie súladu** Zabezpečuje, že systém bude spĺňať definované požiadavky.
GEN005140	1,2,3	Každý aktívny démon TFTP musí byť autorizovaný a schválený v akreditačnom balíku systému.	**Umiestnenie** /etc/security/pscexpert/dodv2/inetdservices **Akcia na zabezpečenie súladu** Zabezpečuje, že démon bude autorizovaný.
GEN005160	1,2	Každý hostiteľ servera X Window System musí zapisovať súbory .Xauthority.	**Umiestnenie** /etc/security/pscexpert/dodv2/dodv2disableX **Akcia na zabezpečenie súladu** Zabezpečuje, že hostiteľ bude zapisovať určené súbory.
GEN005200	1,2	Žiadne zobrazenia servera X Window System nesmú byť verejne exportované.	**Umiestnenie** /etc/security/pscexpert/dodv2/dodv2disableX **Akcia na zabezpečenie súladu** Zakáže propagáciu určených programov.
GEN005220	1,2	Musia sa používať súbory .Xauthority alebo X*.hosts (alebo ekvivalentné) na obmedzenie prístupu k serveru X Window System.	**Umiestnenie** /etc/security/pscexpert/dodv2/dodv2disableX **Akcia na zabezpečenie súladu** Zabezpečuje, že určené súbory budú k dispozícii na obmedzenie prístupu k serveru.
GEN005240	1,2	Pomocný program .Xauthority musí umožňovať prístup iba k oprávneným hostiteľom.	**Umiestnenie** /etc/security/pscexpert/dodv2/dodv2disableX **Akcia na zabezpečenie súladu** Zabezpečuje, že prístup bude obmedzený iba na oprávnených hostiteľov.

Tabuľka 2. Všeobecné požiadavky Ministerstva obrany USA (pokračovanie)

ID kontrolného bodu STIG Ministerstva obrany USA	Kategória pravidla STIG	Popis	Umiestnenie skriptu, v ktorom je definovaná akcia, a výsledky akcie zabezpečujúcej súlad
GEN005260	2	Toto pravidlo zakáže pripojenia k serveru X Window System a správcu prihlásenia XServer.	**Umiestnenie** /etc/security/pscexpert/dodv2/dodv2cmntrows **Akcia na zabezpečenie súladu** Zakáže vyžadované pripojenia a manažéra prihlásenia.
GEN005280	1,2,3	V systéme nesmie byť aktívna služba UUCP.	**Umiestnenie** /etc/security/pscexpert/dodv2/inetdservices **Akcia na zabezpečenie súladu** Zakáže vyžadovaných démonov a služby označením položiek v súbore /etc/inetd.conf znakom komentára.
GEN005300	2	Musia byť nastavené iné ako predvolené nastavenia komunít SNMP.	**Umiestnenie** /etc/security/pscexpert/dodv2/chsnmp **Akcia na zabezpečenie súladu** Zabezpečuje, že systém bude spĺňať definované požiadavky.
GEN005305	2	Služba SNMP môže mať iba verziu SNMPv3 alebo novšiu.	**Umiestnenie** /etc/security/pscexpert/dodv2/chsnmp **Akcia na zabezpečenie súladu** Zabezpečuje, že systém bude spĺňať definované požiadavky.
GEN005306	2	Služba SNMP musí vyžadovať použitie FIPS 140-2.	**Umiestnenie** /etc/security/pscexpert/dodv2/chsnmp **Akcia na zabezpečenie súladu** Zabezpečuje, že systém bude spĺňať definované požiadavky.
GEN005440	2	Systém musí používať vzdialený server syslog (hostiteľ protokolov).	**Umiestnenie** /etc/security/pscexpert/dodv2/EnableTrustedLogging **Akcia na zabezpečenie súladu** Zabezpečuje, že systém bude používať vzdialený server syslog.
GEN005450	2	Systém musí používať vzdialený server syslog (hostiteľ protokolov).	**Umiestnenie** /etc/security/pscexpert/dodv2/ EnableTrustedLogging **Akcia na zabezpečenie súladu** Zabezpečuje, že systém bude používať vzdialený server syslog.
GEN005460	2	Systém musí používať vzdialený server syslog (hostiteľ protokolov).	**Umiestnenie** /etc/security/pscexpert/dodv2/ EnableTrustedLogging **Akcia na zabezpečenie súladu** Zabezpečuje, že systém bude používať vzdialený server syslog.
GEN005480	2	Systém musí používať vzdialený server syslog (hostiteľ protokolov).	**Umiestnenie** /etc/security/pscexpert/dodv2/EnableTrustedLogging **Akcia na zabezpečenie súladu** Zabezpečuje, že systém bude používať vzdialený server syslog.
GEN005500	2	Démon SSH musí byť nakonfigurovaný tak, aby používal iba protokol Secure Shell verzie 2 (SSHv2).	**Umiestnenie** /etc/security/pscexpert/dodv2/sshDoDconfig **Akcia na zabezpečenie súladu** Zabezpečuje, že systém bude spĺňať definované požiadavky.

Tabuľka 2. Všeobecné požiadavky Ministerstva obrany USA (pokračovanie)

ID kontrolného bodu STIG Ministerstva obrany USA	Kategória pravidla STIG	Popis	Umiestnenie skriptu, v ktorom je definovaná akcia, a výsledky akcie zabezpečujúcej súlad
GEN005501	2	Klient SSH musí byť nakonfigurovaný tak, aby používal iba protokol SSHv2.	**Umiestnenie** /etc/security/pscexpert/dodv2/sshDoDconfig **Akcia na zabezpečenie súladu** Zabezpečuje, že systém bude spĺňať definované požiadavky.
GEN005504	2	Démon SSH môže načúvať iba na sieťových adresách riadenia, pokiaľ nie je autorizovaný pre iné použitia ako riadenie.	**Umiestnenie** /etc/security/pscexpert/dodv2/sshDoDconfig **Akcia na zabezpečenie súladu** Zabezpečuje, že systém bude spĺňať definované požiadavky.
GEN005505	2	Démon SSH musí byť nakonfigurovaný tak, aby používal iba šifry vyhovujúce štandardom FIPS (Federal Information Processing Standards) 140-2.	**Umiestnenie** /etc/security/pscexpert/dodv2/sshDoDconfig **Akcia na zabezpečenie súladu** Zabezpečuje, že systém bude spĺňať definované požiadavky.
GEN005506	2	Démon SSH musí byť nakonfigurovaný tak, aby používal iba šifry vyhovujúce štandardom FIPS 140-2.	**Umiestnenie** /etc/security/pscexpert/dodv2/sshDoDconfig **Akcia na zabezpečenie súladu** Zabezpečuje, že systém bude spĺňať definované požiadavky.
GEN005507	2	Démon SSH musí byť nakonfigurovaný tak, aby používal kódy MAC (Message Authentication Code) s kryptografickými hashovacími algoritmami v súlade so štandardmi FIPS 140-2.	**Umiestnenie** /etc/security/pscexpert/dodv2/sshDoDconfig **Akcia na zabezpečenie súladu** Zabezpečuje, že systém bude spĺňať definované požiadavky.
GEN005510	2	Klient SSH musí byť nakonfigurovaný tak, aby používal iba kódy MAC so šiframi vyhovujúcimi štandardom FIPS 140-2.	**Umiestnenie** /etc/security/pscexpert/dodv2/sshDoDconfig **Akcia na zabezpečenie súladu** Zabezpečuje, že systém bude spĺňať definované požiadavky.
GEN005511	2	Klient SSH musí byť nakonfigurovaný tak, aby používal iba kódy MAC so šiframi vyhovujúcimi štandardom FIPS 140-2.	**Umiestnenie** /etc/security/pscexpert/dodv2/sshDoDconfig **Akcia na zabezpečenie súladu** Zabezpečuje, že systém bude spĺňať definované požiadavky.
GEN005512	2	Démon SSH musí byť nakonfigurovaný tak, aby používal kódy MAC s kryptografickými hashovacími algoritmami v súlade so štandardmi FIPS 140-2.	**Umiestnenie** /etc/security/pscexpert/dodv2/sshDoDconfig **Akcia na zabezpečenie súladu** Zabezpečuje, že systém bude spĺňať definované požiadavky.
GEN005521	2	Démon SSH musí povoľovať prihlásenie iba pre konkrétnych užívateľov alebo skupiny.	**Umiestnenie** /etc/security/pscexpert/dodv2/sshDoDconfig **Akcia na zabezpečenie súladu** Zabezpečuje, že systém bude spĺňať definované požiadavky.

Tabuľka 2. Všeobecné požiadavky Ministerstva obrany USA (pokračovanie)

ID kontrolného bodu STIG Ministerstva obrany USA	Kategória pravidla STIG	Popis	Umiestnenie skriptu, v ktorom je definovaná akcia, a výsledky akcie zabezpečujúcej súlad
GEN005536	2	Démon SSH musí vykonávať prísnu kontrolu režimu pre konfiguračné súbory v domovskom adresári.	**Umiestnenie** /etc/security/pscexpert/dodv2/sshDoDconfig **Akcia na zabezpečenie súladu** Zabezpečuje, že systém bude spĺňať definované požiadavky.
GEN005537	2	Démon SSH musí používať oddeľovanie privilégií.	**Umiestnenie** /etc/security/pscexpert/dodv2/sshDoDconfig **Akcia na zabezpečenie súladu** Zabezpečuje, že systém bude spĺňať definované požiadavky.
GEN005538	2	Démon SSH nesmie povoľovať autentifikáciu cez rhosts prostredníctvom kryptografického systému RSA (Rivest-Shamir-Adleman).	**Umiestnenie** /etc/security/pscexpert/dodv2/sshDoDconfig **Akcia na zabezpečenie súladu** Zabezpečuje, že systém bude spĺňať definované požiadavky.
GEN005539	2	Démon SSH nesmie povoľovať kompresiu alebo môže povoľovať kompresiu až po úspešnej autentifikácii.	**Umiestnenie** /etc/security/pscexpert/dodv2/sshDoDconfig **Akcia na zabezpečenie súladu** Zabezpečuje, že systém bude spĺňať definované požiadavky.
GEN005550	2	Démon SSH musí byť nakonfigurovaný s prihlasovacím pruhom Ministerstva obrany USA.	**Umiestnenie** /etc/security/pscexpert/dodv2/sshDoDconfig **Akcia na zabezpečenie súladu** Zabezpečuje, že systém bude spĺňať definované požiadavky.
GEN005560	2	Zistiť, či existuje predvolená brána, ktorá by bola nakonfigurovaná pre IPv4.	**Umiestnenie** /etc/security/pscexpert/dodv2/chkgtway **Akcia na zabezpečenie súladu** Zabezpečuje, že systém bude spĺňať definované požiadavky. **Poznámka:** Toto nastavenie nebude automaticky zmenené pri obnovení predvolenej politiky systému AIX prostredníctvom súboru DoDv2_to_ AIXDefault.xml. Toto nastavenie je potrebné manuálne zmeniť. **Poznámka:** Ak sa vo vašom systéme používa protokol IPv6, uistite sa, že nastavenie *ipv6_enabled* v súbore /etc/security/pscexpert/ipv6.conf má hodnotu yes. Ak sa v systéme nepoužíva protokol IPv6, uistite sa, že má nastavenie *ipv6_enabled* hodnotu no.
GEN005570	2	Zistiť, či existuje predvolená brána, ktorá by bola nakonfigurovaná pre IPv6.	**Umiestnenie** /etc/security/pscexpert/dodv2/chkgtway **Akcia na zabezpečenie súladu** Zabezpečuje, že systém bude spĺňať definované požiadavky. **Poznámka:** Toto nastavenie nebude automaticky zmenené pri obnovení predvolenej politiky systému AIX prostredníctvom súboru DoDv2_to_ AIXDefault.xml. Toto nastavenie je potrebné manuálne zmeniť. **Poznámka:** Ak sa vo vašom systéme používa protokol IPv6, uistite sa, že nastavenie *ipv6_enabled* v súbore /etc/security/pscexpert/ipv6.conf má hodnotu yes. Ak sa v systéme nepoužíva protokol IPv6, uistite sa, že má nastavenie *ipv6_enabled* hodnotu no.

Tabuľka 2. Všeobecné požiadavky Ministerstva obrany USA (pokračovanie)

ID kontrolného bodu STIG Ministerstva obrany USA	Kategória pravidla STIG	Popis	Umiestnenie skriptu, v ktorom je definovaná akcia, a výsledky akcie zabezpečujúcej súlad
GEN005590	2	V systéme nesmú byť spustené žiadne služby smerovania protokolov, pokiaľ systém neslúži ako smerovač.	**Umiestnenie** /etc/security/pscexpert/dodv2/dodv2cmntrows **Akcia na zabezpečenie súladu** Zabezpečuje, že systém bude spĺňať definované požiadavky.
GEN005590	2	V systéme nesmú byť spustené žiadne služby smerovania protokolov, pokiaľ systém neslúži ako smerovač.	**Umiestnenie** /etc/security/pscexpert/dodv2/dodv2cmntrows **Akcia na zabezpečenie súladu** Zabezpečuje, že systém bude spĺňať definované požiadavky.
GEN005600	2	Nesmie byť povolené preposielanie IP paketov pre IPv4, pokiaľ systém neslúži ako smerovač.	**Umiestnenie** /etc/security/pscexpert/dodv2/ntwkoptsdod **Akcia na zabezpečenie súladu** Nastaví hodnotu voľby siete ipforwarding na *0*.
GEN005610	2	V systéme nesmie byť povolené preposielanie IP paketov pre IPv6, pokiaľ systém neslúži ako smerovač IPv6.	**Umiestnenie** /etc/security/pscexpert/dodv2/ntwkoptsdod **Akcia na zabezpečenie súladu** Nastaví hodnotu voľby siete ip6forwarding na *1*.
GEN005820	2	Anonymné identifikátory UID a GID pre NFS musia byť nakonfigurované s hodnotami bez oprávnení.	**Umiestnenie** /etc/security/pscexpert/dodv2/nfsoptions **Akcia na zabezpečenie súladu** Zabezpečuje, že určené identifikátory nebudú mať žiadne oprávnenia.
GEN005840	2	Server NFS musí byť nakonfigurovaný tak, aby prístup k súborovému systému povoľoval len lokálnym hostiteľom.	**Umiestnenie** /etc/security/pscexpert/dodv2/nfsoptions **Akcia na zabezpečenie súladu** Nakonfiguruje server NFS, aby prístup povoľoval len lokálnym hostiteľom.
GEN005880	2	Server NFS nesmie povoľovať vzdialený prístup užívateľa root.	**Umiestnenie** /etc/security/pscexpert/dodv2/nfsoptions **Akcia na zabezpečenie súladu** Zakáže vzdialený prístup užívateľa root na serveri NFS.
GEN005900	2	Voľba *nosuid* musí byť povolená na všetkých klientskych pripojeniach NFS.	**Umiestnenie** /etc/security/pscexpert/dodv2/nosuid **Akcia na zabezpečenie súladu** Povolí voľbu *nosuid* na všetkých klientskych pripojeniach NFS.
GEN006060	2	V systéme sa nesmie spúšťať server Samba, pokiaľ nie je potrebný.	**Umiestnenie** /etc/security/pscexpert/dodv2/dodv2services **Akcia na zabezpečenie súladu** Zabezpečuje, že systém bude spĺňať definované požiadavky.
GEN006380	1	Systém nesmie používať protokol UDP pre NIS alebo NIS+.	**Umiestnenie** /etc/security/pscexpert/dodv2/dodv2cat1 **Akcia na zabezpečenie súladu** Zobrazí výsledky určených testov pravidiel.

Tabuľka 2. Všeobecné požiadavky Ministerstva obrany USA (pokračovanie)

ID kontrolného bodu STIG Ministerstva obrany USA	Kategória pravidla STIG	Popis	Umiestnenie skriptu, v ktorom je definovaná akcia, a výsledky akcie zabezpečujúcej súlad
GEN006400	2	Protokol NIS (Network Information System) sa nesmie používať.	**Umiestnenie** /etc/security/pscexpert/dodv2/nisplus **Akcia na zabezpečenie súladu** Zakáže určený protokol. **Poznámka:** Toto nastavenie nebude automaticky zmenené pri obnovení predvolenej politiky systému AIX prostredníctvom súboru DoDv2_to_ AIXDefault.xml. Toto nastavenie je potrebné manuálne zmeniť.
GEN006420	2	Mapy NIS musia byť chránené použitím ťažko uhádnuteľných názvov domén.	**Umiestnenie** /etc/security/pscexpert/dodv2/nisplus **Akcia na zabezpečenie súladu** Zabezpečuje, že názvy domén nebude možné ľahko zistiť.
GEN006460	2	Všetky servery NIS+ musia by spustené s úrovňou zabezpečenia 2.	**Umiestnenie** /etc/security/pscexpert/dodv2/nisplus **Akcia na zabezpečenie súladu** Zabezpečuje, že server bude používať určenú minimálnu úroveň zabezpečenia. **Poznámka:** Toto nastavenie nebude automaticky zmenené pri obnovení predvolenej politiky systému AIX prostredníctvom súboru DoDv2_to_ AIXDefault.xml. Toto nastavenie je potrebné manuálne zmeniť.
GEN006480	2	Systém musí byť týždenne kontrolovaný, či neobsahuje neoprávnené súbory setuid alebo či nedošlo k neoprávnenej úprave oprávnených súborov setuid.	**Umiestnenie** /etc/security/pscexpert/dodv2/trust **Akcia na zabezpečenie súladu** Týždenne skontroluje, či nedošlo k zmenám v určených súboroch.
GEN006560	2	Systém musí byť týždenne kontrolovaný, či neobsahuje neoprávnené súbory setuid alebo či nedošlo k neoprávnenej úprave oprávnených súborov setuid.	**Umiestnenie** /etc/security/pscexpert/dodv2/trust **Akcia na zabezpečenie súladu** Týždenne skontroluje, či nedošlo k zmenám v určených súboroch.
GEN006580	2	V systéme sa musí používať program na riadenie prístupu.	**Umiestnenie** /etc/security/pscexpert/dodv2/checktcpd **Akcia na zabezpečenie súladu** Zabezpečuje, že systém bude spĺňať definované požiadavky.
GEN006600	2	Program na riadenie prístupu používaný v systéme musí zaznamenávať každý pokus o prístup do systému do protokolu.	**Umiestnenie** /etc/security/pscexpert/dodv2/chsyslogdod **Akcia na zabezpečenie súladu** Zabezpečuje, že pokusy o prístup budú zaznamenané do protokolu.

Tabuľka 2. Všeobecné požiadavky Ministerstva obrany USA (pokračovanie)

ID kontrolného bodu STIG Ministerstva obrany USA	Kategória pravidla STIG	Popis	Umiestnenie skriptu, v ktorom je definovaná akcia, a výsledky akcie zabezpečujúcej súlad
GEN006620	2	Program na riadenie prístupu používaný v systéme musí byť nakonfigurovaný tak, aby povoľoval alebo zakazoval prístup do systému pre určitých hostiteľov.	**Umiestnenie** /etc/security/pscexpert/dodv2/chetchostsdod **Akcia na zabezpečenie súladu** Nakonfiguruje požadované nastavenia v súboroch hosts.deny a hosts.allow.
GEN007020	2	Protokol SCTP (Stream Control Transmission Protocol) musí byť zakázaný.	**Umiestnenie** /etc/security/pscexpert/dodv2/dodv2netrules **Akcia na zabezpečenie súladu** Zakáže určený protokol.
GEN007700	2	Obslužný program protokolu IPv6 nesmie byť naviazaný na sieťový zásobník, pokiaľ nebude potrebný.	**Umiestnenie** /etc/security/pscexpert/dodv2/rminet6 **Akcia na zabezpečenie súladu** Zakáže obslužný program protokolu IPv6 v sieťovom zásobníku, pokiaľ tento obslužný program nie je určený v súbore /etc/ipv6.conf. **Poznámka:** Ak sa vo vašom systéme používa protokol IPv6, uistite sa, že nastavenie *ipv6_enabled* v súbore /etc/security/pscexpert/ipv6.conf má hodnotu yes. Ak sa v systéme nepoužíva protokol IPv6, uistite sa, že má nastavenie *ipv6_enabled* hodnotu no.
GEN007780	2	V systéme nesmú byť povolené tunely 6to4.	**Umiestnenie** /etc/security/pscexpert/dodv2/rmiface **Akcia na zabezpečenie súladu** Zakáže určené tunely. **Poznámka:** Toto nastavenie nebude automaticky zmenené pri obnovení predvolenej politiky systému AIX prostredníctvom súboru DoDv2_to_ AIXDefault.xml. Toto nastavenie je potrebné manuálne zmeniť.
GEN007820	2	V systéme nesmú byť nakonfigurované tunely IP.	**Umiestnenie** /etc/security/pscexpert/dodv2/rmtunnel **Akcia na zabezpečenie súladu** Zakáže tunely IP. **Poznámka:** Toto nastavenie nebude automaticky zmenené pri obnovení predvolenej politiky systému AIX prostredníctvom súboru DoDv2_to_ AIXDefault.xml. Toto nastavenie je potrebné manuálne zmeniť.
GEN007840	2	Klient DHCP musí byť zakázaný, ak sa nepoužíva.	**Umiestnenie** /etc/security/pscexpert/dodv2/dodv2services **Akcia na zabezpečenie súladu** Zabezpečuje, že systém bude spĺňať definované požiadavky.
GEN007850	2	Klient DHCP nesmie posielať dynamické zmeny DNS.	**Umiestnenie** /etc/security/pscexpert/dodv2/dodv2services **Akcia na zabezpečenie súladu** Zabezpečuje, že systém bude spĺňať definované požiadavky.

Tabuľka 2. Všeobecné požiadavky Ministerstva obrany USA (pokračovanie)

ID kontrolného bodu STIG Ministerstva obrany USA	Kategória pravidla STIG	Popis	Umiestnenie skriptu, v ktorom je definovaná akcia, a výsledky akcie zabezpečujúcej súlad
GEN007860	2	Systém musí ignorovať správy o presmerovaní IPv6 ICMP.	**Umiestnenie** /etc/security/pscexpert/dodv2/ntwkoptsdod **Akcia na zabezpečenie súladu** Nastaví hodnotu voľby siete ipignoreredirects na *1*.
GEN007880	2	Systém nesmie posielať správy o presmerovaní IPv6 ICMP.	**Umiestnenie** /etc/security/pscexpert/dodv2/ntwkoptsdod **Akcia na zabezpečenie súladu** Nastaví hodnotu voľby siete ipsendredirects na *0*.
GEN007900	2	Systém musí používať príslušný filter spätnej trasy pre sieťové prenosy IPv6, ak sa v systéme používa protokol IPv6.	**Umiestnenie** /etc/security/pscexpert/dodv2/chuserstanzadod **Akcia na zabezpečenie súladu** Zabezpečuje, že systém bude spĺňať definované požiadavky.
GEN007920	2	Systém nesmie preposielať pakety IPv6 smerované zo zdroja.	**Umiestnenie** /etc/security/pscexpert/dodv2/ntwkoptsdod **Akcia na zabezpečenie súladu** Nastaví hodnotu voľby siete ip6srcrouteforward na *0*.
GEN007940: GEN003607	2	Systém nesmie akceptovať pakety IPv4 alebo IPv6 smerované zo zdroja.	**Umiestnenie** /etc/security/pscexpert/dodv2/ntwkoptsdod **Akcia na zabezpečenie súladu** Nastaví hodnotu voľby siete ipsrcrouterecv na *0*.
GEN007950	2	Systém nesmie reagovať na požiadavky echo ICMPv6 odoslané na adresu vysielania.	**Umiestnenie** /etc/security/pscexpert/dodv2/ntwkoptsdod **Akcia na zabezpečenie súladu** Nastaví hodnotu voľby siete bcastping na *0*.
GEN008000	2	Ak sa v systéme používa protokol LDAP (Lightweight Directory Access Protocol) na autentifikáciu alebo získanie informácií o konte, certifikáty používané na autentifikáciu na serveri LDAP musia byť poskytnuté z infraštruktúry PKI Ministerstva obrany USA alebo spôsobom schváleným Ministerstvom obrany USA.	**Umiestnenie** /etc/security/pscexpert/dodv2/ldap_config **Akcia na zabezpečenie súladu** Zabezpečuje, že systém bude spĺňať definované požiadavky.

Tabuľka 2. Všeobecné požiadavky Ministerstva obrany USA (pokračovanie)

ID kontrolného bodu STIG Ministerstva obrany USA	Kategória pravidla STIG	Popis	Umiestnenie skriptu, v ktorom je definovaná akcia, a výsledky akcie zabezpečujúcej súlad
GEN008020	2	Ak sa v systéme používa protokol LDAP na autentifikáciu alebo získanie informácií o konte, pripojenie Transport Layer Security (TLS) k serveru LDAP musí vyžadovať, aby server poskytoval certifikát s platnou dôveryhodnou cestou.	**Umiestnenie** /etc/security/pscexpert/dodv2/ldap_config **Akcia na zabezpečenie súladu** Zabezpečuje, že systém bude spĺňať definované požiadavky.
GEN008050	2	Ak sa v systéme používa protokol LDAP na autentifikáciu alebo získanie informácií o konte, súbor /etc/ldap.conf (alebo ekvivalentný) nesmie obsahovať heslá.	**Umiestnenie** /etc/security/pscexpert/dodv2/ldap_config **Akcia na zabezpečenie súladu** Zabezpečuje, že systém bude spĺňať definované požiadavky.
GEN008380	2	Systém musí byť týždenne kontrolovaný, či neobsahuje neoprávnené súbory setuid alebo či nedošlo k neoprávnenej úprave oprávnených súborov setuid.	**Umiestnenie** /etc/security/pscexpert/dodv2/trust **Akcia na zabezpečenie súladu** Týždenne skontroluje, či nedošlo k zmenám v určených súboroch.
GEN008520	2	Systém musí využívať lokálnu bránu firewall, ktorá bude chrániť hostiteľa pred skenovaním portov. Firewall musí zakázať prístup k zraniteľným portom na 5 minút v záujme ochrany hostiteľa pred skenovaním portov.	**Umiestnenie** /etc/security/pscexpert/dodv2/ipsecshunports **Akcia na zabezpečenie súladu** Zabezpečuje, že systém bude spĺňať definované požiadavky.
GEN008540	2	Lokálna brána firewall systému musí implementovať politiku *deny-all*, *allow-by-exception*.	**Umiestnenie** /etc/security/pscexpert/dodv2/ipsecshunhosthls **Akcia na zabezpečenie súladu** Zabezpečuje, že systém bude spĺňať definované požiadavky. **Poznámka:** Ďalšie pravidlá filtrovania môžete zadať v súbore /etc/security/aixpert/bin/filter.txt. Tieto pravidlá sú integrované skriptom ipsecshunhosthls.sh pri uplatnení profilu. Tieto položky musia byť v nasledujúcom formáte: *číslo_portu*:*IP_adresa*: *akcia* Možné hodnoty pre premennú *akcia* sú Allow a Deny.
GEN008600	1	Systém musí byť nakonfigurovaný tak, aby sa spúšťal iba z konfigurácie zavedenia systému.	**Umiestnenie** /etc/security/pscexpert/dodv2/dodv2cat1 **Akcia na zabezpečenie súladu** Zabezpečuje, že pri spúšťaní systému sa použije iba konfigurácia zavedenia systému.

Tabuľka 2. Všeobecné požiadavky Ministerstva obrany USA (pokračovanie)

ID kontrolného bodu STIG Ministerstva obrany USA	Kategória pravidla STIG	Popis	Umiestnenie skriptu, v ktorom je definovaná akcia, a výsledky akcie zabezpečujúcej súlad
GEN008640	1	Systém nesmie používať vymeniteľné médiá ako zdroj zavedenia.	**Umiestnenie** /etc/security/pscexpert/dodv2/dodv2cat1 **Akcia na zabezpečenie súladu** Zabezpečuje, že systém sa nebude zavádzať z jednotky vymeniteľných médií.
GEN009140	1,2,3	V systéme nesmie byť aktívna služba chargen.	**Umiestnenie** /etc/security/pscexpert/dodv2/inetdservices **Akcia na zabezpečenie súladu** Zakáže vyžadovaných démonov a služby označením položiek v súbore /etc/inetd.conf znakom komentára.
GEN009160	1,2,3	V systéme nesmie byť aktívna služba Calendar Management Service Daemon (CMSD).	**Umiestnenie** /etc/security/pscexpert/dodv2/inetdservices **Akcia na zabezpečenie súladu** Zakáže vyžadovaných démonov a služby označením položiek v súbore /etc/inetd.conf znakom komentára.
GEN009180	1,2,3	V systéme nesmie byť aktívna služba tool-talk database server (ttdbserver).	**Umiestnenie** /etc/security/pscexpert/dodv2/inetdservices **Akcia na zabezpečenie súladu** Zakáže vyžadovaných démonov a služby označením položiek v súbore /etc/inetd.conf znakom komentára.
GEN009190	1,2,3	V systéme nesmie byť aktívna služba comsat.	**Umiestnenie** /etc/security/pscexpert/dodv2/inetdservices **Akcia na zabezpečenie súladu** Zakáže vyžadovaných démonov a služby označením položiek v súbore /etc/inetd.conf znakom komentára.
GEN009200-9330	1,2,3	V systéme nesmú byť aktívne iné služby a démoni.	**Umiestnenie** /etc/security/pscexpert/dodv2/inetdservices **Akcia na zabezpečenie súladu** Zakáže vyžadovaných démonov a služby označením položiek v súbore /etc/inetd.conf znakom komentára.
GEN009210	2	V systéme nesmie byť aktívna služba discard.	**Umiestnenie** /etc/security/pscexpert/dodv2/inetdservices **Akcia na zabezpečenie súladu** Zakáže vyžadovaných démonov a služby označením položiek v súbore /etc/inetd.conf znakom komentára.
GEN009220	2	V systéme nesmie byť aktívna služba dtspc.	**Umiestnenie** /etc/security/pscexpert/dodv2/inetdservices **Akcia na zabezpečenie súladu** Zakáže vyžadovaných démonov a služby označením položiek v súbore /etc/inetd.conf znakom komentára.
GEN009230	2	V systéme nesmie byť aktívna služba echo.	**Umiestnenie** /etc/security/pscexpert/dodv2/inetdservices **Akcia na zabezpečenie súladu** Zakáže vyžadovaných démonov a služby označením položiek v súbore /etc/inetd.conf znakom komentára.

Tabuľka 2. Všeobecné požiadavky Ministerstva obrany USA (pokračovanie)

ID kontrolného bodu STIG Ministerstva obrany USA	Kategória pravidla STIG	Popis	Umiestnenie skriptu, v ktorom je definovaná akcia, a výsledky akcie zabezpečujúcej súlad
GEN009240	2	V systéme nesmie byť aktívna služba Internet Message Access Protocol (IMAP).	**Umiestnenie** /etc/security/pscexpert/dodv2/inetdservices **Akcia na zabezpečenie súladu** Zakáže vyžadovaných démonov a služby označením položiek v súbore /etc/inetd.conf znakom komentára.
GEN009250	2	V systéme nesmie byť aktívna služba PostOffice Protocol (POP3).	**Umiestnenie** /etc/security/pscexpert/dodv2/inetdservices **Akcia na zabezpečenie súladu** Zakáže vyžadovaných démonov a služby označením položiek v súbore /etc/inetd.conf znakom komentára.
GEN009260	2	V systéme nesmie byť aktívna služba talk alebo ntalk.	**Umiestnenie** /etc/security/pscexpert/dodv2/inetdservices **Akcia na zabezpečenie súladu** Zakáže vyžadovaných démonov a služby označením položiek v súbore /etc/inetd.conf znakom komentára.
GEN009270	2	V systéme nesmie byť aktívna služba netstat v procese InetD.	**Umiestnenie** /etc/security/pscexpert/dodv2/inetdservices **Akcia na zabezpečenie súladu** Zakáže vyžadovaných démonov a služby označením položiek v súbore /etc/inetd.conf znakom komentára.
GEN009280	2	V systéme nesmie byť aktívna služba PCNFS.	**Umiestnenie** /etc/security/pscexpert/dodv2/inetdservices **Akcia na zabezpečenie súladu** Zakáže vyžadovaných démonov a služby označením položiek v súbore /etc/inetd.conf znakom komentára.
GEN009290	2	V systéme nesmie byť aktívna služba systat.	**Umiestnenie** /etc/security/pscexpert/dodv2/inetdservices **Akcia na zabezpečenie súladu** Zakáže vyžadovaných démonov a služby označením položiek v súbore /etc/inetd.conf znakom komentára.
GEN009300	2	V systéme nesmie byť aktívna služba inetd time v démonovi inetd.	**Umiestnenie** /etc/security/pscexpert/dodv2/inetdservices **Akcia na zabezpečenie súladu** Zakáže vyžadovaných démonov a služby označením položiek v súbore /etc/inetd.conf znakom komentára.
GEN009310	2	V systéme nesmie byť aktívna služba rusersd.	**Umiestnenie** /etc/security/pscexpert/dodv2/inetdservices **Akcia na zabezpečenie súladu** Zakáže vyžadovaných démonov a služby označením položiek v súbore /etc/inetd.conf znakom komentára.
GEN009320	2	V systéme nesmie byť aktívna služba sprayd.	**Umiestnenie** /etc/security/pscexpert/dodv2/inetdservices **Akcia na zabezpečenie súladu** Zakáže vyžadovaných démonov a služby označením položiek v súbore /etc/inetd.conf znakom komentára.

Tabuľka 2. Všeobecné požiadavky Ministerstva obrany USA (pokračovanie)

ID kontrolného bodu STIG Ministerstva obrany USA	Kategória pravidla STIG	Popis	Umiestnenie skriptu, v ktorom je definovaná akcia, a výsledky akcie zabezpečujúcej súlad
GEN009330	2	V systéme nesmie byť aktívna služba rstatd.	**Umiestnenie** /etc/security/pscexpert/dodv2/inetdservices **Akcia na zabezpečenie súladu** Zakáže vyžadovaných démonov a služby označením položiek v súbore /etc/inetd.conf znakom komentára.
GEN009340	2	Manažéri prihlásenia servera X Window System nesmú bežať, pokiaľ nie sú vyžadovaní pre správu relácií X11.	**Umiestnenie** /etc/security/pscexpert/dodv2/dodv2cmntrows **Akcia na zabezpečenie súladu** Toto pravidlo zakáže pripojenia k serveru X Window System a správcu prihlásenia XServer.

Tabuľka 3. Požiadavky Ministerstva obrany USA na vlastníctvo

ID kontrolného bodu STIG Ministerstva obrany USA	Popis	Umiestnenie skriptu, v ktorom je definovaná akcia, a výsledky akcie zabezpečujúcej súlad
AIX00085	Vlastníkom súboru /etc/netsvc.conf musí byť užívateľ root.	**Umiestnenie** /etc/security/pscexpert/dodv2/chowndodfiles **Akcia na zabezpečenie súladu** Zabezpečuje, že vlastníkom určeného súboru bude užívateľ root.
AIX00090	Vlastníkom súboru /etc/netsvc.conf musí byť skupina bin, sys alebo system.	**Umiestnenie** /etc/security/pscexpert/dodv2/chowndodfiles **Akcia na zabezpečenie súladu** Zabezpečuje, že vlastníkom určeného súboru bude skupina bin, sys alebo system.
AIX00320	Vlastníkom súboru /etc/ftpaccess.ctl musí byť užívateľ root.	**Umiestnenie** /etc/security/pscexpert/dodv2/chowndodfiles **Akcia na zabezpečenie súladu** Zabezpečuje, že vlastníkom určeného súboru bude užívateľ root.
AIX00330	Vlastníkom súboru /etc/ftpaccess.ctl musí byť skupina bin, sys alebo system.	**Umiestnenie** /etc/security/pscexpert/dodv2/chowndodfiles **Akcia na zabezpečenie súladu** Zabezpečuje, že vlastníkom určeného súboru bude skupina bin, sys alebo system.
GEN000250	Vlastníkom konfiguračného súboru synchronizácie času (ako napríklad /etc/ntp.conf) musí byť užívateľ root.	**Umiestnenie** /etc/security/pscexpert/dodv2/chowndodfiles **Akcia na zabezpečenie súladu** Zabezpečuje, že vlastníkom určeného súboru bude užívateľ root.
GEN000251	Vlastníkom konfiguračného súboru synchronizácie času (ako napríklad /etc/ntp.conf) musí byť skupina bin, sys alebo systém.	**Umiestnenie** /etc/security/pscexpert/dodv2/chowndodfiles **Akcia na zabezpečenie súladu** Zabezpečuje, že vlastníkom určeného súboru bude skupina bin, sys alebo system.

Tabuľka 3. Požiadavky Ministerstva obrany USA na vlastníctvo (pokračovanie)

ID kontrolného bodu STIG Ministerstva obrany USA	Popis	Umiestnenie skriptu, v ktorom je definovaná akcia, a výsledky akcie zabezpečujúcej súlad
GEN001160	Všetky súbory a adresáre musia mať platného vlastníka.	**Umiestnenie** /etc/security/pscexpert/dodv2/chowndodfiles **Akcia na zabezpečenie súladu** Zabezpečuje, že všetky súbory a adresáre budú mať platného vlastníka.
GEN001170	Všetky súbory a adresáre musia mať platného skupinového vlastníka.	**Umiestnenie** /etc/security/pscexpert/dodv2/chowndodfiles **Akcia na zabezpečenie súladu** Zabezpečuje, že všetky súbory a adresáre budú mať platného vlastníka.
GEN001220	Vlastníkom všetkých systémových súborov, programov a adresárov musí byť konto system.	**Umiestnenie** /etc/security/pscexpert/dodv2/chowndodfiles **Akcia na zabezpečenie súladu** Zabezpečuje, že vlastníkom všetkých systémových súborov, programov a adresárov bude konto system.
GEN001240	Vlastníkom systémových súborov, programov a adresárov musí byť skupina system.	**Umiestnenie** /etc/security/pscexpert/dodv2/chowndodfiles **Akcia na zabezpečenie súladu** Zabezpečuje, že vlastníkom všetkých systémových súborov, programov a adresárov bude skupina system.
GEN001320	Vlastníkom súborov NIS (Network Information Systems)/NIS+/yp musí byť užívateľ root alebo skupina sys alebo bin.	**Umiestnenie** /etc/security/pscexpert/dodv2/chowndodfiles **Akcia na zabezpečenie súladu** Zabezpečuje, že vlastníkom určených súborov bude užívateľ root alebo skupina sys alebo bin.
GEN001340	Vlastníkom súborov NIS/NIS+/yp musí byť skupina sys, bin, other alebo system.	**Umiestnenie** /etc/security/pscexpert/dodv2/chowndodfiles **Akcia na zabezpečenie súladu** Zabezpečuje, že vlastníkom určených súborov bude skupina sys, bin, other alebo system.
GEN001362	Vlastníkom súboru /etc/resolv.conf musí byť užívateľ root.	**Umiestnenie** /etc/security/pscexpert/dodv2/chowndodfiles **Akcia na zabezpečenie súladu** Zabezpečuje, že vlastníkom určeného súboru bude užívateľ root.
GEN001363	Vlastníkom súboru /etc/resolv.conf musí byť skupina bin, sys alebo system.	**Umiestnenie** /etc/security/pscexpert/dodv2/chowndodfiles **Akcia na zabezpečenie súladu** Zabezpečuje, že vlastníkom určeného súboru bude skupina bin, sys alebo system.
GEN001366	Vlastníkom súboru /etc/hosts musí byť užívateľ root.	**Umiestnenie** /etc/security/pscexpert/dodv2/chowndodfiles **Akcia na zabezpečenie súladu** Zabezpečuje, že vlastníkom určeného súboru bude užívateľ root.

Tabuľka 3. Požiadavky Ministerstva obrany USA na vlastníctvo (pokračovanie)

ID kontrolného bodu STIG Ministerstva obrany USA	Popis	Umiestnenie skriptu, v ktorom je definovaná akcia, a výsledky akcie zabezpečujúcej súlad
GEN001367	Vlastníkom súboru /etc/hosts musí byť skupina bin, sys alebo system.	**Umiestnenie** /etc/security/pscexpert/dodv2/chowndodfiles **Akcia na zabezpečenie súladu** Zabezpečuje, že vlastníkom určeného súboru bude skupina bin, sys alebo system.
GEN001371	Vlastníkom súboru /etc/nsswitch.conf musí byť užívateľ root.	**Umiestnenie** /etc/security/pscexpert/dodv2/chowndodfiles **Akcia na zabezpečenie súladu** Zabezpečuje, že vlastníkom určeného súboru bude užívateľ root.
GEN001372	Vlastníkom súboru /etc/nsswitch.conf musí byť užívateľ root alebo skupina bin, sys alebo system.	**Umiestnenie** /etc/security/pscexpert/dodv2/chowndodfiles **Akcia na zabezpečenie súladu** Zabezpečuje, že vlastníkom určeného súboru bude užívateľ root alebo skupina bin, sys alebo system.
GEN001378	Vlastníkom súboru /etc/passwd musí byť užívateľ root.	**Umiestnenie** /etc/security/pscexpert/dodv2/chowndodfiles **Akcia na zabezpečenie súladu** Zabezpečuje, že vlastníkom určeného súboru bude užívateľ root.
GEN001379	Vlastníkom súboru /etc/passwd musí byť skupina bin, security, sys alebo system.	**Umiestnenie** /etc/security/pscexpert/dodv2/chowndodfiles **Akcia na zabezpečenie súladu** Zabezpečuje, že vlastníkom určeného súboru bude skupina bin, security, sys alebo system.
GEN001391	Vlastníkom súboru /etc/group musí byť užívateľ root.	**Umiestnenie** /etc/security/pscexpert/dodv2/chowndodfiles **Akcia na zabezpečenie súladu** Zabezpečuje, že vlastníkom určeného súboru bude užívateľ root.
GEN001392	Vlastníkom súboru /etc/group musí byť skupina bin, security, sys alebo system.	**Umiestnenie** /etc/security/pscexpert/dodv2/chowndodfiles **Akcia na zabezpečenie súladu** Zabezpečuje, že vlastníkom určeného súboru bude skupina bin, security, sys alebo system.
GEN001400	Vlastníkom súboru /etc/security/passwd musí byť užívateľ root.	**Umiestnenie** /etc/security/pscexpert/dodv2/chowndodfiles **Akcia na zabezpečenie súladu** Zabezpečuje, že vlastníkom určeného súboru bude užívateľ root.
GEN001410	Vlastníkom súboru /etc/security/passwd musí byť skupina bin, security, sys alebo system.	**Umiestnenie** /etc/security/pscexpert/dodv2/chowndodfiles **Akcia na zabezpečenie súladu** Zabezpečuje, že vlastníkom určeného súboru bude skupina bin, security, sys alebo system.

Tabuľka 3. Požiadavky Ministerstva obrany USA na vlastníctvo (pokračovanie)

ID kontrolného bodu STIG Ministerstva obrany USA	Popis	Umiestnenie skriptu, v ktorom je definovaná akcia, a výsledky akcie zabezpečujúcej súlad
GEN001500	Domovské adresáre všetkých interaktívnych užívateľov musia byť vlastnené príslušnými užívateľmi.	**Umiestnenie** /etc/security/pscexpert/dodv2/chowndodfiles **Akcia na zabezpečenie súladu** Zabezpečuje, že domovské adresáre všetkých interaktívnych užívateľov budú vlastnené príslušnými užívateľmi.
GEN001520	Domovské adresáre všetkých interaktívnych užívateľov musia byť vlastnené primárnou skupinou vlastníka príslušného domovského adresára.	**Umiestnenie** /etc/security/pscexpert/dodv2/chowndodfiles **Akcia na zabezpečenie súladu** Zabezpečuje, že domovské adresáre všetkých interaktívnych užívateľov budú vlastnené primárnou skupinou vlastníka príslušného domovského adresára.
GEN001540	Vlastníkom všetkých súborov a adresárov v domovských adresároch interaktívnych užívateľov musí byť vlastník príslušného domovského adresára.	**Umiestnenie** /etc/security/pscexpert/dodv2/chowndodfiles **Akcia na zabezpečenie súladu** Zabezpečuje, že vlastníkom všetkých súborov a adresárov v domovských adresároch interaktívnych užívateľov bude vlastník príslušného domovského adresára.
GEN001550	Vlastníkom všetkých súborov a adresárov v domovských adresároch interaktívnych užívateľov musí byť skupina, do ktorej patrí vlastník príslušného domovského adresára.	**Umiestnenie** /etc/security/pscexpert/dodv2/chowndodfiles **Akcia na zabezpečenie súladu** Zabezpečuje, že vlastníkom všetkých súborov a adresárov v domovských adresároch interaktívnych užívateľov bude skupina, do ktorej patrí vlastník príslušného domovského adresára.
GEN001660	Vlastníkom všetkých systémových spúšťacích súborov musí byť užívateľ root.	**Umiestnenie** /etc/security/pscexpert/dodv2/chowndodfiles **Akcia na zabezpečenie súladu** Zabezpečuje, že vlastníkom určených súborov bude užívateľ root.
GEN001680	Vlastníkom všetkých systémových spúšťacích súborov musí byť skupina sys, bin, other alebo system.	**Umiestnenie** /etc/security/pscexpert/dodv2/chowndodfiles **Akcia na zabezpečenie súladu** Zabezpečuje, že vlastníkom určených súborov bude skupina sys, bin, other alebo system.
GEN001740	Vlastníkom všetkých globálnych inicializačných súborov musí byť užívateľ root.	**Umiestnenie** /etc/security/pscexpert/dodv2/chowndodfiles **Akcia na zabezpečenie súladu** Zabezpečuje, že vlastníkom určených súborov bude užívateľ root.
GEN001760	Vlastníkom všetkých globálnych inicializačných súborov musí byť skupina sys, bin, system alebo security.	**Umiestnenie** /etc/security/pscexpert/dodv2/chowndodfiles **Akcia na zabezpečenie súladu** Zabezpečuje, že vlastníkom určených súborov bude skupina sys, bin, system alebo security.

Tabuľka 3. Požiadavky Ministerstva obrany USA na vlastníctvo (pokračovanie)

ID kontrolného bodu STIG Ministerstva obrany USA	Popis	Umiestnenie skriptu, v ktorom je definovaná akcia, a výsledky akcie zabezpečujúcej súlad
GEN001820	Vlastníkom všetkých skeletových súborov a adresárov (zvyčajne pod adresárom /etc/skel) musí byť užívateľ root alebo skupina bin.	**Umiestnenie** /etc/security/pscexpert/dodv2/chowndodfiles **Akcia na zabezpečenie súladu** Zabezpečuje, že vlastníkom určených súborov bude užívateľ root alebo skupina bin.
GEN001830	Vlastníkom všetkých skeletových súborov a adresárov (zvyčajne pod adresárom /etc/skel) musí byť skupina security.	**Umiestnenie** /etc/security/pscexpert/dodv2/chowndodfiles **Akcia na zabezpečenie súladu** Zabezpečuje, že vlastníkom určených súborov bude skupina security.
GEN001860	Vlastníkom všetkých lokálnych inicializačných súborov musí byť užívateľ alebo konto root.	**Umiestnenie** /etc/security/pscexpert/dodv2/chowndodfiles **Akcia na zabezpečenie súladu** Zabezpečuje, že vlastníkom určených súborov bude užívateľ alebo konto root.
GEN001870	Vlastníkom lokálnych inicializačných súborov musí byť primárna skupina užívateľa alebo konto root.	**Umiestnenie** /etc/security/pscexpert/dodv2/chowndodfiles **Akcia na zabezpečenie súladu** Zabezpečuje, že vlastníkom lokálnych inicializačných súborov bude primárna skupina užívateľa alebo konto root.
GEN002060	Prístup k súborom .rhosts, .shosts, .netrc alebo hosts.equiv môže mať len užívateľ root alebo ich vlastník.	**Umiestnenie** /etc/security/pscexpert/dodv2/chowndodfiles /etc/security/pscexpert/dodv2/fpmdodfiles **Akcia na zabezpečenie súladu** Zabezpečuje, že k určeným súborom bude mať prístup iba užívateľ root alebo ich vlastník.
GEN002100	Súbor .rhosts nesmie byť podporovaný modulom PAM (Pluggable Authentication Module).	**Umiestnenie** /etc/security/pscexpert/dodv2/chowndodfiles **Akcia na zabezpečenie súladu** Zabezpečuje, že určený súbor nebude dostupný cez modul PAM.
GEN002200	Vlastníkom všetkých súborov prostredia shell musí byť užívateľ root alebo skupina bin.	**Umiestnenie** /etc/security/pscexpert/dodv2/chowndodfiles **Akcia na zabezpečenie súladu** Zabezpečuje, že vlastníkom určených súborov bude užívateľ root alebo skupina bin.
GEN002210	Vlastníkom všetkých súborov prostredia shell musí byť užívateľ root alebo skupina bin, sys alebo system.	**Umiestnenie** /etc/security/pscexpert/dodv2/chowndodfiles **Akcia na zabezpečenie súladu** Zabezpečuje, že vlastníkom určených súborov bude užívateľ root alebo skupina bin, sys alebo system.
GEN002340	Vlastníkom audio zariadení musí byť užívateľ root.	**Umiestnenie** /etc/security/pscexpert/dodv2/chowndodfiles **Akcia na zabezpečenie súladu** Zabezpečuje, že vlastníkom všetkých audio zariadení bude užívateľ root.

Tabuľka 3. Požiadavky Ministerstva obrany USA na vlastníctvo (pokračovanie)

ID kontrolného bodu STIG Ministerstva obrany USA	Popis	Umiestnenie skriptu, v ktorom je definovaná akcia, a výsledky akcie zabezpečujúcej súlad
GEN002360	Vlastníkom všetkých audio zariadení musí byť užívateľ root alebo skupina sys, bin alebo system.	**Umiestnenie** /etc/security/pscexpert/dodv2/chowndodfiles **Akcia na zabezpečenie súladu** Zabezpečuje, že vlastníkom všetkých audio zariadení bude užívateľ root alebo skupina sys, bin alebo system.
GEN002520	Vlastníkom všetkých verejných adresárov musí byť užívateľ root alebo konto aplikácie.	**Umiestnenie** /etc/security/pscexpert/dodv2/chowndodfiles **Akcia na zabezpečenie súladu** Zabezpečuje, že vlastníkom všetkých verejných adresárov bude užívateľ root alebo konto aplikácie.
GEN002540	Vlastníkom všetkých verejných adresárov musí byť skupina system alebo skupina aplikácie.	**Umiestnenie** /etc/security/pscexpert/dodv2/chowndodfiles **Akcia na zabezpečenie súladu** Zabezpečuje, že vlastníkom všetkých verejných adresárov bude skupina system alebo skupina aplikácie.
GEN002680	Vlastníkom protokolov z auditu systému musí byť užívateľ root.	**Umiestnenie** /etc/security/pscexpert/dodv2/chowndodfiles **Akcia na zabezpečenie súladu** Zabezpečuje, že vlastníkom určených súborov bude užívateľ root.
GEN002690	Vlastníkom protokolov z auditu systému bude musí byť skupina bin, sys alebo system.	**Umiestnenie** /etc/security/pscexpert/dodv2/chowndodfiles **Akcia na zabezpečenie súladu** Zabezpečuje, že vlastníkom určených súborov bude skupina bin, sys alebo system.
GEN003020	Program cron nesmie spúšťať programy v globálne zapisovateľných adresároch alebo pod nimi.	**Umiestnenie** /etc/security/pscexpert/dodv2/chowndodfiles **Akcia na zabezpečenie súladu** Zabraňuje programu cron v spúšťaní programov v globálne zapisovateľných adresároch alebo pod nimi.
GEN003040	Vlastníkom súborov crontab musí byť užívateľ root alebo tvorca súboru crontab.	**Umiestnenie** /etc/security/pscexpert/dodv2/chowndodfiles **Akcia na zabezpečenie súladu** Zabezpečuje, že vlastníkom súborov crontab bude užívateľ root alebo tvorca súboru crontab.
GEN003050	Vlastníkom súborov crontab musí byť skupina system, cron alebo primárna skupina tvorcu súboru crontab.	**Umiestnenie** /etc/security/pscexpert/dodv2/chowndodfiles **Akcia na zabezpečenie súladu** Zabezpečuje, že vlastníkom súborov crontab bude skupina system, cron alebo primárna skupina tvorcu súboru crontab.

Tabuľka 3. Požiadavky Ministerstva obrany USA na vlastníctvo (pokračovanie)

ID kontrolného bodu STIG Ministerstva obrany USA	Popis	Umiestnenie skriptu, v ktorom je definovaná akcia, a výsledky akcie zabezpečujúcej súlad
GEN003110	Adresáre cron a crontab nesmú mať zoznamy rozšíreného riadenia prístupu.	**Umiestnenie** /etc/security/pscexpert/dodv2/chowndodfiles **Akcia na zabezpečenie súladu** Zabezpečuje, že určené adresáre nebudú mať zoznamy rozšíreného riadenia prístupu.
GEN003120	Vlastníkom adresárov cron a crontab musí byť užívateľ root alebo skupina bin.	**Umiestnenie** /etc/security/pscexpert/dodv2/chowndodfiles **Akcia na zabezpečenie súladu** Zabezpečuje, že vlastníkom adresárov cron a crontab bude užívateľ root alebo skupina bin.
GEN003140	Vlastníkom adresárov cron a crontab musí byť skupina system, sys, bin alebo cron.	**Umiestnenie** /etc/security/pscexpert/dodv2/chowndodfiles **Akcia na zabezpečenie súladu** Zabezpečuje, že vlastníkom určených adresárov bude skupina system, sys, bin alebo cron.
GEN003160	Musí byť implementované zaznamenávanie do protokolu programu cron.	**Umiestnenie** /etc/security/pscexpert/dodv2/chowndodfiles **Akcia na zabezpečenie súladu** Zabezpečuje, že je implementované zaznamenávanie do protokolu programu cron.
GEN003240	Vlastníkom súboru cron.allow musí byť užívateľ root alebo skupina bin alebo sys.	**Umiestnenie** /etc/security/pscexpert/dodv2/chowndodfiles **Akcia na zabezpečenie súladu** Zabezpečuje, že vlastníkom určeného súboru bude užívateľ root, bin alebo sys.
GEN003250	Vlastníkom súboru cron.allow musí byť skupina system, bin, sys alebo cron.	**Umiestnenie** /etc/security/pscexpert/dodv2/chowndodfiles **Akcia na zabezpečenie súladu** Zabezpečuje, že vlastníkom určeného súboru bude skupina system, bin, sys alebo cron.
GEN003260	Vlastníkom súboru cron.deny musí byť užívateľ root alebo skupina bin alebo sys.	**Umiestnenie** /etc/security/pscexpert/dodv2/chowndodfiles **Akcia na zabezpečenie súladu** Zabezpečuje, že vlastníkom určeného súboru bude užívateľ root, bin alebo sys.
GEN003270	Vlastníkom súboru cron.deny musí byť skupina system, bin, sys alebo cron.	**Umiestnenie** /etc/security/pscexpert/dodv2/chowndodfiles **Akcia na zabezpečenie súladu** Zabezpečuje, že vlastníkom určeného súboru bude skupina system, bin, sys alebo cron.
GEN003420	Vlastníkom adresára at musí byť užívateľ root alebo skupina bin, sys, deamon alebo cron.	**Umiestnenie** /etc/security/pscexpert/dodv2/chowndodfiles **Akcia na zabezpečenie súladu** Zabezpečuje, že vlastníkom určeného súboru bude užívateľ root alebo skupina sys, daemon alebo cron.

Tabuľka 3. Požiadavky Ministerstva obrany USA na vlastníctvo (pokračovanie)

ID kontrolného bodu STIG Ministerstva obrany USA	Popis	Umiestnenie skriptu, v ktorom je definovaná akcia, a výsledky akcie zabezpečujúcej súlad
GEN003430	Vlastníkom adresára at musí byť skupina system, bin, sys alebo cron.	**Umiestnenie** /etc/security/pscexpert/dodv2/chowndodfiles **Akcia na zabezpečenie súladu** Zabezpečuje, že vlastníkom určeného adresára bude skupina system, bin, sys alebo cron.
GEN003460	Vlastníkom súboru at.allow musí byť užívateľ root alebo skupina bin alebo sys.	**Umiestnenie** /etc/security/pscexpert/dodv2/chowndodfiles **Akcia na zabezpečenie súladu** Zabezpečuje, že vlastníkom určeného súboru bude užívateľ root, bin alebo sys.
GEN003470	Vlastníkom súboru at.allow musí byť skupina system, bin, sys alebo cron.	**Umiestnenie** /etc/security/pscexpert/dodv2/chowndodfiles **Akcia na zabezpečenie súladu** Zabezpečuje, že vlastníkom určeného súboru bude skupina system, bin, sys alebo cron.
GEN003480	Vlastníkom súboru at.deny musí byť užívateľ root alebo skupina bin alebo sys.	**Umiestnenie** /etc/security/pscexpert/dodv2/chowndodfiles **Akcia na zabezpečenie súladu** Zabezpečuje, že vlastníkom určeného súboru bude užívateľ root, bin alebo sys.
GEN003490	Vlastníkom súboru at.deny musí byť skupina system, bin, sys alebo cron.	**Umiestnenie** /etc/security/pscexpert/dodv2/chowndodfiles **Akcia na zabezpečenie súladu** Zabezpečuje, že vlastníkom určeného súboru bude skupina system, bin, sys alebo cron.
GEN003720	Vlastníkom súborov inetd.conf a xinetd.conf a adresára xinetd.d musí byť užívateľ root alebo skupina bin.	**Umiestnenie** /etc/security/pscexpert/dodv2/chowndodfiles **Akcia na zabezpečenie súladu** Zabezpečuje, že vlastníkom určených súborov a adresára bude užívateľ root alebo skupina bin.
GEN003730	Vlastníkom súborov inetd.conf a xinetd.conf a adresára xinetd.d musí byť skupina bin, sys alebo system.	**Umiestnenie** /etc/security/pscexpert/dodv2/chowndodfiles **Akcia na zabezpečenie súladu** Zabezpečuje, že vlastníkom určených súborov a adresára bude skupina bin, sys alebo system.
GEN003760	Vlastníkom súboru services musí byť užívateľ root alebo skupina bin.	**Umiestnenie** /etc/security/pscexpert/dodv2/chowndodfiles **Akcia na zabezpečenie súladu** Zabezpečuje, že vlastníkom určeného súboru bude užívateľ root alebo skupina bin.
GEN003770	Vlastníkom súboru services musí byť skupina bin, sys alebo system.	**Umiestnenie** /etc/security/pscexpert/dodv2/chowndodfiles **Akcia na zabezpečenie súladu** Zabezpečuje, že vlastníkom určeného súboru bude skupina bin, sys alebo system.

Tabuľka 3. Požiadavky Ministerstva obrany USA na vlastníctvo (pokračovanie)

ID kontrolného bodu STIG Ministerstva obrany USA	Popis	Umiestnenie skriptu, v ktorom je definovaná akcia, a výsledky akcie zabezpečujúcej súlad
GEN003920	Vlastníkom súboru hosts.lpd (alebo ekvivalentného) musí byť užívateľ root alebo skupina bin, sys alebo lp.	**Umiestnenie** /etc/security/pscexpert/dodv2/chowndodfiles **Akcia na zabezpečenie súladu** Zabezpečuje, že vlastníkom určeného súboru bude užívateľ root alebo skupina bin, sys alebo lp.
GEN003930	Vlastníkom súboru hosts.lpd (alebo ekvivalentného) musí byť skupina bin, sys alebo system.	**Umiestnenie** /etc/security/pscexpert/dodv2/chowndodfiles **Akcia na zabezpečenie súladu** Zabezpečuje, že vlastníkom určeného súboru bude skupina bin, sys alebo system.
GEN003960	Vlastníkom príkazu **traceroute** musí byť užívateľ root.	**Umiestnenie** /etc/security/pscexpert/dodv2/chowndodfiles **Akcia na zabezpečenie súladu** Zabezpečuje, že vlastníkom príkazu bude užívateľ root.
GEN003980	Vlastníkom príkazu **traceroute** musí byť skupina sys, bin alebo system.	**Umiestnenie** /etc/security/pscexpert/dodv2/chowndodfiles **Akcia na zabezpečenie súladu** Zabezpečuje, že vlastníkom príkazu bude skupina sys, bin alebo system.
GEN004360	Vlastníkom súboru alias musí byť užívateľ root.	**Umiestnenie** /etc/security/pscexpert/dodv2/chowndodfiles **Akcia na zabezpečenie súladu** Zabezpečuje, že vlastníkom určeného súboru bude užívateľ root.
GEN004370	Vlastníkom súboru aliases musí byť skupina sys, bin alebo system.	**Umiestnenie** /etc/security/pscexpert/dodv2/chowndodfiles **Akcia na zabezpečenie súladu** Zabezpečuje, že vlastníkom určeného súboru bude skupina sys, bin alebo system.
GEN004400	Vlastníkom súborov spúšťaných prostredníctvom súboru aliases pošty musí byť užívateľ root a musia sa nachádzať v adresári, ktorého vlastníkom je užívateľ root a iba tento užívateľ môže doň zapisovať.	**Umiestnenie** /etc/security/pscexpert/dodv2/chowndodfiles **Akcia na zabezpečenie súladu** Zabezpečuje, že vlastníkom súborov spúšťaných prostredníctvom súboru aliases pošty bude užívateľ root a že sa tieto súbory budú nachádzať v adresári, ktorého vlastníkom je užívateľ root a iba tento užívateľ môže doň zapisovať.
GEN004410	Vlastníkom súborov spúšťaných prostredníctvom súboru aliases pošty musí byť užívateľ root alebo skupina bin, sys alebo other. Tieto súbory sa musia tiež nachádzať v adresári vlastnenom užívateľom root alebo skupinou bin, sys alebo other.	**Umiestnenie** /etc/security/pscexpert/dodv2/chowndodfiles **Akcia na zabezpečenie súladu** Zabezpečuje, že vlastníkom súborov spúšťaných prostredníctvom súboru aliases pošty bude užívateľ root alebo skupina bin, sys alebo other a že tieto súbory sa budú nachádzať v adresári vlastnenom užívateľom root alebo skupinou bin, sys alebo other.

Tabuľka 3. Požiadavky Ministerstva obrany USA na vlastníctvo (pokračovanie)

ID kontrolného bodu STIG Ministerstva obrany USA	Popis	Umiestnenie skriptu, v ktorom je definovaná akcia, a výsledky akcie zabezpečujúcej súlad
GEN004480	Vlastníkom protokolového súboru služby SMTP musí byť užívateľ root.	**Umiestnenie** /etc/security/pscexpert/dodv2/chowndodfiles **Akcia na zabezpečenie súladu** Zabezpečuje, že vlastníkom určeného súboru bude užívateľ root.
GEN004920	Vlastníkom súboru ftpusers musí byť užívateľ root.	**Umiestnenie** /etc/security/pscexpert/dodv2/chowndodfiles **Akcia na zabezpečenie súladu** Zabezpečuje, že vlastníkom určeného súboru bude užívateľ root.
GEN004930	Vlastníkom súboru ftpusers musí byť skupina bin, sys alebo system.	**Umiestnenie** /etc/security/pscexpert/dodv2/chowndodfiles **Akcia na zabezpečenie súladu** Zabezpečuje, že vlastníkom určeného súboru bude skupina bin, sys alebo system.
GEN005360	Vlastníkom súboru snmpd.conf musí byť užívateľ root.	**Umiestnenie** /etc/security/pscexpert/dodv2/chowndodfiles **Akcia na zabezpečenie súladu** Zabezpečuje, že vlastníkom určeného súboru bude užívateľ root.
GEN005365	Vlastníkom súboru snmpd.conf musí byť skupina bin, sys alebo system.	**Umiestnenie** /etc/security/pscexpert/dodv2/chowndodfiles **Akcia na zabezpečenie súladu** Zabezpečuje, že vlastníkom určeného súboru bude skupina bin, sys alebo system.
GEN005400	Vlastníkom súboru /etc/syslog.conf musí byť užívateľ root.	**Umiestnenie** /etc/security/pscexpert/dodv2/chowndodfiles **Akcia na zabezpečenie súladu** Zabezpečuje, že vlastníkom určeného súboru bude užívateľ root.
GEN005420	Vlastníkom súboru /etc/syslog.conf musí byť skupina bin, sys alebo system.	**Umiestnenie** /etc/security/pscexpert/dodv2/chowndodfiles **Akcia na zabezpečenie súladu** Zabezpečuje, že vlastníkom určeného súboru bude skupina bin, sys alebo system.
GEN005610	V systéme nesmie byť povolené preposielanie IP paketov pre IPv6, pokiaľ systém neslúži ako smerovač IPv6.	**Umiestnenie** /etc/security/pscexpert/dodv2/chowndodfiles **Akcia na zabezpečenie súladu** Zabezpečuje, že v systéme nebude povolené preposielanie IP paketov pre IPv6, pokiaľ systém neslúži ako smerovač IPv6.
GEN005740	Vlastníkom konfiguračného súboru exportu pre NFS musí byť užívateľ root.	**Umiestnenie** /etc/security/pscexpert/dodv2/chowndodfiles **Akcia na zabezpečenie súladu** Zabezpečuje, že vlastníkom určeného súboru bude užívateľ root.

Tabuľka 3. Požiadavky Ministerstva obrany USA na vlastníctvo (pokračovanie)

ID kontrolného bodu STIG Ministerstva obrany USA	Popis	Umiestnenie skriptu, v ktorom je definovaná akcia, a výsledky akcie zabezpečujúcej súlad
GEN005750	Vlastníkom konfiguračného súboru exportu pre NFS musí byť užívateľ root alebo skupina bin, sys alebo system.	**Umiestnenie** /etc/security/pscexpert/dodv2/chowndodfiles **Akcia na zabezpečenie súladu** Zabezpečuje, že vlastníkom určeného súboru bude užívateľ root alebo skupina bin, sys alebo system.
GEN005800	Vlastníkom všetkých systémových súborov a systémových adresárov exportovaných z NFS musí byť užívateľ root.	**Umiestnenie** /etc/security/pscexpert/dodv2/chowndodfiles **Akcia na zabezpečenie súladu** Zabezpečuje, že vlastníkom určeného súboru bude užívateľ root.
GEN005810	Vlastníkom všetkých systémových súborov a systémových adresárov exportovaných z NFS musí byť užívateľ root alebo skupina bin, sys alebo system.	**Umiestnenie** /etc/security/pscexpert/dodv2/chowndodfiles **Akcia na zabezpečenie súladu** Zabezpečuje, že vlastníkom určených súborov a adresárov bude užívateľ root alebo skupina bin, sys alebo system.
GEN006100	Vlastníkom súboru /usr/lib/smb.conf musí byť užívateľ root.	**Umiestnenie** /etc/security/pscexpert/dodv2/chowndodfiles **Akcia na zabezpečenie súladu** Zabezpečuje, že vlastníkom určeného súboru bude užívateľ root.
GEN006120	Vlastníkom súboru /usr/lib/smb.conf musí byť skupina bin, sys alebo system.	**Umiestnenie** /etc/security/pscexpert/dodv2/chowndodfiles **Akcia na zabezpečenie súladu** Zabezpečuje, že vlastníkom určeného súboru bude skupina bin, sys alebo system.
GEN006160	Vlastníkom súboru /var/private/smbpasswd musí byť užívateľ root.	**Umiestnenie** /etc/security/pscexpert/dodv2/chowndodfiles **Akcia na zabezpečenie súladu** Zabezpečuje, že vlastníkom určeného súboru bude užívateľ root.
GEN006180	Vlastníkom súboru /var/private/smbpasswd musí byť skupina sys alebo system.	**Umiestnenie** /etc/security/pscexpert/dodv2/chowndodfiles **Akcia na zabezpečenie súladu** Zabezpečuje, že vlastníkom určeného súboru bude skupina sys alebo system.
GEN006340	Vlastníkom súborov v adresári /etc/news musí byť užívateľ root alebo news.	**Umiestnenie** /etc/security/pscexpert/dodv2/chowndodfiles **Akcia na zabezpečenie súladu** Zabezpečuje, že vlastníkom určeného adresára bude užívateľ root alebo news.
GEN006360	Súbory v priečinku /etc/news musia byť vlastnené skupinou system alebo news.	**Umiestnenie** /etc/security/pscexpert/dodv2/chowndodfiles **Akcia na zabezpečenie súladu** Zabezpečuje, že vlastníkom určených súborov bude skupina system alebo news.

Tabuľka 3. Požiadavky Ministerstva obrany USA na vlastníctvo (pokračovanie)

ID kontrolného bodu STIG Ministerstva obrany USA	Popis	Umiestnenie skriptu, v ktorom je definovaná akcia, a výsledky akcie zabezpečujúcej súlad
GEN008080	Ak sa v systéme používa protokol LDAP na autentifikáciu alebo získanie informácií o konte, vlastníkom súboru /etc/ldap.conf (alebo ekvivalentného) musí byť užívateľ root.	**Umiestnenie** /etc/security/pscexpert/dodv2/chowndodfiles **Akcia na zabezpečenie súladu** Zabezpečuje, že vlastníkom určeného súboru bude užívateľ root.
GEN008100	Ak sa v systéme používa protokol LDAP na autentifikáciu alebo získanie informácií o konte, vlastníkom súboru /etc/ldap.conf (alebo ekvivalentného) musí byť skupina security, bin, sys alebo system.	**Umiestnenie** /etc/security/pscexpert/dodv2/chowndodfiles **Akcia na zabezpečenie súladu** Zabezpečuje, že vlastníkom určeného súboru bude skupina bin, sys alebo system.
GEN008140	Ak sa v systéme používa protokol LDAP na autentifikáciu alebo získanie informácií o konte, vlastníkom súboru certifikačnej autority TLS alebo adresára musí byť užívateľ root.	**Umiestnenie** /etc/security/pscexpert/dodv2/chowndodfiles **Akcia na zabezpečenie súladu** Zabezpečuje, že vlastníkom určeného súboru bude užívateľ root.
GEN008160	Ak sa v systéme používa protokol LDAP na autentifikáciu alebo získanie informácií o konte, vlastníkom súboru certifikačnej autority TLS alebo adresára musí byť užívateľ root alebo skupina bin, sys alebo system.	**Umiestnenie** /etc/security/pscexpert/dodv2/chowndodfiles **Akcia na zabezpečenie súladu** Zabezpečuje, že vlastníkom určeného súboru bude skupina bin, sys alebo system.

Tabuľka 4. Štandardy Ministerstva obrany USA týkajúce sa oprávnení pre súbory

ID kontrolného bodu STIG Ministerstva obrany USA	Popis	Umiestnenie skriptu, v ktorom je definovaná akcia, a výsledky akcie zabezpečujúcej súlad
AIX00100	Súbor /etc/netsvc.conf musí mať režim 0644 alebo prísnejší.	**Umiestnenie** /etc/security/pscexpert/dodv2/fpmdodfiles **Akcia na zabezpečenie súladu** Zabezpečuje, že bude pre súbor nastavený určený alebo prísnejší režim oprávnení.
AIX00340	Súbor /etc/ftpaccess.ctl musí mať režim 0640 alebo prísnejší.	**Umiestnenie** /etc/security/pscexpert/dodv2/fpmdodfiles **Akcia na zabezpečenie súladu** Zabezpečuje, že bude pre súbor nastavený určený alebo prísnejší režim oprávnení.
GEN000252	Konfiguračný súbor synchronizácie času (napríklad /etc/ntp.conf) musí mať režim 0640 alebo prísnejší.	**Umiestnenie** /etc/security/pscexpert/dodv2/fpmdodfiles **Akcia na zabezpečenie súladu** Zabezpečuje, že bude pre súbor nastavený určený alebo prísnejší režim oprávnení.
GEN000920	Domovský adresár konta užívateľa root (iný ako /) musí mať režim 0700.	**Umiestnenie** /etc/security/pscexpert/dodv2/fpmdodfiles **Akcia na zabezpečenie súladu** Zabezpečuje, že bude pre adresár nastavený určený alebo prísnejší režim oprávnení.

Tabuľka 4. Štandardy Ministerstva obrany USA týkajúce sa oprávnení pre súbory (pokračovanie)

ID kontrolného bodu STIG Ministerstva obrany USA	Popis	Umiestnenie skriptu, v ktorom je definovaná akcia, a výsledky akcie zabezpečujúcej súlad
GEN001140	Systémové súbory a adresáre nesmú mať rôzne prístupové oprávnenia.	**Umiestnenie** /etc/security/pscexpert/dodv2/fpmdodfiles **Akcia na zabezpečenie súladu** Zabezpečuje, že prístupové oprávnenie budú konzistentné.
GEN001180	Všetky súbory démonov sieťových služieb musia mať režim 0755 alebo prísnejší.	**Umiestnenie** /etc/security/pscexpert/dodv2/fpmdodfiles **Akcia na zabezpečenie súladu** Zabezpečuje, že bude pre súbory nastavený určený alebo prísnejší režim oprávnení.
GEN001200	Všetky súbory systémových príkazov musia mať režim 0755 alebo prísnejší.	**Umiestnenie** /etc/security/pscexpert/dodv2/fpmdodfiles **Akcia na zabezpečenie súladu** Zabezpečuje, že bude pre súbory nastavený určený alebo prísnejší režim oprávnení.
GEN001260	Systémové protokolové súbory musia mať režim 0640 alebo prísnejší.	**Umiestnenie** /etc/security/pscexpert/dodv2/fpmdodfiles **Akcia na zabezpečenie súladu** Zabezpečuje, že bude pre súbory nastavený určený alebo prísnejší režim oprávnení.
GEN001280	Súbory stránok manuálu musia mať režim 0644 alebo prísnejší.	**Umiestnenie** /etc/security/pscexpert/dodv2/fpmdodfiles **Akcia na zabezpečenie súladu** Zabezpečuje, že bude pre súbory nastavený určený alebo prísnejší režim oprávnení.
GEN001300	Súbory knižníc musia mať režim 0755 alebo prísnejší.	**Umiestnenie** /etc/security/pscexpert/dodv2/fpmdodfiles **Akcia na zabezpečenie súladu** Zabezpečuje, že bude pre súbory nastavený určený alebo prísnejší režim oprávnení.
GEN001360	Súbory NIS/NIS+/yp musia mať režim 0755 alebo prísnejší.	**Umiestnenie** /etc/security/pscexpert/dodv2/fpmdodfiles **Akcia na zabezpečenie súladu** Zabezpečuje, že bude pre súbory nastavený určený alebo prísnejší režim oprávnení.
GEN001364	Súbor /etc/resolv.conf musí mať režim 0644 alebo prísnejší.	**Umiestnenie** /etc/security/pscexpert/dodv2/fpmdodfiles **Akcia na zabezpečenie súladu** Zabezpečuje, že bude pre súbor nastavený určený alebo prísnejší režim oprávnení.
GEN001368	Súbor /etc/hosts musí mať režim 0644 alebo prísnejší.	**Umiestnenie** /etc/security/pscexpert/dodv2/fpmdodfiles **Akcia na zabezpečenie súladu** Zabezpečuje, že bude pre súbor nastavený určený alebo prísnejší režim oprávnení.

Tabuľka 4. Štandardy Ministerstva obrany USA týkajúce sa oprávnení pre súbory (pokračovanie)

ID kontrolného bodu STIG Ministerstva obrany USA	Popis	Umiestnenie skriptu, v ktorom je definovaná akcia, a výsledky akcie zabezpečujúcej súlad
GEN001373	Súbor /etc/nsswitch.conf musí mať režim 0644 alebo prísnejší.	**Umiestnenie** /etc/security/pscexpert/dodv2/fpmdodfiles **Akcia na zabezpečenie súladu** Zabezpečuje, že bude pre súbor nastavený určený alebo prísnejší režim oprávnení.
GEN001380	Súbor /etc/passwd musí mať režim 0644 alebo prísnejší.	**Umiestnenie** /etc/security/pscexpert/dodv2/fpmdodfiles **Akcia na zabezpečenie súladu** Zabezpečuje, že bude pre súbor nastavený určený alebo prísnejší režim oprávnení.
GEN001393	Súbor /etc/group musí mať režim 0644 alebo prísnejší.	**Umiestnenie** /etc/security/pscexpert/dodv2/fpmdodfiles **Akcia na zabezpečenie súladu** Zabezpečuje, že bude pre súbor nastavený určený alebo prísnejší režim oprávnení.
GEN001420	Súbor /etc/security/passwd musí mať režim 0400.	**Umiestnenie** /etc/security/pscexpert/dodv2/fpmdodfiles **Akcia na zabezpečenie súladu** Zabezpečuje, že bude pre súbor nastavený určený alebo prísnejší režim oprávnení.
GEN001480	Všetky domovské adresáre užívateľov musia mať režim 0750 alebo prísnejší.	**Umiestnenie** /etc/security/pscexpert/dodv2/fpmdodfiles **Akcia na zabezpečenie súladu** Zabezpečuje, že bude pre súbor nastavený určený alebo prísnejší režim oprávnení.
GEN001560	Všetky súbory a adresáre uložené v domovských adresároch užívateľov musia mať režim 0750 alebo prísnejší.	**Umiestnenie** /etc/security/pscexpert/dodv2/fpmdodfiles **Akcia na zabezpečenie súladu** Zabezpečuje, že bude pre súbory nastavený určený alebo prísnejší režim oprávnení.
GEN001580	Všetky skripty riadenia spúšťania musia mať režim 0755 alebo prísnejší.	**Umiestnenie** /etc/security/pscexpert/dodv2/fpmdodfiles **Akcia na zabezpečenie súladu** Zabezpečuje, že bude pre súbory nastavený určený alebo prísnejší režim oprávnení.
GEN001640	Skripty na riadenie spúšťania sa nesmú spúšťať v rámci globálne zapisovateľných programov alebo skriptov.	**Umiestnenie** /etc/security/pscexpert/dodv2/fpmdodfiles **Akcia na zabezpečenie súladu** Skontroluje globálne zapisovateľné programy alebo skripty v programoch, ako je napríklad cron.
GEN001720	Všetky globálne inicializačné súbory musia mať režim 0644 alebo prísnejší.	**Umiestnenie** /etc/security/pscexpert/dodv2/fpmdodfiles **Akcia na zabezpečenie súladu** Zabezpečuje, že bude pre súbory nastavený určený alebo prísnejší režim oprávnení.

Tabuľka 4. Štandardy Ministerstva obrany USA týkajúce sa oprávnení pre súbory (pokračovanie)

ID kontrolného bodu STIG Ministerstva obrany USA	Popis	Umiestnenie skriptu, v ktorom je definovaná akcia, a výsledky akcie zabezpečujúcej súlad
GEN001800	Všetky skeletové súbory (ako sú súbory v adresári /etc/skel) musia mať režim 0644 alebo prísnejší.	**Umiestnenie** /etc/security/pscexpert/dodv2/fpmdodfiles **Akcia na zabezpečenie súladu** Zabezpečuje, že bude pre súbory nastavený určený alebo prísnejší režim oprávnení.
GEN001880	Všetky lokálne inicializačné súbory musia mať režim 0740 alebo prísnejší.	**Umiestnenie** /etc/security/pscexpert/dodv2/fpmdodfiles **Akcia na zabezpečenie súladu** Zabezpečuje, že bude pre súbory nastavený určený alebo prísnejší režim oprávnení.
GEN002220	Všetky súbory prostredia shell musia mať režim 0755 alebo prísnejší.	**Umiestnenie** /etc/security/pscexpert/dodv2/fpmdodfiles **Akcia na zabezpečenie súladu** Zabezpečuje, že bude pre súbory nastavený určený alebo prísnejší režim oprávnení.
GEN002320	Zvukové zariadenia musia mať režim 0660 alebo prísnejší.	**Umiestnenie** /etc/security/pscexpert/dodv2/fpmdodfiles **Akcia na zabezpečenie súladu** Zabezpečuje, že pre zvukové zariadenia bude nastavený určený alebo prísnejší režim oprávnení.
GEN002560	Predvolená hodnota systémového aj užívateľského parametra **umask** musí byť 077.	**Umiestnenie** /etc/security/pscexpert/dodv2/fpmdodfiles **Akcia na zabezpečenie súladu** Zabezpečuje, že určené nastavenie bude *077*.
GEN002700	Protokoly z auditu systému musia mať režim 0640 alebo prísnejší.	**Umiestnenie** /etc/security/pscexpert/dodv2/fpmdodfiles **Akcia na zabezpečenie súladu** Zabezpečuje, že bude pre súbory nastavený určený alebo prísnejší režim oprávnení.
GEN002717	Spustiteľné súbory nástroja auditu systému musia mať režim 0750 alebo prísnejší.	**Umiestnenie** /etc/security/pscexpert/dodv2/fpmdodfiles **Akcia na zabezpečenie súladu** Zabezpečuje, že bude pre súbory nastavený určený alebo prísnejší režim oprávnení.
GEN002980	Súbor cron.allow musí mať režim 0600 alebo prísnejší.	**Umiestnenie** /etc/security/pscexpert/dodv2/fpmdodfiles **Akcia na zabezpečenie súladu** Zabezpečuje, že bude pre súbor nastavený určený alebo prísnejší režim oprávnení.
GEN003080	S/bory crontab musia mať režim 0600 alebo prísnejší.	**Umiestnenie** /etc/security/pscexpert/dodv2/fpmdodfiles **Akcia na zabezpečenie súladu** Zabezpečuje, že bude pre súbory nastavený určený alebo prísnejší režim oprávnení.

Tabuľka 4. Štandardy Ministerstva obrany USA týkajúce sa oprávnení pre súbory (pokračovanie)

ID kontrolného bodu STIG Ministerstva obrany USA	Popis	Umiestnenie skriptu, v ktorom je definovaná akcia, a výsledky akcie zabezpečujúcej súlad
GEN003090	Súbory ccrontab nesmú mať rozšírené zoznamy riadenia prístupu (ACL).	**Umiestnenie** /etc/security/pscexpert/dodv2/fpmdodfiles **Akcia na zabezpečenie súladu** Zabezpečuje, že určené súbory nebudú mať rozšírené súbory ACL.
GEN003100	Adresáre cron a crontab musia mať režim 0755 alebo prísnejší.	**Umiestnenie** /etc/security/pscexpert/dodv2/fpmdodfiles **Akcia na zabezpečenie súladu** Zabezpečuje, že pre určené adresáre bude nastavený určený alebo prísnejší režim oprávnení.
GEN003180	Súbor cronlog musí mať režim 0600 alebo prísnejší.	**Umiestnenie** /etc/security/pscexpert/dodv2/fpmdodfiles **Akcia na zabezpečenie súladu** Zabezpečuje, že bude pre súbor nastavený určený alebo prísnejší režim oprávnení.
GEN003200	Súbor cron.deny musí mať režim 0600 alebo prísnejší.	**Umiestnenie** /etc/security/pscexpert/dodv2/fpmdodfiles **Akcia na zabezpečenie súladu** Zabezpečuje, že bude pre súbor nastavený určený alebo prísnejší režim oprávnení.
GEN003252	Súbor at.deny musí mať režim 0640 alebo prísnejší.	**Umiestnenie** /etc/security/pscexpert/dodv2/fpmdodfiles **Akcia na zabezpečenie súladu** Zabezpečuje, že bude pre súbor nastavený určený alebo prísnejší režim oprávnení.
GEN003340	Súbor at.allow musí mať režim 0600 alebo prísnejší.	**Umiestnenie** /etc/security/pscexpert/dodv2/fpmdodfiles **Akcia na zabezpečenie súladu** Zabezpečuje, že bude pre súbor nastavený určený alebo prísnejší režim oprávnení.
GEN003400	Adresár at musí mať režim 0755 alebo prísnejší.	**Umiestnenie** /etc/security/pscexpert/dodv2/fpmdodfiles **Akcia na zabezpečenie súladu** Zabezpečuje, že bude pre adresár nastavený určený alebo prísnejší režim oprávnení.
GEN003440	Úlohy at nesmú nastavovať menej prísnu hodnotu pre parameter **umask** ako 077.	**Umiestnenie** /etc/security/pscexpert/dodv2/fpmdodfiles **Akcia na zabezpečenie súladu** Zabezpečuje, že pre parameter bude nastavený určený alebo prísnejší režim oprávnení.
GEN003740	Súbory inetd.conf a xinetd.conf musia mať režim 0440 alebo prísnejší.	**Umiestnenie** /etc/security/pscexpert/dodv2/fpmdodfiles **Akcia na zabezpečenie súladu** Zabezpečuje, že bude pre súbory nastavený určený alebo prísnejší režim oprávnení.

Tabuľka 4. Štandardy Ministerstva obrany USA týkajúce sa oprávnení pre súbory (pokračovanie)

ID kontrolného bodu STIG Ministerstva obrany USA	Popis	Umiestnenie skriptu, v ktorom je definovaná akcia, a výsledky akcie zabezpečujúcej súlad
GEN003780	Súbor services musí mať režim 0444 alebo prísnejší.	**Umiestnenie** /etc/security/pscexpert/dodv2/fpmdodfiles **Akcia na zabezpečenie súladu** Zabezpečuje, že bude pre súbor nastavený určený alebo prísnejší režim oprávnení.
GEN003940	Súbor hosts.lpd (alebo ekvivalentný) musí mať režim 0644 alebo prísnejší.	**Umiestnenie** /etc/security/pscexpert/dodv2/fpmdodfiles **Akcia na zabezpečenie súladu** Zabezpečuje, že bude pre súbor nastavený určený alebo prísnejší režim oprávnení.
GEN004000	Súbor traceroute musí mať režim 0700 alebo prísnejší.	**Umiestnenie** /etc/security/pscexpert/dodv2/fpmdodfiles **Akcia na zabezpečenie súladu** Zabezpečuje, že bude pre súbor nastavený určený alebo prísnejší režim oprávnení.
GEN004380	Súbor alias musí mať režim 0644 alebo prísnejší.	**Umiestnenie** /etc/security/pscexpert/dodv2/fpmdodfiles **Akcia na zabezpečenie súladu** Zabezpečuje, že bude pre súbor nastavený určený alebo prísnejší režim oprávnení.
GEN004420	Súbory, ktoré sa spúšťajú prostredníctvom súboru aliases pošty musia mať režim 0755 alebo prísnejší.	**Umiestnenie** /etc/security/pscexpert/dodv2/fpmdodfiles **Akcia na zabezpečenie súladu** Zabezpečuje, že bude pre súbory nastavený určený alebo prísnejší režim oprávnení.
GEN004500	Protokolový súbor služby SMTP musí mať režim 0644 alebo prísnejší.	**Umiestnenie** /etc/security/pscexpert/dodv2/fpmdodfiles **Akcia na zabezpečenie súladu** Zabezpečuje, že bude pre súbor nastavený určený alebo prísnejší režim oprávnení.
GEN004940	Súbor ftpusers musí mať režim 0640 alebo prísnejší.	**Umiestnenie** /etc/security/pscexpert/dodv2/fpmdodfiles **Akcia na zabezpečenie súladu** Zabezpečuje, že bude pre súbor nastavený určený alebo prísnejší režim oprávnení.
GEN005040	Všetci užívatelia FTP musia mať predvolené nastavenie parametra **umask** s hodnotou 077.	**Umiestnenie** /etc/security/pscexpert/dodv2/fpmdodfiles **Akcia na zabezpečenie súladu** Zabezpečuje správne nastavenie.
GEN005100	Démon TFTP musí mať režim 0755 alebo prísnejší.	**Umiestnenie** /etc/security/pscexpert/dodv2/fpmdodfiles **Akcia na zabezpečenie súladu** Zabezpečuje, že démon bude mať určený režim alebo prísnejší.

Tabuľka 4. Štandardy Ministerstva obrany USA týkajúce sa oprávnení pre súbory (pokračovanie)

ID kontrolného bodu STIG Ministerstva obrany USA	Popis	Umiestnenie skriptu, v ktorom je definovaná akcia, a výsledky akcie zabezpečujúcej súlad
GEN005180	Všetky súbory .Xauthority musia mať režim 0600 alebo prísnejší.	**Umiestnenie** /etc/security/pscexpert/dodv2/fpmdodfiles **Akcia na zabezpečenie súladu** Zabezpečuje, že bude pre súbory nastavený určený alebo prísnejší režim oprávnení.
GEN005320	Súbor snmpd.conf musí mať režim 0600 alebo prísnejší.	**Umiestnenie** /etc/security/pscexpert/dodv2/fpmdodfiles **Akcia na zabezpečenie súladu** Zabezpečuje, že bude pre súbor nastavený určený alebo prísnejší režim oprávnení.
GEN005340	Súbory MIB (Management Information Base) musia mať režim 0640 alebo prísnejší.	**Umiestnenie** /etc/security/pscexpert/dodv2/fpmdodfiles **Akcia na zabezpečenie súladu** Zabezpečuje, že bude pre súbory nastavený určený alebo prísnejší režim oprávnení.
GEN005390	Súbor /etc/syslog.conf musí mať režim 0640 alebo prísnejší.	**Umiestnenie** /etc/security/pscexpert/dodv2/fpmdodfiles **Akcia na zabezpečenie súladu** Zabezpečuje, že bude pre súbor nastavený určený alebo prísnejší režim oprávnení.
GEN005522	Súbory verejného hostiteľského kľúča SSH musia mať režim 0644 alebo prísnejší.	**Umiestnenie** /etc/security/pscexpert/dodv2/fpmdodfiles **Akcia na zabezpečenie súladu** Zabezpečuje, že bude pre súbory nastavený určený alebo prísnejší režim oprávnení.
GEN005523	Súbory verejného hostiteľského kľúča SSH musia mať režim 0600 alebo prísnejší.	**Umiestnenie** /etc/security/pscexpert/dodv2/fpmdodfiles **Akcia na zabezpečenie súladu** Zabezpečuje, že bude pre súbory nastavený určený alebo prísnejší režim oprávnení.
GEN006140	Súbor /usr/lib/smb.conf musí mať režim 0644 alebo prísnejší.	**Umiestnenie** /etc/security/pscexpert/dodv2/fpmdodfiles **Akcia na zabezpečenie súladu** Zabezpečuje, že bude pre súbor nastavený určený alebo prísnejší režim oprávnení.
GEN006200	Súbor /var/private/smbpasswd musí mať režim 0600 alebo prísnejší.	**Umiestnenie** /etc/security/pscexpert/dodv2/fpmdodfiles **Akcia na zabezpečenie súladu** Zabezpečuje, že bude pre súbor nastavený určený alebo prísnejší režim oprávnení.
GEN006260	Súbor /etc/news/hosts.nntp (alebo ekvivalentný) musí mať režim 0600 alebo prísnejší.	**Umiestnenie** /etc/security/pscexpert/dodv2/fpmdodfiles **Akcia na zabezpečenie súladu** Zabezpečuje, že bude pre súbor nastavený určený alebo prísnejší režim oprávnení.

Tabuľka 4. Štandardy Ministerstva obrany USA týkajúce sa oprávnení pre súbory (pokračovanie)

ID kontrolného bodu STIG Ministerstva obrany USA	Popis	Umiestnenie skriptu, v ktorom je definovaná akcia, a výsledky akcie zabezpečujúcej súlad
GEN006280	Súbor /etc/news/hosts.nntp.nolimit (alebo ekvivalentný) musí mať režim 0600 alebo prísnejší.	**Umiestnenie** /etc/security/pscexpert/dodv2/fpmdodfiles **Akcia na zabezpečenie súladu** Zabezpečuje, že bude pre súbor nastavený určený alebo prísnejší režim oprávnení.
GEN006300	Súbor /etc/news/nnrp.access (alebo ekvivalentný) musí mať režim 0600 alebo prísnejší.	**Umiestnenie** /etc/security/pscexpert/dodv2/fpmdodfiles **Akcia na zabezpečenie súladu** Zabezpečuje, že bude pre súbor nastavený určený alebo prísnejší režim oprávnení.
GEN006320	Súbor /etc/news/passwd.nntp (alebo ekvivalentný) musí mať režim 0600 alebo prísnejší.	**Umiestnenie** /etc/security/pscexpert/dodv2/fpmdodfiles **Akcia na zabezpečenie súladu** Zabezpečuje, že bude pre súbor nastavený určený alebo prísnejší režim oprávnení.
GEN008060	Ak sa v systéme používa protokol LDAP na autentifikáciu alebo získanie informácií o konte, súbor /etc/ldap.conf (alebo ekvivalentný) musí mať režim 0644 alebo prísnejší.	**Umiestnenie** /etc/security/pscexpert/dodv2/fpmdodfiles **Akcia na zabezpečenie súladu** Zabezpečuje, že bude pre súbor nastavený určený alebo prísnejší režim oprávnení.
GEN008180	Ak sa v systéme používa protokol LDAP na autentifikáciu alebo získanie informácií o konte, súbor alebo adresár certifikačnej autority TLS musia mať režim 0644 (0755 v prípade adresára) alebo prísnejší.	**Umiestnenie** /etc/security/pscexpert/dodv2/fpmdodfiles **Akcia na zabezpečenie súladu** Zabezpečuje, že pre určené súbory alebo adresáre bude nastavený určený alebo prísnejší režim oprávnení.

Tabuľka 5. Požiadavky Ministerstva obrany USA na zoznamy riadenia prístupu (ACL)

ID kontrolného bodu STIG Ministerstva obrany USA	Popis	Umiestnenie skriptu, v ktorom je definovaná akcia, a výsledky akcie zabezpečujúcej súlad
AIX00110	Súbor /etc/netsvc.conf nesmie mať rozšírený zoznam riadenia prístupu.	**Umiestnenie** /etc/security/pscexpert/dodv2/acldodfiles **Akcia na zabezpečenie súladu** Zakáže určený rozšírený zoznam ACL. **Poznámka:** Toto nastavenie nebude automaticky zmenené pri obnovení predvolenej politiky systému AIX prostredníctvom súboru DoDv2_to_AIXDefault.xml. Toto nastavenie je potrebné manuálne zmeniť.

Tabuľka 5. Požiadavky Ministerstva obrany USA na zoznamy riadenia prístupu (ACL) (pokračovanie)

ID kontrolného bodu STIG Ministerstva obrany USA	Popis	Umiestnenie skriptu, v ktorom je definovaná akcia, a výsledky akcie zabezpečujúcej súlad
AIX00350	Súbor /etc/ftpaccess.ctl nesmie mať rozšírený zoznam riadenia prístupu.	**Umiestnenie** /etc/security/pscexpert/dodv2/acldodfiles **Akcia na zabezpečenie súladu** Zakáže určený rozšírený zoznam ACL. **Poznámka:** Toto nastavenie nebude automaticky zmenené pri obnovení predvolenej politiky systému AIX prostredníctvom súboru DoDv2_to_AIXDefault.xml. Toto nastavenie je potrebné manuálne zmeniť.
GEN000253	Konfiguračný súbor synchronizácie času (napríklad /etc/ntp.conf) nesmie mať rozšírený zoznam ACL.	**Umiestnenie** /etc/security/pscexpert/dodv2/acldodfiles **Akcia na zabezpečenie súladu** Zakáže určený rozšírený zoznam ACL. **Poznámka:** Toto nastavenie nebude automaticky zmenené pri obnovení predvolenej politiky systému AIX prostredníctvom súboru DoDv2_to_AIXDefault.xml. Toto nastavenie je potrebné manuálne zmeniť.
GEN000930	Domovský adresár konta užívateľa root nesmie mať rozšírený zoznam ACL.	**Umiestnenie** /etc/security/pscexpert/dodv2/acldodfiles **Akcia na zabezpečenie súladu** Zakáže určený rozšírený zoznam ACL. **Poznámka:** Toto nastavenie nebude automaticky zmenené pri obnovení predvolenej politiky systému AIX prostredníctvom súboru DoDv2_to_AIXDefault.xml. Toto nastavenie je potrebné manuálne zmeniť.
GEN001190	Žiadne súbory démonov sieťových služieb nesmú mať rozšírené zoznamy riadenia prístupu.	**Umiestnenie** /etc/security/pscexpert/dodv2/acldodfiles **Akcia na zabezpečenie súladu** Zakáže určený rozšírený zoznam ACL. **Poznámka:** Toto nastavenie nebude automaticky zmenené pri obnovení predvolenej politiky systému AIX prostredníctvom súboru DoDv2_to_AIXDefault.xml. Toto nastavenie je potrebné manuálne zmeniť.
GEN001210	Žiadne súbory systémových príkazov nesmú mať rozšírené zoznamy riadenia prístupu.	**Umiestnenie** /etc/security/pscexpert/dodv2/acldodfiles **Akcia na zabezpečenie súladu** Zakáže určený rozšírený zoznam ACL. **Poznámka:** Toto nastavenie nebude automaticky zmenené pri obnovení predvolenej politiky systému AIX prostredníctvom súboru DoDv2_to_AIXDefault.xml. Toto nastavenie je potrebné manuálne zmeniť.

Tabuľka 5. Požiadavky Ministerstva obrany USA na zoznamy riadenia prístupu (ACL) (pokračovanie)

ID kontrolného bodu STIG Ministerstva obrany USA	Popis	Umiestnenie skriptu, v ktorom je definovaná akcia, a výsledky akcie zabezpečujúcej súlad
GEN001270	Systémové protokolové súbory nesmú mať rozšírené zoznamy riadenia prístupu, pokiaľ nie sú vyžadované na podporu autorizovaného softvéru.	**Umiestnenie** /etc/security/pscexpert/dodv2/acldodfiles **Akcia na zabezpečenie súladu** Zakáže určený rozšírený zoznam ACL. **Poznámka:** Toto nastavenie nebude automaticky zmenené pri obnovení predvolenej politiky systému AIX prostredníctvom súboru DoDv2_to_AIXDefault.xml. Toto nastavenie je potrebné manuálne zmeniť.
GEN001310	Žiadne súbory knižníc nesmú mať rozšírené zoznamy riadenia prístupu.	**Umiestnenie** /etc/security/pscexpert/dodv2/acldodfiles **Akcia na zabezpečenie súladu** Zakáže určený rozšírený zoznam ACL. **Poznámka:** Toto nastavenie nebude automaticky zmenené pri obnovení predvolenej politiky systému AIX prostredníctvom súboru DoDv2_to_AIXDefault.xml. Toto nastavenie je potrebné manuálne zmeniť.
GEN001361	Súbory príkazov NIS/NIS+/yp nesmú mať rozšírené zoznamy riadenia prístupu.	**Umiestnenie** /etc/security/pscexpert/dodv2/acldodfiles **Akcia na zabezpečenie súladu** Zakáže určený rozšírený zoznam ACL. **Poznámka:** Toto nastavenie nebude automaticky zmenené pri obnovení predvolenej politiky systému AIX prostredníctvom súboru DoDv2_to_AIXDefault.xml. Toto nastavenie je potrebné manuálne zmeniť.
GEN001365	Súbor /etc/resolv.conf nesmie mať rozšírený zoznam riadenia prístupu.	**Umiestnenie** /etc/security/pscexpert/dodv2/acldodfiles **Akcia na zabezpečenie súladu** Zakáže určený rozšírený zoznam ACL. **Poznámka:** Toto nastavenie nebude automaticky zmenené pri obnovení predvolenej politiky systému AIX prostredníctvom súboru DoDv2_to_AIXDefault.xml. Toto nastavenie je potrebné manuálne zmeniť.
GEN001369	Súbor /etc/hosts nesmie mať rozšírený zoznam riadenia prístupu.	**Umiestnenie** /etc/security/pscexpert/dodv2/acldodfiles **Akcia na zabezpečenie súladu** Zakáže určený rozšírený zoznam ACL. **Poznámka:** Toto nastavenie nebude automaticky zmenené pri obnovení predvolenej politiky systému AIX prostredníctvom súboru DoDv2_to_AIXDefault.xml. Toto nastavenie je potrebné manuálne zmeniť.

Tabuľka 5. Požiadavky Ministerstva obrany USA na zoznamy riadenia prístupu (ACL) (pokračovanie)

ID kontrolného bodu STIG Ministerstva obrany USA	Popis	Umiestnenie skriptu, v ktorom je definovaná akcia, a výsledky akcie zabezpečujúcej súlad
GEN001374	Súbor /etc/nsswitch.conf nesmie mať rozšírený zoznam riadenia prístupu.	**Umiestnenie** /etc/security/pscexpert/dodv2/acldodfiles **Akcia na zabezpečenie súladu** Zakáže určený rozšírený zoznam ACL. **Poznámka:** Toto nastavenie nebude automaticky zmenené pri obnovení predvolenej politiky systému AIX prostredníctvom súboru DoDv2_to_AIXDefault.xml. Toto nastavenie je potrebné manuálne zmeniť.
GEN001390	Súbor /etc/passwd nesmie mať rozšírený zoznam riadenia prístupu.	**Umiestnenie** /etc/security/pscexpert/dodv2/acldodfiles **Akcia na zabezpečenie súladu** Zakáže určený rozšírený zoznam ACL. **Poznámka:** Toto nastavenie nebude automaticky zmenené pri obnovení predvolenej politiky systému AIX prostredníctvom súboru DoDv2_to_AIXDefault.xml. Toto nastavenie je potrebné manuálne zmeniť.
GEN001394	Súbor /etc/group nesmie mať rozšírený zoznam riadenia prístupu.	**Umiestnenie** /etc/security/pscexpert/dodv2/acldodfiles **Akcia na zabezpečenie súladu** Zakáže určený rozšírený zoznam ACL. **Poznámka:** Toto nastavenie nebude automaticky zmenené pri obnovení predvolenej politiky systému AIX prostredníctvom súboru DoDv2_to_AIXDefault.xml. Toto nastavenie je potrebné manuálne zmeniť.
GEN001430	Súbor /etc/security/passwd nesmie mať rozšírený zoznam riadenia prístupu.	**Umiestnenie** /etc/security/pscexpert/dodv2/acldodfiles **Akcia na zabezpečenie súladu** Zakáže určený rozšírený zoznam ACL. **Poznámka:** Toto nastavenie nebude automaticky zmenené pri obnovení predvolenej politiky systému AIX prostredníctvom súboru DoDv2_to_AIXDefault.xml. Toto nastavenie je potrebné manuálne zmeniť.
GEN001570	Žiadne súbory ani adresáre pod domovskými adresármi užívateľov nesmú mať rozšírené zoznamy riadenia prístupu.	**Umiestnenie** /etc/security/pscexpert/dodv2/acldodfiles **Akcia na zabezpečenie súladu** Zakáže určený rozšírený zoznam ACL. **Poznámka:** Toto nastavenie nebude automaticky zmenené pri obnovení predvolenej politiky systému AIX prostredníctvom súboru DoDv2_to_AIXDefault.xml. Toto nastavenie je potrebné manuálne zmeniť.

Tabuľka 5. Požiadavky Ministerstva obrany USA na zoznamy riadenia prístupu (ACL) (pokračovanie)

ID kontrolného bodu STIG Ministerstva obrany USA	Popis	Umiestnenie skriptu, v ktorom je definovaná akcia, a výsledky akcie zabezpečujúcej súlad
GEN001590	Žiadne skripty riadenia spúšťania nesmú mať rozšírené zoznamy riadenia prístupu.	**Umiestnenie** /etc/security/pscexpert/dodv2/acldodfiles **Akcia na zabezpečenie súladu** Zakáže určený rozšírený zoznam ACL. **Poznámka:** Toto nastavenie nebude automaticky zmenené pri obnovení predvolenej politiky systému AIX prostredníctvom súboru DoDv2_to_AIXDefault.xml. Toto nastavenie je potrebné manuálne zmeniť.
GEN001730	Žiadne globálne inicializačné súbory nesmú mať rozšírené zoznamy riadenia prístupu.	**Umiestnenie** /etc/security/pscexpert/dodv2/acldodfiles **Akcia na zabezpečenie súladu** Zakáže určený rozšírený zoznam ACL. **Poznámka:** Toto nastavenie nebude automaticky zmenené pri obnovení predvolenej politiky systému AIX prostredníctvom súboru DoDv2_to_AIXDefault.xml. Toto nastavenie je potrebné manuálne zmeniť.
GEN001810	Skeletové súbory nesmú mať rozšírené zoznamy riadenia prístupu.	**Umiestnenie** /etc/security/pscexpert/dodv2/acldodfiles **Akcia na zabezpečenie súladu** Zakáže určený rozšírený zoznam ACL. **Poznámka:** Toto nastavenie nebude automaticky zmenené pri obnovení predvolenej politiky systému AIX prostredníctvom súboru DoDv2_to_AIXDefault.xml. Toto nastavenie je potrebné manuálne zmeniť.
GEN001890	Lokálne inicializačné súbory nesmú mať rozšírené zoznamy riadenia prístupu.	**Umiestnenie** /etc/security/pscexpert/dodv2/acldodfiles **Akcia na zabezpečenie súladu** Zakáže určený rozšírený zoznam ACL. **Poznámka:** Toto nastavenie nebude automaticky zmenené pri obnovení predvolenej politiky systému AIX prostredníctvom súboru DoDv2_to_AIXDefault.xml. Toto nastavenie je potrebné manuálne zmeniť.
GEN002230	Žiadne súbory prostredia shell nesmú mať rozšírené zoznamy riadenia prístupu.	**Umiestnenie** /etc/security/pscexpert/dodv2/acldodfiles **Akcia na zabezpečenie súladu** Zakáže určený rozšírený zoznam ACL. **Poznámka:** Toto nastavenie nebude automaticky zmenené pri obnovení predvolenej politiky systému AIX prostredníctvom súboru DoDv2_to_AIXDefault.xml. Toto nastavenie je potrebné manuálne zmeniť.

Tabuľka 5. Požiadavky Ministerstva obrany USA na zoznamy riadenia prístupu (ACL) (pokračovanie)

ID kontrolného bodu STIG Ministerstva obrany USA	Popis	Umiestnenie skriptu, v ktorom je definovaná akcia, a výsledky akcie zabezpečujúcej súlad
GEN002330	Audio zariadenia nesmú mať rozšírené zoznamy riadenia prístupu.	**Umiestnenie** /etc/security/pscexpert/dodv2/acldodfiles **Akcia na zabezpečenie súladu** Zakáže určený rozšírený zoznam ACL. **Poznámka:** Toto nastavenie nebude automaticky zmenené pri obnovení predvolenej politiky systému AIX prostredníctvom súboru DoDv2_to_AIXDefault.xml. Toto nastavenie je potrebné manuálne zmeniť.
GEN002710	Žiadne súbory z auditu systému nesmú mať rozšírené zoznamy riadenia prístupu.	**Umiestnenie** /etc/security/pscexpert/dodv2/acldodfiles **Akcia na zabezpečenie súladu** Zakáže určený rozšírený zoznam ACL. **Poznámka:** Toto nastavenie nebude automaticky zmenené pri obnovení predvolenej politiky systému AIX prostredníctvom súboru DoDv2_to_AIXDefault.xml. Toto nastavenie je potrebné manuálne zmeniť.
GEN002990	Rozšírené zoznamy riadenia prístupu musia byť zakázané pre súbory cron.allow a cron.deny.	**Umiestnenie** /etc/security/pscexpert/dodv2/acldodfiles **Akcia na zabezpečenie súladu** Zakáže určený rozšírený zoznam ACL. **Poznámka:** Toto nastavenie nebude automaticky zmenené pri obnovení predvolenej politiky systému AIX prostredníctvom súboru DoDv2_to_AIXDefault.xml. Toto nastavenie je potrebné manuálne zmeniť.
GEN003090	Súbory crontab nesmú mať rozšírené zoznamy riadenia prístupu.	**Umiestnenie** /etc/security/pscexpert/dodv2/acldodfiles **Akcia na zabezpečenie súladu** Zakáže určený rozšírený zoznam ACL. **Poznámka:** Toto nastavenie nebude automaticky zmenené pri obnovení predvolenej politiky systému AIX prostredníctvom súboru DoDv2_to_AIXDefault.xml. Toto nastavenie je potrebné manuálne zmeniť.
GEN003110	Adresáre cron a crontab nesmú mať rozšírené zoznamy riadenia prístupu.	**Umiestnenie** /etc/security/pscexpert/dodv2/acldodfiles **Akcia na zabezpečenie súladu** Zakáže určený rozšírený zoznam ACL. **Poznámka:** Toto nastavenie nebude automaticky zmenené pri obnovení predvolenej politiky systému AIX prostredníctvom súboru DoDv2_to_AIXDefault.xml. Toto nastavenie je potrebné manuálne zmeniť.

Tabuľka 5. Požiadavky Ministerstva obrany USA na zoznamy riadenia prístupu (ACL) (pokračovanie)

ID kontrolného bodu STIG Ministerstva obrany USA	Popis	Umiestnenie skriptu, v ktorom je definovaná akcia, a výsledky akcie zabezpečujúcej súlad
GEN003190	Protokolové súbory programu cron nesmú mať rozšírené zoznamy riadenia prístupu.	**Umiestnenie** /etc/security/pscexpert/dodv2/acldodfiles **Akcia na zabezpečenie súladu** Zakáže určený rozšírený zoznam ACL. **Poznámka:** Toto nastavenie nebude automaticky zmenené pri obnovení predvolenej politiky systému AIX prostredníctvom súboru DoDv2_to_AIXDefault.xml. Toto nastavenie je potrebné manuálne zmeniť.
GEN003210	Súbor cron.deny nesmie mať rozšírený zoznam riadenia prístupu.	**Umiestnenie** /etc/security/pscexpert/dodv2/acldodfiles **Akcia na zabezpečenie súladu** Zakáže určený rozšírený zoznam ACL. **Poznámka:** Toto nastavenie nebude automaticky zmenené pri obnovení predvolenej politiky systému AIX prostredníctvom súboru DoDv2_to_AIXDefault.xml. Toto nastavenie je potrebné manuálne zmeniť.
GEN003245	Súbor at.allow nesmie mať rozšírený zoznam riadenia prístupu.	**Umiestnenie** /etc/security/pscexpert/dodv2/acldodfiles **Akcia na zabezpečenie súladu** Zakáže určený rozšírený zoznam ACL. **Poznámka:** Toto nastavenie nebude automaticky zmenené pri obnovení predvolenej politiky systému AIX prostredníctvom súboru DoDv2_to_AIXDefault.xml. Toto nastavenie je potrebné manuálne zmeniť.
GEN003255	Súbor at.deny nesmie mať rozšírený zoznam riadenia prístupu.	**Umiestnenie** /etc/security/pscexpert/dodv2/acldodfiles **Akcia na zabezpečenie súladu** Zakáže určený rozšírený zoznam ACL. **Poznámka:** Toto nastavenie nebude automaticky zmenené pri obnovení predvolenej politiky systému AIX prostredníctvom súboru DoDv2_to_AIXDefault.xml. Toto nastavenie je potrebné manuálne zmeniť.
GEN003410	Adresár at nesmie mať rozšírený zoznam riadenia prístupu.	**Umiestnenie** /etc/security/pscexpert/dodv2/acldodfiles **Akcia na zabezpečenie súladu** Zakáže určený rozšírený zoznam ACL. **Poznámka:** Toto nastavenie nebude automaticky zmenené pri obnovení predvolenej politiky systému AIX prostredníctvom súboru DoDv2_to_AIXDefault.xml. Toto nastavenie je potrebné manuálne zmeniť.

Tabuľka 5. Požiadavky Ministerstva obrany USA na zoznamy riadenia prístupu (ACL) (pokračovanie)

ID kontrolného bodu STIG Ministerstva obrany USA	Popis	Umiestnenie skriptu, v ktorom je definovaná akcia, a výsledky akcie zabezpečujúcej súlad
GEN003745	Súbory inetd.conf a xinetd.conf nesmú mať rozšírené zoznamy riadenia prístupu.	**Umiestnenie** /etc/security/pscexpert/dodv2/acldodfiles **Akcia na zabezpečenie súladu** Zakáže určený rozšírený zoznam ACL. **Poznámka:** Toto nastavenie nebude automaticky zmenené pri obnovení predvolenej politiky systému AIX prostredníctvom súboru DoDv2_to_AIXDefault.xml. Toto nastavenie je potrebné manuálne zmeniť.
GEN003790	Súbor services nesmie mať rozšírený zoznam riadenia prístupu.	**Umiestnenie** /etc/security/pscexpert/dodv2/acldodfiles **Akcia na zabezpečenie súladu** Zakáže určený rozšírený zoznam ACL. **Poznámka:** Toto nastavenie nebude automaticky zmenené pri obnovení predvolenej politiky systému AIX prostredníctvom súboru DoDv2_to_AIXDefault.xml. Toto nastavenie je potrebné manuálne zmeniť.
GEN003950	Súbor hosts.lpd (alebo ekvivalentný) nesmie mať rozšírený zoznam riadenia prístupu.	**Umiestnenie** /etc/security/pscexpert/dodv2/acldodfiles **Akcia na zabezpečenie súladu** Zakáže určený rozšírený zoznam ACL. **Poznámka:** Toto nastavenie nebude automaticky zmenené pri obnovení predvolenej politiky systému AIX prostredníctvom súboru DoDv2_to_AIXDefault.xml. Toto nastavenie je potrebné manuálne zmeniť.
GEN004010	Súbor traceroute nesmie mať rozšírený zoznam riadenia prístupu.	**Umiestnenie** /etc/security/pscexpert/dodv2/acldodfiles **Akcia na zabezpečenie súladu** Zakáže určený rozšírený zoznam ACL. **Poznámka:** Toto nastavenie nebude automaticky zmenené pri obnovení predvolenej politiky systému AIX prostredníctvom súboru DoDv2_to_AIXDefault.xml. Toto nastavenie je potrebné manuálne zmeniť.
GEN004390	Súbor alias nesmie mať rozšírený zoznam riadenia prístupu.	**Umiestnenie** /etc/security/pscexpert/dodv2/acldodfiles **Akcia na zabezpečenie súladu** Zakáže určený rozšírený zoznam ACL. **Poznámka:** Toto nastavenie nebude automaticky zmenené pri obnovení predvolenej politiky systému AIX prostredníctvom súboru DoDv2_to_AIXDefault.xml. Toto nastavenie je potrebné manuálne zmeniť.

Tabuľka 5. Požiadavky Ministerstva obrany USA na zoznamy riadenia prístupu (ACL) (pokračovanie)

ID kontrolného bodu STIG Ministerstva obrany USA	Popis	Umiestnenie skriptu, v ktorom je definovaná akcia, a výsledky akcie zabezpečujúcej súlad
GEN004430	Súbory, ktoré sa spúšťajú prostredníctvom súboru aliases pošty, nesmú mať rozšírené zoznamy riadenia prístupu.	**Umiestnenie** /etc/security/pscexpert/dodv2/acldodfiles **Akcia na zabezpečenie súladu** Zakáže určený rozšírený zoznam ACL. **Poznámka:** Toto nastavenie nebude automaticky zmenené pri obnovení predvolenej politiky systému AIX prostredníctvom súboru DoDv2_to_AIXDefault.xml. Toto nastavenie je potrebné manuálne zmeniť.
GEN004510	Protokolový súbor služby SMTP nesmie mať rozšírený zoznam riadenia prístupu.	**Umiestnenie** /etc/security/pscexpert/dodv2/acldodfiles **Akcia na zabezpečenie súladu** Zakáže určený rozšírený zoznam ACL. **Poznámka:** Toto nastavenie nebude automaticky zmenené pri obnovení predvolenej politiky systému AIX prostredníctvom súboru DoDv2_to_AIXDefault.xml. Toto nastavenie je potrebné manuálne zmeniť.
GEN004950	Súbor ftpusers nesmie mať rozšírený zoznam riadenia prístupu.	**Umiestnenie** /etc/security/pscexpert/dodv2/acldodfiles **Akcia na zabezpečenie súladu** Zakáže určený rozšírený zoznam ACL. **Poznámka:** Toto nastavenie nebude automaticky zmenené pri obnovení predvolenej politiky systému AIX prostredníctvom súboru DoDv2_to_AIXDefault.xml. Toto nastavenie je potrebné manuálne zmeniť.
GEN005190	Súbory .Xauthority nesmú mať rozšírené zoznamy riadenia prístupu.	**Umiestnenie** /etc/security/pscexpert/dodv2/acldodfiles **Akcia na zabezpečenie súladu** Zakáže určený rozšírený zoznam ACL. **Poznámka:** Toto nastavenie nebude automaticky zmenené pri obnovení predvolenej politiky systému AIX prostredníctvom súboru DoDv2_to_AIXDefault.xml. Toto nastavenie je potrebné manuálne zmeniť.
GEN005350	Súbory MIB (Management Information Base) nesmú mať rozšírené zoznamy riadenia prístupu.	**Umiestnenie** /etc/security/pscexpert/dodv2/acldodfiles **Akcia na zabezpečenie súladu** Zakáže určený rozšírený zoznam ACL. **Poznámka:** Toto nastavenie nebude automaticky zmenené pri obnovení predvolenej politiky systému AIX prostredníctvom súboru DoDv2_to_AIXDefault.xml. Toto nastavenie je potrebné manuálne zmeniť.

Tabuľka 5. Požiadavky Ministerstva obrany USA na zoznamy riadenia prístupu (ACL) (pokračovanie)

ID kontrolného bodu STIG Ministerstva obrany USA	Popis	Umiestnenie skriptu, v ktorom je definovaná akcia, a výsledky akcie zabezpečujúcej súlad
GEN005375	Súbor snmpd.conf nesmie mať rozšírený zoznam riadenia prístupu.	**Umiestnenie** /etc/security/pscexpert/dodv2/acldodfiles **Akcia na zabezpečenie súladu** Zakáže určený rozšírený zoznam ACL. **Poznámka:** Toto nastavenie nebude automaticky zmenené pri obnovení predvolenej politiky systému AIX prostredníctvom súboru DoDv2_to_AIXDefault.xml. Toto nastavenie je potrebné manuálne zmeniť.
GEN005395	Súbor /etc/syslog.conf nesmie mať rozšírený zoznam riadenia prístupu.	**Umiestnenie** /etc/security/pscexpert/dodv2/acldodfiles **Akcia na zabezpečenie súladu** Zakáže určený rozšírený zoznam ACL. **Poznámka:** Toto nastavenie nebude automaticky zmenené pri obnovení predvolenej politiky systému AIX prostredníctvom súboru DoDv2_to_AIXDefault.xml. Toto nastavenie je potrebné manuálne zmeniť.
GEN006150	Súbor /usr/lib/smb.conf nesmie mať rozšírený zoznam riadenia prístupu.	**Umiestnenie** /etc/security/pscexpert/dodv2/acldodfiles **Akcia na zabezpečenie súladu** Zakáže určený rozšírený zoznam ACL. **Poznámka:** Toto nastavenie nebude automaticky zmenené pri obnovení predvolenej politiky systému AIX prostredníctvom súboru DoDv2_to_AIXDefault.xml. Toto nastavenie je potrebné manuálne zmeniť.
GEN006210	Súbor /var/private/smbpasswd nesmie mať rozšírený zoznam riadenia prístupu.	**Umiestnenie** /etc/security/pscexpert/dodv2/acldodfiles **Akcia na zabezpečenie súladu** Zakáže určený rozšírený zoznam ACL. **Poznámka:** Toto nastavenie nebude automaticky zmenené pri obnovení predvolenej politiky systému AIX prostredníctvom súboru DoDv2_to_AIXDefault.xml. Toto nastavenie je potrebné manuálne zmeniť.
GEN006270	Súbor /etc/news/hosts.nntp nesmie mať rozšírený zoznam riadenia prístupu.	**Umiestnenie** /etc/security/pscexpert/dodv2/acldodfiles **Akcia na zabezpečenie súladu** Zakáže určený rozšírený zoznam ACL. **Poznámka:** Toto nastavenie nebude automaticky zmenené pri obnovení predvolenej politiky systému AIX prostredníctvom súboru DoDv2_to_AIXDefault.xml. Toto nastavenie je potrebné manuálne zmeniť.

Tabuľka 5. Požiadavky Ministerstva obrany USA na zoznamy riadenia prístupu (ACL) (pokračovanie)

ID kontrolného bodu STIG Ministerstva obrany USA	Popis	Umiestnenie skriptu, v ktorom je definovaná akcia, a výsledky akcie zabezpečujúcej súlad
GEN006290	Súbor /etc/news/hosts.nntp.nolimit nesmie mať rozšírený zoznam riadenia prístupu.	**Umiestnenie** /etc/security/pscexpert/dodv2/acldodfiles **Akcia na zabezpečenie súladu** Zakáže určený rozšírený zoznam ACL. **Poznámka:** Toto nastavenie nebude automaticky zmenené pri obnovení predvolenej politiky systému AIX prostredníctvom súboru DoDv2_to_AIXDefault.xml. Toto nastavenie je potrebné manuálne zmeniť.
GEN006310	Súbor /etc/news/nnrp.access nesmie mať rozšírený zoznam riadenia prístupu.	**Umiestnenie** /etc/security/pscexpert/dodv2/acldodfiles **Akcia na zabezpečenie súladu** Zakáže určený rozšírený zoznam ACL. **Poznámka:** Toto nastavenie nebude automaticky zmenené pri obnovení predvolenej politiky systému AIX prostredníctvom súboru DoDv2_to_AIXDefault.xml. Toto nastavenie je potrebné manuálne zmeniť.
GEN006330	Súbor /etc/news/passwd.nntp nesmie mať rozšírený zoznam riadenia prístupu.	**Umiestnenie** /etc/security/pscexpert/dodv2/acldodfiles **Akcia na zabezpečenie súladu** Zakáže určený rozšírený zoznam ACL. **Poznámka:** Toto nastavenie nebude automaticky zmenené pri obnovení predvolenej politiky systému AIX prostredníctvom súboru DoDv2_to_AIXDefault.xml. Toto nastavenie je potrebné manuálne zmeniť.
GEN008120	Ak sa v systéme používa protokol LDAP na autentifikáciu alebo získanie informácií o konte, súbor /etc/ldap.conf (alebo ekvivalentný) nesmie mať rozšírený zoznam riadenia prístupu.	**Umiestnenie** /etc/security/pscexpert/dodv2/acldodfiles **Akcia na zabezpečenie súladu** Zabezpečuje, že určené súbory nebudú mať rozšírený zoznam riadenia prístupu. **Poznámka:** Toto nastavenie nebude automaticky zmenené pri obnovení predvolenej politiky systému AIX prostredníctvom súboru DoDv2_to_AIXDefault.xml. Toto nastavenie je potrebné manuálne zmeniť.
GEN008200	Ak sa v systéme používa protokol LDAP na autentifikáciu alebo získanie informácií o konte, súbor alebo adresár certifikačnej autority LDAP TLS nesmie mať rozšírený zoznam riadenia prístupu.	**Umiestnenie** /etc/security/pscexpert/dodv2/acldodfiles **Akcia na zabezpečenie súladu** Zabezpečuje, že určený súbory alebo adresár nebude mať rozšírený zoznam riadenia prístupu. **Poznámka:** Toto nastavenie nebude automaticky zmenené pri obnovení predvolenej politiky systému AIX prostredníctvom súboru DoDv2_to_AIXDefault.xml. Toto nastavenie je potrebné manuálne zmeniť.

Súvisiace informácie:

Súlad s pokynmi STIG Ministerstva obrany USA

Súlad s požiadavkami štandardu PCI - DSS (Payment Card Industry - Data Security Standard)

Štandard PCI -DSS (Payment Card Industry - Data Security Standard) kategorizuje bezpečnosť IT do 12 častí, ktoré sa nazývajú 12 požiadaviek a postupov hodnotenia bezpečnosti.

Týchto 12 požiadaviek a postupov hodnotenia bezpečnosti IT, ktoré definuje PCI - DSS, zahŕňa tieto položky:

Požiadavka 1: Nainštalovať a udržiavať konfiguráciu firewallu na ochranu údajov držiteľov kariet.
Dokumentovaný zoznam služieb a portov potrebných pre podnikanie. Táto požiadavka je implementovaná zakázaním nepotrebných a nie bezpečných služieb.

Požiadavka 2: Nepoužívať predvolené nastavenia dodané predajcom pre systémové heslá a iné bezpečnostné parametre.
Vždy zmeňte predvolené nastavenia dodané predajcom skôr než nainštalujete systém do siete. Táto požiadavka je implementovaná zakázaním démona SNMP (Simple Network Management Protocol).

Požiadavka 3: Chrániť uložené údaje držiteľov kariet.
Táto požiadavka je implementovaná povolením funkcie EFS (Encrypted File System), ktorú poskytuje operačný systém AIX.

Požiadavka 4: Šifrovať údaje držiteľov kariet, keď prenášate údaje cez otvorené verejné siete.
Táto požiadavka je implementovaná povolením funkcie IPSEC (IP Security), ktorú poskytuje operačný systém AIX.

Požiadavka 5: Používať a pravidelne aktualizovať antivírusové softvérové programy.
Táto požiadavka je implementovaná používaním programu politiky Trusted Execution. Trusted Execution je odporúčaný antivírusový softvér a je natívny pre operačný systém AIX. PCI vyžaduje, aby ste zaznamenávali protokoly z programu Trusted Execution povolením SIEM (security information and event management) monitorovať výstrahy. Spustenie programu Trusted Execution v režime len protokolovania nezastaví kontroly, keď nezhoda hodnoty hash spôsobí chybu.

Požiadavka 6: Vyvíjať a udržiavať bezpečné systémy a aplikácie.
Na implementáciu tejto požiadavky musíte na váš systém manuálne nainštalovať požadované opravy. Ak ste zakúpili PowerSC Standard Edition, môžete používať funkciu TNC (Trusted Network Connect).

Požiadavka 7: Obmedziť prístup k údajom držiteľov kariet podľa toho, či ich firma potrebuje poznať.
Silné opatrenia na riadenie prístupu môžete implementovať pomocou funkcie RBAC na povolenie pravidiel a rolí. Funkciu RBAC nie je možné automatizovať, pretože vyžaduje, aby bol povolený vstup od administrátora.

RbacEnablement kontroluje systém, aby určil, či na systéme existujú vlastnosti ISSO, SO a SA pre roly. Ak tieto vlastnosti neexistujú, skript ich vytvorí. Tento skript sa tiež spustí ako súčasť kontrol pscexpert, ktoré vykoná, keď spúšťa príkazy, ako napríklad pscxpert -c.

Požiadavka 8: Priradiť jedinečný identifikátor každej osobe, ktorá má prístup k počítaču.
Túto požiadavku môžete implementovať povolením profilov PCI. Pre profil PCI sa používajú tieto pravidlá:

- Zmeniť heslá užívateľov aspoň každých 90 dní.
- Vyžadovať minimálnu dĺžku hesla 7 znakov.
- Používať heslo, ktoré obsahuje číselné aj abecedné znaky.
- Nepovoliť osobám odoslať nové heslo, ktoré je rovnaké ako predchádzajúce štyri heslá, ktoré boli použité.
- Obmedziť opakované pokusy o prístup uzamknutím ID užívateľa po šiestich neúspešných pokusoch.
- Nastaviť trvanie uzamknutia na 30 minút alebo pokiaľ administrátor znova nepovolí ID užívateľa.
- Vyžadovať od užívateľa, aby znova zadal heslo na reaktiváciu terminálu po jeho 15 minútovej alebo dlhšej neaktivite.

Požiadavka 9: Obmedziť fyzický prístup k údajom držiteľov kariet.

Archívy, ktoré obsahujú citlivé údaje držiteľov kariet, ukladajte v miestnosti s obmedzeným prístupom.

Požiadavka 10: Sledovať a monitorovať všetky prístupy k sieťovým prostriedkom a k údajom držiteľov kariet.

Táto požiadavka je implementovaná protokolovaním prístupu k systémovým komponentom povolením automatických protokolov na systémových komponentoch.

Požiadavka 11: Pravidelne testujte bezpečnostné systémy a procesy.

Táto požiadavka je implementovaná používaním funkcie Real-Time Compliance.

Požiadavka 12: Udržiavať bezpečnostnú politiku, ktorá zahŕňa informačnú bezpečnosť pre zamestnancov a zmluvných partnerov.

Aktivácia modemov pre dodávateľov len vtedy, keď ich potrebujú, s okamžitou deaktiváciou po ich použití. Táto požiadavka je implementovaná zakázaním vzdialeného prihlasovania užívateľa root, aktiváciou systémovým administrátorom v prípade potreby a potom deaktiváciou, keď už nie je potrebné.

PowerSC Standard Edition redukuje konfiguračný manažment, ktorý je potrebný na splnenie smerníc, ktoré definuje PCI DSS verzia 2.0 a PCI DSS verzia 3.0. Avšak celý proces nemôže byť automatizovaný.

Napríklad, obmedzenie prístupu k údajom držiteľov kariet na základe požiadavky firmy nie je možné automatizovať. Operačný systém AIX poskytuje silné bezpečnostné technológie, ako je RBAC (Role Based Access Control); avšak PowerSC Standard Edition nemôže automatizovať túto konfiguráciu, pretože nemôže určiť osoby, ktoré vyžadujú prístup, a osoby, ktoré ho nevyžadujú. IBM Compliance Expert môže automatizovať konfiguráciu ostatných nastavení bezpečnosti, ktoré sú konzistentné s požiadavkami PCI.

Keď sa profil PCI aplikuje na databázové prostredie, niektoré porty TCP a UDP, ktoré používajú softvérové programy, sú zakázané obmedzeniami. Pre spustenie aplikácie a pracovného zaťaženia musíte povoliť tieto porty a zakázať funkciu Trusted Execution. Pre odstránenie obmedzení na portoch a zakázanie funkcie Trusted Execution spustite tieto príkazy:

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

Poznámka: Všetky vlastné skriptové súbory, ktoré sú poskytované na udržiavanie súladu s požiadavkami PCI - DSS, sú v adresári /etc/security/pscexpert/bin.

Nasledujúca tabuľka ukazuje ako systém PowerSC Standard Edition spĺňa požiadavky štandardu PCI DSS pomocou funkcií pomocného programu AIX Security Expert:

Tabuľka 6. Nastavenia súvisiace so štandardmi súladu s PCI DSS verzia 2.0 a verzia 3.0

Implementuje tieto štandardy PCI DSS	Špecifikácia implementácie	Implementácia AIX Security Expert	Umiestnenie skriptu, ktorý modifikuje hodnotu
2.1	Vždy zmeňte predvolené nastavenia dodané predajcom pred inštaláciou systému v sieti. Napríklad, zahrňte heslá, reťazce komunity protokolu SNMP (simple network management protocol) a eliminujte nepotrebné kontá.	Nastavuje minimálny počet týždňov, ktoré musia uplynúť než môžete zmeniť heslo, na 0 týždňov nastavením parametra **minage** na hodnotu 0.	/etc/security/pscexpert/bin/chusrattr
PCI verzia 2 8.5.9 **PCI verzia 3** 8.2.4	Zmeniť heslá užívateľov aspoň každých 90 dní.	Nastavuje maximálny počet týždňov, kedy je platné heslo, na 13 týždňov nastavením parametra **maxage** na hodnotu 13.	/etc/security/pscexpert/bin/chusrattr

Tabuľka 6. Nastavenia súvisiace so štandardmi súladu s PCI DSS verzia 2.0 a verzia 3.0 (pokračovanie)

Implementuje tieto štandardy PCI DSS	Špecifikácia implementácie	Implementácia AIX Security Expert	Umiestnenie skriptu, ktorý modifikuje hodnotu
2.1	Vždy zmeňte predvolené nastavenia dodané predajcom pred inštaláciou systému v sieti. Napríklad, zahrňte heslá, reťazce komunity protokolu SNMP (simple network management protocol) a eliminujte nepotrebné kontá.	Nastavuje počet týždňov, kedy zostane konto s expirovaným heslom v systéme, na 8 týždňov nastavením parametra **maxexpired** na hodnotu 8.	/etc/security/pscexpert/bin/chusrattr
PCI verzia 2 8.5.10 **PCI verzia 3** 8.2.3	Vyžadovať minimálnu dĺžku hesla aspoň 7 znakov.	Nastavuje minimálnu dĺžku hesla na 7 znakov nastavením parametra **minlen** na hodnotu 7.	/etc/security/pscexpert/bin/chusrattr
PCI verzia 2 8.5.11 **PCI verzia 3** 8.2.3	Používať heslá, ktoré obsahujú numerické aj abecedné znaky.	Nastavuje minimálny počet abecedných znakov, ktoré sa vyžadujú v hesle, na 1. Toto nastavenie zabezpečí, že heslo bude obsahovať abecedné znaky, nastavením parametra **minalpha** na hodnotu 1.	/etc/security/pscexpert/bin/chusrattr
PCI verzia 2 8.5.11 **PCI verzia 3** 8.2.3	Používať heslá, ktoré obsahujú numerické aj abecedné znaky.	Nastavuje minimálny počet neabecedných znakov, ktoré sa vyžadujú v hesle, na 1. Toto nastavenie zabezpečí, že heslo bude obsahovať neabecedné znaky, nastavením parametra **minother** na hodnotu 1.	/etc/security/pscexpert/bin/chusrattr
PCI verzia 2 2.1 **PCI verzia 3** 8.2.2	Vždy zmeňte predvolené nastavenia dodané predajcom pred inštaláciou systému v sieti. Napríklad, zahrňte heslá, reťazce komunity protokolu SNMP (simple network management protocol) a eliminujte nepotrebné kontá.	Nastavuje maximálny počet, koľkokrát sa nejaký znak môže opakovať v hesle, na 8 nastavením parametra **maxrepeats** na hodnotu 8. Toto nastavenie znamená, že znak sa v hesle môže opakovať neobmedzený počet krát, keď je v súlade s ostatnými obmedzeniami hesla.	/etc/security/pscexpert/bin/chusrattr
PCI verzia 2 8.5.12 **PCI verzia 3** 8.2.5	Nepovoliť osobe odoslať nové heslo, ktoré je rovnaké ako niektoré z posledných štyroch hesiel, ktoré používala.	Nastavuje počet týždňov, kedy sa heslo znova môže použiť, na 52 nastavením parametra **histexpire** na hodnotu 52.	/etc/security/pscexpert/bin/chusrattr
PCI verzia 2 8.5.12 **PCI verzia 3** 8.2.5	Nepovoliť osobe odoslať nové heslo, ktoré je rovnaké ako niektoré z posledných štyroch hesiel, ktoré používala.	Nastavuje počet predchádzajúcich hesiel, ktoré nemôžete znova použiť, na 4 nastavením parametra **histsize** na hodnotu 4.	/etc/security/pscexpert/bin/chusrattr
PCI verzia 2 8.5.13 **PCI verzia 3** 8.1.6	Obmedziť počet opakovaných pokusov o prístup uzamknutím ID užívateľa po najviac šiestich pokusoch.	Nastavuje počet opakovaných neúspešných pokusov o prihlásenie, kedy sa zablokuje konto, na 6 pokusov pre každé konto, iné ako root, nastavením parametra **loginentries** na hodnotu 6.	/etc/security/pscexpert/bin/chusrattr

Tabuľka 6. Nastavenia súvisiace so štandardmi súladu s PCI DSS verzia 2.0 a verzia 3.0 (pokračovanie)

Implementuje tieto štandardy PCI DSS	Špecifikácia implementácie	Implementácia AIX Security Expert	Umiestnenie skriptu, ktorý modifikuje hodnotu
PCI verzia 2 8.5.13 **PCI verzia 3** 8.1.6	Obmedziť počet opakovaných pokusov o prístup uzamknutím ID užívateľa po najviac šiestich pokusoch.	Nastavuje počet opakovaných neúspešných pokusov o prihlásenie, kedy sa zablokuje port, na 6 pokusov nastavením parametra **logindisable** na hodnotu 6.	• /etc/security/pscexpert/bin/chdefstanza • /etc/security/login.cfg
PCI verzia 2 8.5.14 **PCI verzia 3** 8.1.7	Nastaviť trvanie uzamknutia na minimálne 30 minút alebo pokiaľ administrátor nepovolí ID užívateľa.	Nastavuje trvanie kedy je port uzamknutý po tom, čo ho zablokuje atribút *logindisable* na 30 minút, nastavením parametra **loginreenable** na hodnotu 30.	• /etc/security/pscexpert/bin/chdefstanza • /etc/security/login.cfg
12.3.9	Aktivácia technológií na vzdialený prístup pre dodávateľov a obchodných partnerov, len keď ich potrebujú, s okamžitou deaktiváciou po ich použití.	Zakazuje funkciu vzdialeného prihlásenia užívateľa root nastavením tejto hodnoty na false. Systémový administrátor môže aktivovať funkciu vzdialeného prihlásenia v prípade potreby a potom ju deaktivuje, keď je úloha dokončená.	• /etc/security/pscexpert/bin/chuserstanza • /etc/security/user
8.1.1	Priradiť všetkým užívateľom jedinečné ID pred povolením ich prístupu k systémovým komponentom alebo údajom držiteľov kariet.	Povoľuje funkciu, ktorá zabezpečí, že všetci užívatelia majú jedinečné meno užívateľa skôr než môžu pristupovať k systémovým komponentom alebo údajom držiteľov kariet, nastavením tejto funkcie na hodnotu true.	• /etc/security/pscexpert/bin/chuserstanza • /etc/security/user
10.2	Povoliť auditovanie na systéme.	Povoľuje auditovanie binárnych súborov na systéme.	/etc/security/pscexpert/bin/pciaudit
PCI verzia 2 1.1.5 2.2.2 **PCI verzia 3** 2.2.2	Zakázať nepotrebné a nie bezpečné služby, ktoré zahŕňajú CDE (Common Desktop Environment).	Zakazuje funkciu CDE, keď nie je nakonfigurovaný mechanizmus LFT (layer four traceroute).	/etc/security/pscexpert/bin/comntrows
PCI verzia 2 1.1.5 2.2.2 **PCI verzia 3** 2.2.2	Zakázať nepotrebné a nie bezpečné služby, ktoré zahŕňajú démona timed.	Zastaví démona timed a označí ako komentár príslušnú položku v súbore /etc/rc.tcpip, ktorá automaticky spúšťa tohto démona.	/etc/security/pscexpert/bin/rctcpip
PCI verzia 2 1.1.5 2.2.2 **PCI verzia 3** 2.2.2	Zakázať nepotrebné a nie bezpečné služby, ktoré zahŕňajú démona rwhod.	Zastaví démona rwhod a označí ako komentár príslušnú položku v súbore /etc/rc.tcpip, ktorá automaticky spúšťa tohto démona.	/etc/security/pscexpert/bin/rctcpip
PCI verzia 2 2.1 **PCI verzia 3** 2.1.1	Vykonať zmenu predvoleného nastavenia dodaného predajcom pred inštaláciou systému v sieti, ktorá zahŕňa zakázanie démona SNMP.	Zastaví démona SNMP a označí ako komentár príslušnú položku v súbore /etc/rc.tcpip, ktorá automaticky spúšťa tohto démona.	/etc/security/pscexpert/bin/rctcpip

Tabuľka 6. Nastavenia súvisiace so štandardmi súladu s PCI DSS verzia 2.0 a verzia 3.0 (pokračovanie)

Implementuje tieto štandardy PCI DSS	Špecifikácia implementácie	Implementácia AIX Security Expert	Umiestnenie skriptu, ktorý modifikuje hodnotu
PCI verzia 2 2.1 **PCI verzia 3** 2.1.1	Vykonať zmenu predvoleného nastavenia dodaného predajcom pred inštaláciou systému v sieti, ktorá zahŕňa zakázanie démona SNMPMIBD.	Zakáže démona SNMPMIBD a označí ako komentár príslušnú položku v súbore /etc/rc.tcpip, ktorá automaticky spúšťa tohto démona.	/etc/security/pscexpert/bin/rctcpip
2.1	Vykonať zmenu predvoleného nastavenia dodaného predajcom pred inštaláciou systému v sieti, ktorá zahŕňa zakázanie démona AIXMIBD.	Zakáže démona AIXMIBD a označí ako komentár príslušnú položku v súbore /etc/rc.tcpip, ktorá automaticky spúšťa tohto démona.	/etc/security/pscexpert/bin/rctcpip
2.1	Vykonať zmenu predvoleného nastavenia dodaného predajcom pred inštaláciou systému v sieti, ktorá zahŕňa zakázanie démona HOSTMIBD.	Zakáže démona HOSTMIBD a označí ako komentár príslušnú položku v súbore /etc/rc.tcpip, ktorá automaticky spúšťa tohto démona.	/etc/security/pscexpert/bin/rctcpip
PCI verzia 2 1.1.5 2.2.2 **PCI verzia 3** 2.2.2	Zakázať nepotrebné a nie bezpečné služby, ktoré zahŕňajú démona DPID2.	Zastaví démona DPID2 a označí ako komentár príslušnú položku v súbore /etc/rc.tcpip, ktorá automaticky spúšťa tohto démona.	/etc/security/pscexpert/bin/rctcpip
PCI verzia 2 2.1 **PCI verzia 3** 2.2.2	Vykonať zmenu predvoleného nastavenia dodaného predajcom pred inštaláciou systému v sieti, ktorá zahŕňa zastavenie servera DHCP.	Zakáže server DHCP.	/etc/security/pscexpert/bin/rctcpip
PCI verzia 2 1.1.5 2.2.2 **PCI verzia 3** 2.2.2	Zakázať nepotrebné a nie bezpečné služby, ktoré zahŕňajú agenta DHCP.	Zastaví a zakáže relay agenta DHCP a označí ako komentár príslušnú položku v súbore /etc/rc.tcpip, ktorá automaticky spúšťa tohto agenta.	/etc/security/pscexpert/bin/rctcpip
PCI verzia 2 1.1.5 2.2.2 **PCI verzia 3** 2.2.2	Zakázať nepotrebné a nie bezpečné služby, ktoré zahŕňajú démona rshd.	Zastaví a zakáže všetky inštancie démona rshd a službu shell, a označí ako komentár príslušné položky v súbore /etc/inetd.conf, ktoré automaticky spúšťajú tieto inštancie.	/etc/security/pscexpert/bin/cominetdconf
PCI verzia 2 1.1.5 2.2.2 **PCI verzia 3** 2.2.2	Zakázať nepotrebné a nie bezpečné služby, ktoré zahŕňajú démona rlogind.	Zastaví a zakáže všetky inštancie démona rlogind a službu rlogin. Pomocný program AIX Security Expert tiež označí ako komentár príslušné položky v súbore /etc/inetd.conf, ktoré automaticky spúšťajú tieto inštancie.	/etc/security/pscexpert/bin/cominetdconf
PCI verzia 2 1.1.5 2.2.2 **PCI verzia 3** 2.2.2	Zakázať nepotrebné a nie bezpečné služby, ktoré zahŕňajú démona rexecd.	Zastaví a zakáže všetky inštancie démona rexecd. Pomocný program AIX Security Expert tiež označí ako komentár príslušnú položku v súbore /etc/inetd.conf, ktorá automaticky spúšťa tohto démona.	/etc/security/pscexpert/bin/cominetdconf

Tabuľka 6. Nastavenia súvisiace so štandardmi súladu s PCI DSS verzia 2.0 a verzia 3.0 (pokračovanie)

Implementuje tieto štandardy PCI DSS	Špecifikácia implementácie	Implementácia AIX Security Expert	Umiestnenie skriptu, ktorý modifikuje hodnotu
PCI verzia 2 1.1.5 2.2.2 **PCI verzia 3** 2.2.2	Zakázať nepotrebné a nie bezpečné služby, ktoré zahŕňajú démona comsat.	Zastaví a zakáže všetky inštancie démona comsat. Pomocný program AIX Security Expert tiež označí ako komentár príslušnú položku v súbore /etc/inetd.conf, ktorá automaticky spúšťa tohto démona.	/etc/security/pscexpert/bin/cominetdconf
PCI verzia 2 1.1.5 2.2.2 **PCI verzia 3** 2.2.2	Zakázať nepotrebné a nie bezpečné služby, ktoré zahŕňajú démona fingerd.	Zastaví a zakáže všetky inštancie démona fingerd. Pomocný program AIX Security Expert tiež označí ako komentár príslušnú položku v súbore /etc/inetd.conf, ktorá automaticky spúšťa tohto démona.	/etc/security/pscexpert/bin/cominetdconf
PCI verzia 2 1.1.5 2.2.2 **PCI verzia 3** 2.2.2	Zakázať nepotrebné a nie bezpečné služby, ktoré zahŕňajú démona systat.	Zastaví a zakáže všetky inštancie démona systat. Pomocný program AIX Security Expert tiež označí ako komentár príslušnú položku v súbore /etc/inetd.conf, ktorá automaticky spúšťa tohto démona.	/etc/security/pscexpert/bin/cominetdconf
2.1	Vykonať zmenu predvoleného nastavenia dodaného predajcom pred inštaláciou systému v sieti, ktorá zahŕňa zakázanie príkazu netstat.	Zakáže príkaz netstat označením ako komentár príslušnej položky v súbore /etc/inetd.conf.	/etc/security/pscexpert/bin/cominetdconf
PCI verzia 2 1.1.5 2.2.2 **PCI verzia 3** 2.2.3	Zakázať nepotrebné a nie bezpečné služby, ktoré zahŕňajú démona tftp.	Zastaví a zakáže všetky inštancie démona tftp. Pomocný program AIX Security Expert tiež označí ako komentár príslušnú položku v súbore /etc/inetd.conf, ktorá automaticky spúšťa tohto démona.	/etc/security/pscexpert/bin/cominetdconf
PCI verzia 2 1.1.5 2.2.2 **PCI verzia 3** 2.2.2	Zakázať nepotrebné a nie bezpečné služby, ktoré zahŕňajú démona talkd.	Zastaví a zakáže všetky inštancie démona talkd. Pomocný program AIX Security Expert tiež označí ako komentár príslušnú položku v súbore /etc/inetd.conf, ktorá automaticky spúšťa tohto démona.	/etc/security/pscexpert/bin/cominetdconf
PCI verzia 2 1.1.5 2.2.2 **PCI verzia 3** 2.2.2	Zakázať nepotrebné a nie bezpečné služby, ktoré zahŕňajú démona rquotad.	Zastaví a zakáže všetky inštancie démona rquotad. Pomocný program AIX Security Expert tiež označí ako komentár príslušnú položku v súbore /etc/inetd.conf, ktorá automaticky spúšťa tohto démona.	/etc/security/pscexpert/bin/cominetdconf
PCI verzia 2 1.1.5 2.2.2 **PCI verzia 3** 2.2.2	Zakázať nepotrebné a nie bezpečné služby, ktoré zahŕňajú démona rstatd.	Zastaví a zakáže všetky inštancie démona rstatd. Pomocný program AIX Security Expert tiež označí ako komentár príslušnú položku v súbore /etc/inetd.conf, ktorá automaticky spúšťa tohto démona.	/etc/security/pscexpert/bin/cominetdconf

Tabuľka 6. Nastavenia súvisiace so štandardmi súladu s PCI DSS verzia 2.0 a verzia 3.0 (pokračovanie)

Implementuje tieto štandardy PCI DSS	Špecifikácia implementácie	Implementácia AIX Security Expert	Umiestnenie skriptu, ktorý modifikuje hodnotu
PCI verzia 2 1.1.5 2.2.2 **PCI verzia 3** 2.2.2	Zakázať nepotrebné a nie bezpečné služby, ktoré zahŕňajú démona rusersd.	Zastaví a zakáže všetky inštancie démona rusersd. Pomocný program AIX Security Expert tiež označí ako komentár príslušnú položku v súbore /etc/inetd.conf, ktorá automaticky spúšťa tohto démona.	/etc/security/pscexpert/bin/cominetdconf
PCI verzia 2 1.1.5 2.2.2 **PCI verzia 3** 2.2.2	Zakázať nepotrebné a nie bezpečné služby, ktoré zahŕňajú démona rwalld.	Zastaví a zakáže všetky inštancie démona rwalld. Pomocný program AIX Security Expert tiež označí ako komentár príslušnú položku v súbore /etc/inetd.conf, ktorá automaticky spúšťa tohto démona.	/etc/security/pscexpert/bin/cominetdconf
PCI verzia 2 1.1.5 2.2.2 **PCI verzia 3** 2.2.2	Zakázať nepotrebné a nie bezpečné služby, ktoré zahŕňajú démona sprayd.	Zastaví a zakáže všetky inštancie démona sprayd. Pomocný program AIX Security Expert tiež označí ako komentár príslušnú položku v súbore /etc/inetd.conf, ktorá automaticky spúšťa tohto démona.	/etc/security/pscexpert/bin/cominetdconf
PCI verzia 2 1.1.5 2.2.2 **PCI verzia 3** 2.2.2	Zakázať nepotrebné a nie bezpečné služby, ktoré zahŕňajú démona pcnfsd.	Zastaví a zakáže všetky inštancie démona pcnfsd. Pomocný program AIX Security Expert tiež označí ako komentár príslušnú položku v súbore /etc/inetd.conf, ktorá automaticky spúšťa tohto démona.	/etc/security/pscexpert/bin/cominetdconf
PCI verzia 2 1.1.5 2.2.2 **PCI verzia 3** 2.2.2	Zakázať nepotrebné a nie bezpečné služby, ktoré zahŕňajú službu TCP echo.	Zastaví a zakáže všetky inštancie služby echo(tcp). Pomocný program AIX Security Expert tiež označí ako komentár príslušnú položku v súbore /etc/inetd.conf, ktorá automaticky spúšťa túto službu.	/etc/security/pscexpert/bin/cominetdconf
PCI verzia 2 1.1.5 2.2.2 **PCI verzia 3** 2.2.2	Zakázať nepotrebné a nie bezpečné služby, ktoré zahŕňajú službu TCP discard.	Zastaví a zakáže všetky inštancie služby discard(tcp). Pomocný program AIX Security Expert tiež označí ako komentár príslušnú položku v súbore /etc/inetd.conf, ktorá automaticky spúšťa túto službu.	/etc/security/pscexpert/bin/cominetdconf
PCI verzia 2 1.1.5 2.2.2 **PCI verzia 3** 2.2.2	Zakázať nepotrebné a nie bezpečné služby, ktoré zahŕňajú službu TCP chargen.	Zastaví a zakáže všetky inštancie služby chargen(tcp). Pomocný program AIX Security Expert tiež označí ako komentár príslušnú položku v súbore /etc/inetd.conf, ktorá automaticky spúšťa túto službu.	/etc/security/pscexpert/bin/cominetdconf
PCI verzia 2 1.1.5 2.2.2 **PCI verzia 3** 2.2.2	Zakázať nepotrebné a nie bezpečné služby, ktoré zahŕňajú službu TCP daytime.	Zastaví a zakáže všetky inštancie služby daytime(tcp). Pomocný program AIX Security Expert tiež označí ako komentár príslušnú položku v súbore /etc/inetd.conf, ktorá automaticky spúšťa túto službu.	/etc/security/pscexpert/bin/cominetdconf

Tabuľka 6. Nastavenia súvisiace so štandardmi súladu s PCI DSS verzia 2.0 a verzia 3.0 (pokračovanie)

Implementuje tieto štandardy PCI DSS	Špecifikácia implementácie	Implementácia AIX Security Expert	Umiestnenie skriptu, ktorý modifikuje hodnotu
PCI verzia 2 1.1.5 2.2.2 **PCI verzia 3** 2.2.2	Zakázať nepotrebné a nie bezpečné služby, ktoré zahŕňajú službu TCP time.	Zastaví a zakáže všetky inštancie služby timed(tcp). Pomocný program AIX Security Expert tiež označí ako komentár príslušnú položku v súbore /etc/inetd.conf, ktorá automaticky spúšťa túto službu.	/etc/security/pscexpert/bin/cominetdconf
PCI verzia 2 1.1.5 2.2.2 **PCI verzia 3** 2.2.2	Zakázať nepotrebné a nie bezpečné služby, ktoré zahŕňajú službu UDP echo.	Zastaví a zakáže všetky inštancie služby echo(udp). Pomocný program AIX Security Expert tiež označí ako komentár príslušnú položku v súbore /etc/inetd.conf, ktorá automaticky spúšťa túto službu.	/etc/security/pscexpert/bin/cominetdconf
PCI verzia 2 1.1.5 2.2.2 **PCI verzia 3** 2.2.2	Zakázať nepotrebné a nie bezpečné služby, ktoré zahŕňajú službu UDP discard.	Zastaví a zakáže všetky inštancie služby discard(udp). Pomocný program AIX Security Expert tiež označí ako komentár príslušnú položku v súbore /etc/inetd.conf, ktorá automaticky spúšťa túto službu.	/etc/security/pscexpert/bin/cominetdconf
PCI verzia 2 1.1.5 2.2.2 **PCI verzia 3** 2.2.2	Zakázať nepotrebné a nie bezpečné služby, ktoré zahŕňajú službu UDP chargen.	Zastaví a zakáže všetky inštancie služby chargen(udp). Pomocný program AIX Security Expert tiež označí ako komentár príslušnú položku v súbore /etc/inetd.conf, ktorá automaticky spúšťa túto službu.	/etc/security/pscexpert/bin/cominetdconf
PCI verzia 2 1.1.5 2.2.2 **PCI verzia 3** 2.2.2	Zakázať nepotrebné a nie bezpečné služby, ktoré zahŕňajú službu UDP daytime.	Zastaví a zakáže všetky inštancie služby daytime(udp). Pomocný program AIX Security Expert tiež označí ako komentár príslušnú položku v súbore /etc/inetd.conf, ktorá automaticky spúšťa túto službu.	/etc/security/pscexpert/bin/cominetdconf
PCI verzia 2 1.1.5 2.2.2 **PCI verzia 3** 2.2.2	Zakázať nepotrebné a nie bezpečné služby, ktoré zahŕňajú službu UDP time.	Zastaví a zakáže všetky inštancie služby timed(udp). Pomocný program AIX Security Expert tiež označí ako komentár príslušnú položku v súbore /etc/inetd.conf, ktorá automaticky spúšťa túto službu.	/etc/security/pscexpert/bin/cominetdconf
PCI verzia 2 1.1.5 2.2.2 **PCI verzia 3** 2.2.3	Zakázať nepotrebné a nie bezpečné služby, ktoré zahŕňajú službu FTP.	Zastaví a zakáže všetky inštancie démona ftpd. Pomocný program AIX Security Expert tiež označí ako komentár príslušnú položku v súbore /etc/inetd.conf, ktorá automaticky spúšťa tohto démona.	/etc/security/pscexpert/bin/cominetdconf
PCI verzia 2 1.1.5 2.2.2 **PCI verzia 3** 2.2.3	Zakázať nepotrebné a nie bezpečné služby, ktoré zahŕňajú službu telnet.	Zastaví a zakáže všetky inštancie démona telnetd. Pomocný program AIX Security Expert tiež označí ako komentár príslušnú položku v súbore /etc/inetd.conf, ktorá automaticky spúšťa tohto démona.	/etc/security/pscexpert/bin/cominetdconf

Tabuľka 6. Nastavenia súvisiace so štandardmi súladu s PCI DSS verzia 2.0 a verzia 3.0 (pokračovanie)

Implementuje tieto štandardy PCI DSS	Špecifikácia implementácie	Implementácia AIX Security Expert	Umiestnenie skriptu, ktorý modifikuje hodnotu
PCI verzia 2 1.1.5 2.2.2 **PCI verzia 3** 2.2.2	Zakázať nepotrebné a nie bezpečné služby, ktoré zahŕňajú démona dtspc.	Zastaví a zakáže všetky inštancie démona dtspc. Pomocný program AIX Security Expert tiež označí ako komentár príslušnú položku v súbore /etc/inittab, ktorá automaticky spúšťa démona, keď nie je nakonfigurovaný mechanizmus LFT a funkcia CDE je zakázané v súbore /etc/inittab.	/etc/security/pscexpert/bin/cominetdconf
PCI verzia 2 1.1.5 2.2.2 **PCI verzia 3** 2.2.2	Zakázať nepotrebné a nie bezpečné služby, ktoré zahŕňajú službu ttdbserver.	Zastaví a zakáže všetky inštancie služby ttdbserver. Pomocný program AIX Security Expert tiež označí ako komentár príslušnú položku v súbore /etc/inetd.conf, ktorá automaticky spúšťa túto službu.	/etc/security/pscexpert/bin/cominetdconf
PCI verzia 2 1.1.5 2.2.2 **PCI verzia 3** 2.2.2	Zakázať nepotrebné a nie bezpečné služby, ktoré zahŕňajú službu cmsd.	Zastaví a zakáže všetky inštancie služby cmsd. Pomocný program AIX Security Expert tiež označí ako komentár príslušnú položku v súbore /etc/inetd.conf, ktorá automaticky spúšťa túto službu.	/etc/security/pscexpert/bin/cominetdconf
PCI verzia 2 2.2.3 **PCI verzia 3** 2.2.4	Nakonfigurovať bezpečnostné parametre systému na zabránenie zneužitiu.	Odstráni príkazy SUID (Set User ID) označením príslušnej položky ako komentára v súbore /etc/inetd.conf, ktorá automaticky povoľuje tieto príkazy.	/etc/security/pscexpert/bin/rmsuidfrmrcmds
PCI verzia 2 2.2.3 **PCI verzia 3** 2.2.4	Nakonfigurovať bezpečnostné parametre systému na zabránenie zneužitiu.	Povoľuje najnižšiu úroveň zabezpečenia pre File Permissions Manager.	/etc/security/pscexpert/bin/filepermgr
PCI verzia 2 2.2.3 **PCI verzia 3** 2.2.4	Nakonfigurovať bezpečnostné parametre systému na zabránenie zneužitiu.	Modifikuje protokol Network File System s obmedzenými nastaveniami, ktoré sú v súlade s bezpečnostnými požiadavkami PCI. Tieto obmedzené nastavenia zahŕňajú zakázanie vzdialeného prístupu užívateľa root a anonymného prístupu UID a GID.	/etc/security/pscexpert/bin/nfsconfig
PCI verzia 2 2.2.2 **PCI verzia 3** 2.2.3	Povoliť len potrebné a bezpečné služby, protokoly, démonov atď. tak, ako to vyžaduje správne fungovanie systému. Implementovať bezpečnostné funkcie pre všetky požadované služby, protokoly alebo démonov, ktoré nie sú považované za bezpečné.	Zakazuje démonov rlogind, rshd a tftpd, ktorí nie sú bezpeční.	/etc/security/pscexpert/bin/disrmtdmns

Tabuľka 6. Nastavenia súvisiace so štandardmi súladu s PCI DSS verzia 2.0 a verzia 3.0 (pokračovanie)

Implementuje tieto štandardy PCI DSS	Špecifikácia implementácie	Implementácia AIX Security Expert	Umiestnenie skriptu, ktorý modifikuje hodnotu
PCI verzia 2 2.2.2 **PCI verzia 3** 2.2.3	Povoliť len potrebné a bezpečné služby, protokoly, démonov atď. tak, ako to vyžaduje správne fungovanie systému. Implementovať bezpečnostné funkcie pre všetky požadované služby, protokoly alebo démonov, ktoré nie sú považované za bezpečné.	Zakazuje démonov rlogind, rshd a tftpd, ktorí nie sú bezpeční.	/etc/security/pscexpert/bin/rmrhostsnetrc
PCI verzia 2 2.2.2 **PCI verzia 3** 2.2.3	Povoliť len potrebné a bezpečné služby, protokoly, démonov atď. tak, ako to vyžaduje správne fungovanie systému. Implementovať bezpečnostné funkcie pre všetky požadované služby, protokoly alebo démonov, ktoré nie sú považované za bezpečné.	Zakazuje démonov logind, rshd a tftpdpci_rmetchostsequiv, ktorí nie sú bezpeční.	/etc/security/pscexpert/bin/rmetchostsequiv
PCI verzia 2 1.3.6 **PCI verzia 3** 2.2.3	Implementovať stavovú kontrolu, alebo filtrovanie paketov, pri ktorom sú v sieti povolené len vybudované spojenia.	Povoľuje sieťovú voľbu **clean_partial_conns** nastavením jej hodnoty na 1.	/etc/security/pscexpert/bin/ntwkopts
PCI verzia 2 2.2.2 **PCI verzia 3** 2.2.3	Implementovať stavovú kontrolu, alebo filtrovanie paketov, pri ktorom sú v sieti povolené len vybudované spojenia.	Povoľuje bezpečnosť TCP nastavením sieťovej voľby **tcp_tcpsecure** na hodnotu 7. Toto nastavenie poskytuje ochranu proti útokom na údaje, reset (RST) a požiadavkám o pripojenie TCP (SYN).	/etc/security/pscexpert/bin/ntwkopts
1.2	Chrániť proti neautorizovanému prístupu na nepoužívaných portoch.	Konfiguruje systém, aby zablokoval hostiteľov po dobu 5 minút, aby zabránil iným systémom v prístupe k nepoužívaným portom.	/etc/security/pscexpert/bin/ipsecshunhosthls **Poznámka:** Môžete zadať ďalšie pravidlá filtrovania v súbore /etc/security/aixpert/bin/filter.txt. Tieto pravidlá integruje skript ipsecshunhosthls.sh, keď použijete tento profil. Položky by mali byť v nasledujúcom formáte: *číslo_portu*:*ip_adresa*:*akcia* , kde možné hodnoty pre premennú *akcia* sú Allow alebo Deny.
1.2	Chrániť hostiteľa pred skenovaním portov.	Konfiguruje systém, aby zablokoval nechránené porty po dobu 5 minút, čo zabráni skenovaniu portov.	/etc/security/pscexpert/bin/ipsecshunports **Poznámka:** Môžete zadať ďalšie pravidlá filtrovania v súbore /etc/security/aixpert/bin/filter.txt. Tieto pravidlá integruje skript ipsecshunhosthls.sh, keď použijete tento profil. Položky by mali byť v nasledujúcom formáte: *číslo_portu*:*ip_adresa*:*akcia* , kde možné hodnoty pre premennú *akcia* sú Allow alebo Deny.
7.1.1	Obmedziť oprávnenia na vytváranie objektov.	Nastavuje predvolené oprávnenia na vytváranie objektov na 22 nastavením parametra **umask** na hodnotu 22.	/etc/security/pscexpert/bin/chusrattr

Tabuľka 6. Nastavenia súvisiace so štandardmi súladu s PCI DSS verzia 2.0 a verzia 3.0 (pokračovanie)

Implementuje tieto štandardy PCI DSS	Špecifikácia implementácie	Implementácia AIX Security Expert	Umiestnenie skriptu, ktorý modifikuje hodnotu
7.1.1	Obmedziť prístup k systému.	Zabezpečuje, že ID root je jediný identifikátor, ktorý je uvedený v súbore cron.allow, a odstráni súbor cron.deny zo systému.	/etc/security/pscexpert/bin/limitsysacc
6.5.8	Odstrániť znak bodky z koreňového adresára cesty.	Odstráni znak bodky z premennej prostredia PATH v nasledujúcich súboroch, ktoré sa nachádzajú v domovskom adresári užívateľa root: • .cshrc • .kshrc • .login • .profile	/etc/security/pscexpert/bin/rmdotfrmpathroot
6.5.8	Odstrániť znak bodky z nekoreňového adresára cesty.	Odstráni znak bodky z premennej prostredia *PATH* v nasledujúcich súboroch, ktoré sú v domovskom adresári užívateľa: • .cshrc • .kshrc • .login • .profile	/etc/security/pscexpert/bin/rmdotfrmpathnroot
2.2.3	Obmedziť prístup k systému.	Pridáva schopnosť užívateľa root a meno užívateľa do súboru /etc/ftpusers.	/etc/security/pscexpert/bin/chetcftpusers
2.1	Odstrániť konto guest.	Odstráni konto guest a jeho súbory.	/etc/security/pscexpert/bin/execmds
6.5.2	Zabrániť spúšťaniu programov v obsahovom priestore.	Povoľuje funkciu SED (stack execution disable).	/etc/security/pscexpert/bin/sedconfig
8.2	Zabezpečiť, že heslo pre užívateľa root nie je slabé.	Spustí kontrolu integrity hesla užívateľa root oproti heslu užívateľa root, a tak zabezpečí silné heslo užívateľa root.	/etc/security/pscexpert/bin/chuserstanza
PCI verzia 2 8.5.15 **PCI verzia 3** 8.1.8	Obmedziť prístup k systému nastavením času neaktivity relácie.	Nastaví obmedzenie času neaktivity na 15 minút. Ak je relácia neaktívna viac než 15 minút, musíte znova zadať heslo.	/etc/security/pscexpert/bin/autologoff
1.3.5	Obmedziť prístup k informáciám držiteľov kariet.	Nastaví reguláciu premávky TCP na vysoké nastavenie, čím dôjde k minimalizácii rizika útokov DoS na portoch.	/etc/security/pscexpert/bin/tcptr_pscexpert
1.3.5	Zachovať bezpečné spojenie počas migrácie údajov.	Povoľuje automatizované vytvorenie tunela IP Security (IPSec) medzi servermi Virtual I/O Server počas živej migrácie oddielov.	/etc/security/pscexpert/bin/cfgsecmig
1.3.5	Obmedziť pakety z neznámych zdrojov.	Povoľuje pakety z konzoly Hardware Management Console.	/etc/security/pscexpert/bin/ipsecpermithostorport
5.1.1	Udržiavať antivírusový softvér.	Udržiava integritu systému zisťovaním, odstraňovaním a ochranou proti známym typom škodlivého softvéru.	/etc/security/pscexpert/bin/manageITsecurity

Tabuľka 6. Nastavenia súvisiace so štandardmi súladu s PCI DSS verzia 2.0 a verzia 3.0 (pokračovanie)

Implementuje tieto štandardy PCI DSS	Špecifikácia implementácie	Implementácia AIX Security Expert	Umiestnenie skriptu, ktorý modifikuje hodnotu
PCI verzia 2 Časť 7 **PCI verzia 3** Časť 7	Udržiavať prístup na základe potreby.	Povoliť RBAC (role-based access control) vytvorením rolí užívateľa operátor systému, správca systému a správca bezpečnosti informačného systému s požadovanými oprávneniami.	/etc/security/pscexpert/bin/EnableRbac
PCI verzia 2 Nezahrnuté v profile verzie 2, pridané vo verzii 3. **PCI verzia 3** 2.3	Implementovať ďalšie bezpečnostné funkcie pre všetky požadované služby, protokoly alebo démonov, ktoré nie sú považované za bezpečné.	Používa bezpečné technológie, ako je Secure Shell (SSH), SSH File Transfer Protocol (S-FTP), Secure Sockets Layer (SSL) alebo Internet Protocol Security Virtual Private Network (IPsec VPN) na ochranu nie bezpečných služieb, ako je NetBIOS, zdieľanie súborov, Telnet a FTP. Okrem toho nakonfiguruje démona SSH na používanie len protokolu SSHv2.	/etc/security/pscexpert/bin/sshPCIconfig
PCI verzia 2 Nezahrnuté v profile verzie 2, pridané vo verzii 3. **PCI verzia 3** 2.3	Klient SSH musí byť nakonfigurovaný na používanie len protokolu SSHv2.	Konfiguruje klienta SSH na používanie protokolu SSHv2.	/etc/security/pscexpert/bin/sshPCIconfig
PCI verzia 2 Nezahrnuté v profile verzie 2, pridané vo verzii 3. **PCI verzia 3** 2.3	Démon SSH musí načúvať len na riadiacich sieťových adresách, pokiaľ nie je autorizovaný pre používanie iných než riadiacich.	Zabezpečuje, že démon SSH je nastavený len na načúvanie.	/etc/security/pscexpert/bin/sshPCIconfig
PCI verzia 2 Nezahrnuté v profile verzie 2, pridané vo verzii 3. **PCI verzia 3** 2.3	Démon SSH musí byť nakonfigurovaný na používanie len šifier schválených FIPS 140-2	Zabezpečuje, že démon SSH používa len šifry FIPS 140-2.	/etc/security/pscexpert/bin/sshPCIconfig
PCI verzia 2 Nezahrnuté v profile verzie 2, pridané vo verzii 3. **PCI verzia 3** 2.3	Démon SSH musí byť nakonfigurovaný na používanie len kódov MAC (Message Authentication Code), ktoré uplatňujú šifrovací hashovací algoritmus schválený FIPS 140-2.	Zabezpečuje, že kódy MAC používajú schválený algoritmus.	/etc/security/pscexpert/bin/sshPCIconfig
PCI verzia 2 Nezahrnuté v profile verzie 2, pridané vo verzii 3. **PCI verzia 3** 2.3	Démon SSH musí obmedziť schopnosť prihlásenia pre špecifických užívateľov alebo skupiny.	Obmedzuje prihlásenie do systému pre špecifických užívateľov a skupiny.	/etc/security/pscexpert/bin/sshPCIconfig

Tabuľka 6. Nastavenia súvisiace so štandardmi súladu s PCI DSS verzia 2.0 a verzia 3.0 (pokračovanie)

Implementuje tieto štandardy PCI DSS	Špecifikácia implementácie	Implementácia AIX Security Expert	Umiestnenie skriptu, ktorý modifikuje hodnotu
PCI verzia 2 Nezahrnuté v profile verzie 2, pridané vo verzii 3. **PCI verzia 3** 2.3	Systém musí pri prihlásení zobraziť dátum a čas posledného úspešného prihlásenia konta.	Uchováva informácie z posledného úspešného prihlásenia a zobrazuje ich po nasledujúcom úspešnom prihlásení.	/etc/security/pscexpert/bin/sshPCIconfig
PCI verzia 2 Nezahrnuté v profile verzie 2, pridané vo verzii 3. **PCI verzia 3** 2.3	Démon SSH musí vykonať striktnú kontrolu režimu konfiguračných súborov domovského adresára.	Zabezpečí, že konfiguračné súbory domovského adresára sú nastavené na správny režim.	/etc/security/pscexpert/bin/sshPCIconfig
PCI verzia 2 Nezahrnuté v profile verzie 2, pridané vo verzii 3. **PCI verzia 3** 2.3	Démon SSH musí používať oddelenie privilégií.	Zabezpečí, že démon SSH má správny počet oddelení jeho privilégií.	/etc/security/pscexpert/bin/sshPCIconfig
PCI verzia 2 Nezahrnuté v profile verzie 2, pridané vo verzii 3. **PCI verzia 3** 2.3	Démon SSH nesmie povoliť, aby mal súbor rhosts autentifikáciu RSA.	Zakáže autentifikáciu RSA pre súbor rhosts, keď používate démona SSH.	/etc/security/pscexpert/bin/sshPCIconfig
PCI verzia 2 1.1.5 2.2.2 **PCI verzia 3** 10.4	Preskúmať konfiguračné štandardy a procesy na overenie, že je implementovaná a udržiavaná aktuálna technológia na synchronizáciu času a podľa požiadaviek PCI DSS 6.1 a 6.2.	Povoľuje démona ntp.	/etc/security/pscexpert/bin/rctcpip
PCI verzia 2 Nezahrnuté v profile verzie 2, pridané vo verzii 3. **PCI verzia 3** 8.1.5	Zakázať užívateľské konto, keď sa nepoužíva.	Zakáže užívateľské kontá po 35 dňoch neaktivity.	/etc/security/pscexpert/bin/disableacctpci
PCI verzia 3 2.2.3	Zakázať SSL (Secure Sockets Layer) v3 a TLS (Transport Layer Security) v1.0 v aplikáciách.	Zakáže verzie SSLv3 a TLS v1.0 v konfigurácii Courier POP3 server (Pop3d).	/etc/security/pscexpert/bin/disableSSL
PCI verzia 3 2.2.3	Zakázať SSL v3 a TLS v1.0 v aplikáciách.	Zakáže SSLV3 a TLS v1.0 v serveri Courier IMAP (imapd).	/etc/security/pscexpert/bin/disableSSL

Tabuľka 6. Nastavenia súvisiace so štandardmi súladu s PCI DSS verzia 2.0 a verzia 3.0 (pokračovanie)

Implementuje tieto štandardy PCI DSS	Špecifikácia implementácie	Implementácia AIX Security Expert	Umiestnenie skriptu, ktorý modifikuje hodnotu
PCI verzia 3 8.2.1	Zakázať SSL v3 a TLS v1.0 v aplikáciách.	Skontroluje konfiguračný súbor protokolu NTP (Network Time Protocol) pre implementáciu zabezpečenia protokolom TLS 1.1 alebo novším.	/etc/security/pscexpert/bin/checkNTP
PCI verzia 3 2.2.3	Zakázať SSL v3 a TLS v1.0 v aplikáciách.	Skontroluje konfiguračný súbor FTPD (File Transfer Protocol Daemon) pre implementáciu zabezpečenia protokolom TLS 1.1 alebo novším.	/etc/security/pscexpert/bin/secureFTP
PCI verzia 3 2.2.3	Zakázať SSL v3 a TLS v1.0 v aplikáciách.	Skontroluje konfiguračný súbor protokolu FTP (File Transfer Protocol) pre implementáciu zabezpečenia protokolom TLS 1.1 alebo novším.	/etc/security/pscexpert/bin/secureFTP
PCI verzia 3 2.2.3	Zakázať SSL v3 a TLS v1.0 v aplikáciách.	Zakázať SSLv3 a TLS v1.0 v konfigurácii programu sendmail.	/etc/security/pscexpert/bin/sendmailPCIConfig
PCI verzia 3 2.2.3	Zakázať SSL v3 a TLS v1.0 v aplikáciách.	Skontrolovať, či je verzia SSL na AIX väčšia než 1.0.2.	/etc/security/pscexpert/bin/sslversion
PCI verzia 3 8.2.1	Vynútiť dvojfaktorovú autentifikáciu.	Vynútiť dvojfaktorovú autentifikáciu ako je SHA-256 alebo SHA-512.	/etc/security/pscexpert/bin/pwdalgchk

Súvisiace informácie:

Súlad s požiadavkami normy Payment Card Industry - Data Security Standard

Súlad s požiadavkami normy Sarbanes-Oxley Act a COBIT (SOX-COBIT)

Zákon Sarbanes-Oxley (SOX) Act z roku 2002 vyplývajúci zo 107. kongresu Spojených štátov amerických upravuje audit verejných spoločností, ktoré podliehajú právnym predpisom o cenných papieroch a súvisiacich záležitostiach, v záujme ochrany záujmov investorov.

Sekcia 404 zákona SOX nariaďuje hodnotenie interných kontrolných mechanizmov. V prípade väčšiny organizácií interné kontrolné mechanizmy pokrývajú systémy informačných technológií, ktoré spracovávajú a vykazujú finančné údaje spoločnosti. Zákon SOX poskytuje konkrétne nariadenia týkajúce sa prostredí IT a ich zabezpečenia. Mnoho audítorov zameriavajúcich sa na zákon SOX sa spolieha na normy, akou je COBIT, ktorá predstavuje spôsob merania a auditovania správnosti riadenia a kontroly IT prostredia. Konfiguračná voľba The PowerSC Standard Edition SOX/COBIT XML poskytuje konfiguráciu zabezpečenia systémov AIX a Virtual I/O Server (VIOS potrebnú na splnenie požiadaviek normy COBIT.

Softvér IBM Compliance Expert Express Edition podporuje nasledujúce verzie operačného systému AIX:

- AIX 6.1
- AIX 7.1
- AIX 7.2

Zabezpečenie súladu s externými normami je zodpovednosťou administrátora systému AIX. Softvér IBM Compliance Expert Express Edition uľahčuje správu nastavení operačného systému a zostáv, ktoré sú potrebné na zabezpečenie súladu s týmito normami.

Vopred nakonfigurované profily súladu poskytované so softvérom IBM Compliance Expert Express Edition uľahčujú správu tým, že eliminujú potrebu preštudovať si dokumentáciu k normám a implementovať tieto normy ako konkrétne konfiguračné parametre systému.

Funkcie softvéru IBM Compliance Expert Express Edition sú navrhnuté tak, aby klientom pomáhali efektívne spravovať systémové požiadavky súvisiace so súladom s externými normami, vďaka čomu môžu znížiť výdavky a zároveň zlepšiť mieru súladu. Všetky externé bezpečnostné normy sa vzťahujú iné aspekty ako konfiguračné nastavenia systému. Samotné používanie softvéru IBM Compliance Expert Express Edition nezaručuje súlad s týmito normami. Účelom softvéru Compliance Expert je zjednodušenie správy konfiguračných nastavení systému, aby sa administrátori mohli zamerať na iné aspekty súladu s normami.

Súvisiace informácie:

Súlad s požiadavkami normy COBIT

Health Insurance Portability and Accountability Act (HIPAA)

HIPAA (Health Insurance Portability and Accountability Act) je bezpečnostný profil zameraný na ochranu elektronicky chránených zdravotných informácií (EPHI).

Bezpečnostné pravidlo HIPAA sa špecificky zameriava na ochranu informácií EPHI, pričom Bezpečnostnému pravidlu HIPAA podlieha iba niekoľko agentúr, a to v závislosti od ich funkcie a používania informácií EPHI.

Všetky entity, na ktoré sa vzťahujú pravidlá HIPAA, podobne ako niektoré federálne agentúry, musia dodržiavať Bezpečnostné pravidlo HIPAA.

Bezpečnostné pravidlo HIPAA sa zameriava na ochranu dôvernosti, integrity a dostupnosti informácií EPHI, ako je definované v Bezpečnostnom pravidle.

Informácie EPHI vytvorené, prijaté, spravované alebo odosielané príslušnou entitou musia byť chránené pred primerane predvídateľnými hrozbami, nebezpečenstvami a neprípustnými použitiami a vyzradením.

Požiadavky, štandardy a špecifikácie implementácie Bezpečnostného pravidla HIPAA sa vzťahujú na nasledujúce pokryté entity:

- poskytovatelia zdravotnej starostlivosti
- zdravotné poisťovne
- schvaľovacie orgány v zdravotníctve
- vystavovatelia predpisov liečiv a liečebných záznamov

Nasledujúca tabuľka uvádza podrobné informácie o niektorých častiach Bezpečnostného pravidla HIPAA, pričom každá časť pokrýva niekoľko štandardov a špecifikácií implementácie.

Poznámka: Všetky súbory vlastných skriptov na zabezpečenie súladu s požiadavkami pravidiel HIPAA sú uložené v adresári /etc/security/pscexpert/bin.

Tabuľka 7. Podrobnosti o pravidlách HIPAA a ich implementácii

Časti Bezpečnostného pravidla HIPAA	Špecifikácia implementácie	Implementácia aixpert	Príkazy a návratové hodnoty
164.308 (a) (1) (ii) (D) 164.308 (a) (5) (ii) (C) 164.312 (b)	Implementuje procedúry na pravidelnú kontrolu záznamov o aktivite informačných systémov, ako sú protokoly z auditu, správy o prístupe a správy o bezpečnostných incidentoch.	Určuje, či je povolené auditovanie v systéme.	**Príkaz**: **#audit query**. **Návratová hodnota**: Ak je príkaz úspešný, ukončí sa s hodnotou 0. Ak príkaz nie je úspešný, ukončí sa s hodnotou 1.

Tabuľka 7. Podrobnosti o pravidlách HIPAA a ich implementácii (pokračovanie)

Časti Bezpečnostného pravidla HIPAA	Špecifikácia implementácie	Implementácia aixpert	Príkazy a návratové hodnoty
164.308 (a) (1) (ii) (D) 164.308 (a) (5) (ii) (C) 166.312 (b)	Implementuje procedúry na pravidelnú kontrolu záznamov o aktivite informačných systémov, ako sú protokoly z auditu, správy o prístupe a správy o bezpečnostných incidentoch.	Povolí auditovanie v systéme. Taktiež nakonfiguruje zaznamenávané udalosti.	**Príkaz**: **# audit start >/dev/null 2>&1**. **Návratová hodnota**: Ak je príkaz úspešný, ukončí sa s hodnotou 0. Ak príkaz nie je úspešný, ukončí sa s hodnotou 1. Auditované budú nasledujúce udalosti: **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)	Šifrovanie a dešifrovanie (A):Implementuje mechanizmus na šifrovanie a dešifrovanie informácií EPHI.	Určuje, či je v systéme povolený šifrovaný súborový systém (EFS).	**Príkaz**: **# efskeymgr -V >/dev/null 2>&1**. **Návratová hodnota**: Ak je súborový systém EFS už povolený, príkaz sa ukončí s hodnotou 0. Ak súborový systém EFS nie je povolený, príkaz sa ukončí s hodnotou 1.
164.312 (a) (2) (iii)	Automatické odhlásenie (A): Implementuje elektronické postupy na ukončenie elektronickej relácie po uplynutí vopred definovaného obdobia nečinnosti.	Nakonfiguruje systém pre odhlásenie z interaktívnych procesov po 15 minútach nečinnosti.	**Príkaz**: **grep TMOUT= /etc/security /.profile > /dev/null 2>&1** **echo "TMOUT=900 ; TIMEOUT=900; export TMOUT TIMEOUT**. **Návratová hodnota**: Ak príkaz nedokáže nájsť hodnotu **TMOUT=15**, skript sa ukončí s hodnotou 1. V opačnom prípade sa príkaz ukončí s hodnotou 0.
164.308 (a) (5) (ii) (D) 164.312 (a) (2) (i)	Správa hesiel (A):Implementuje postupy pre vytváranie, zmenu a ochranu hesiel.	Zabezpečuje, že všetky heslá budú obsahovať aspoň 14 znakov.	**Príkaz**: **chsec -f /etc/security/user -s user -a minlen=8**. **Návratová hodnota**: Ak je príkaz úspešný, skript sa ukončí s hodnotou 0. Ak nie je úspešný, skript sa ukončí s kódom chyby 1.
164.308 (a) (5) (ii) (D) 164.312 (a) (2) (i)	Správa hesiel (A):Implementuje postupy pre vytváranie, zmenu a ochranu hesiel.	Zabezpečuje, že všetky heslá budú obsahovať aspoň dva abecedné znaky, pričom jeden z nich musí byť veľké písmeno.	**Príkaz**: **chsec -f /etc/security/user -s user –a minalpha=4**. **Návratová hodnota**: Ak je príkaz úspešný, skript sa ukončí s hodnotou 0. Ak nie je úspešný, príkaz sa ukončí s kódom chyby 1.
164.308 (a) (5) (ii) (D) 164.312 (a) (2) (i)	Správa hesiel (A):Implementuje postupy pre vytváranie, zmenu a ochranu hesiel.	Určuje, že minimálny počet neabecedných znakov v hesle je 2.	**Príkaz**: **#chsec –f /etc/security/user –s user –a minother=2**. **Návratová hodnota**: Ak je príkaz úspešný, skript sa ukončí s hodnotou 0. Ak nie je úspešný, príkaz sa ukončí s kódom chyby 1.

Tabuľka 7. Podrobnosti o pravidlách HIPAA a ich implementácii (pokračovanie)

Časti Bezpečnostného pravidla HIPAA	Špecifikácia implementácie	Implementácia aixpert	Príkazy a návratové hodnoty
164.308 (a) (5) (ii) (D) 164.312 (a) (2) (i)	Správa hesiel (A):Implementuje postupy pre vytváranie, zmenu a ochranu hesiel.	Zabezpečuje, že žiadne heslá nebudú obsahovať opakujúce sa znaky.	**Príkaz**: **#chsec –f /etc/security/user –s user –a maxrepeats=1**. **Návratová hodnota**: Ak je príkaz úspešný, skript sa ukončí s hodnotou 0. Ak nie je úspešný, príkaz sa ukončí s kódom chyby 1.
164.308 (a) (5) (ii) (D) 164.312 (a) (2) (i)	Správa hesiel (A):Implementuje postupy pre vytváranie, zmenu a ochranu hesiel.	Zabezpečuje, že heslo nebude znova použité v rámci piatich posledných zmien.	**Príkaz**: **#chsec –f /etc/security/user –s user –a histsize=5**. **Návratová hodnota**: Ak je príkaz úspešný, skript sa ukončí s hodnotou 0. Ak nie je úspešný, príkaz sa ukončí s kódom chyby 1.
164.308 (a) (5) (ii) (D) 164.312 (a) (2) (i)	Správa hesiel (A):Implementuje postupy pre vytváranie, zmenu a ochranu hesiel.	Stanovuje maximálnu dobu platnosti hesla 13 týždňov.	**Príkaz**: **#chsec –f /etc/security/user –s user –a maxage=8**. **Návratová hodnota**: Ak je príkaz úspešný, skript sa ukončí s hodnotou 0. Ak nie je úspešný, príkaz sa ukončí s kódom chyby 1.
164.308 (a) (5) (ii) (D) 164.312 (a) (2) (i)	Správa hesiel (A):Implementuje postupy pre vytváranie, zmenu a ochranu hesiel.	Odstráni požiadavku minimálneho počtu týždňov pred zmenou hesla.	**Príkaz**: **#chsec –f /etc/security/user –s user –a minage=2**. **Návratová hodnota**: Ak je príkaz úspešný, skript sa ukončí s hodnotou 0. Ak nie je úspešný, príkaz sa ukončí s kódom chyby 1.
164.308 (a) (5) (ii) (D) 164.312 (a) (2) (i)	Správa hesiel (A):Implementuje postupy pre vytváranie, zmenu a ochranu hesiel.	Nastaví maximálny počet týždňov na zmenu hesla so skončenou platnosťou na 4 týždne po uplynutí doby určenej hodnotou parametra **maxage** užívateľa.	**Príkaz**: **#chsec –f /etc/security/user –s user –a maxexpired=4**. **Návratová hodnota**: Ak je príkaz úspešný, skript sa ukončí s hodnotou 0. Ak nie je úspešný, príkaz sa ukončí s kódom chyby 1.
164.308 (a) (5) (ii) (D) 164.312 (a) (2) (i)	Správa hesiel (A):Implementuje postupy pre vytváranie, zmenu a ochranu hesiel.	Určuje, že minimálny počet znakov, ktoré sa nemôžu opakovať zo starého hesla, je 4.	**Príkaz**: **#chsec –f /etc/security/user –s user –a mindiff=4**. **Návratová hodnota**: Ak je príkaz úspešný, skript sa ukončí s hodnotou 0. Ak nie je úspešný, príkaz sa ukončí s kódom chyby 1.
164.308 (a) (5) (ii) (D) 164.312 (a) (2) (i)	Správa hesiel (A):Implementuje postupy pre vytváranie, zmenu a ochranu hesiel.	Určuje, že systém má zobraziť varovanie o potrebe zmeniť heslo po 5 dňoch.	**Príkaz**: **#chsec –f /etc/security/user –s user –a pwdwarntime = 5**. **Návratová hodnota**: Ak je príkaz úspešný, skript sa ukončí s hodnotou 0. Ak nie je úspešný, príkaz sa ukončí s kódom chyby 1.
164.308 (a) (5) (ii) (D) 164.312 (a) (2) (i)	Správa hesiel (A):Implementuje postupy pre vytváranie, zmenu a ochranu hesiel.	Overí správnosť užívateľských definícií a opraví chyby.	**Príkaz**: **/usr/bin/usrck -y ALL** **/usr/bin/usrck –n ALL**. **Return value**: Príkaz nevracia žiadnu hodnotu. Príkaz vyhľadá a opraví prípadné chyby.

Tabuľka 7. Podrobnosti o pravidlách HIPAA a ich implementácii (pokračovanie)

Časti Bezpečnostného pravidla HIPAA	Špecifikácia implementácie	Implementácia aixpert	Príkazy a návratové hodnoty
164.308 (a) (5) (ii) (D) 164.312 (a) (2) (i)	Správa hesiel (A):Implementuje postupy pre vytváranie, zmenu a ochranu hesiel.	Uzamkne konto po troch po sebe nasledujúcich neúspešných pokusoch o prihlásenie.	**Príkaz**: **#chsec –f /etc/security/user –s user –a loginretries=3**. **Návratová hodnota**: Ak je príkaz úspešný, skript sa ukončí s hodnotou 0. Ak nie je úspešný, príkaz sa ukončí s kódom chyby 1.
164.308 (a) (5) (ii) (D) 164.312 (a) (2) (i)	Správa hesiel (A):Implementuje postupy pre vytváranie, zmenu a ochranu hesiel.	Určuje, že oneskorenie po neúspešnom pokuse o prihlásenie má byť 5 sekúnd.	**Príkaz**: **chsec -f /etc/security/login.cfg -s default -a logindelay=5**. **Návratová hodnota**: Ak je príkaz úspešný, skript sa ukončí s hodnotou 0. Ak nie je úspešný, príkaz sa ukončí s kódom chyby 1.
164.308 (a) (5) (ii) (D) 164.312 (a) (2) (i)	Správa hesiel (A):Implementuje postupy pre vytváranie, zmenu a ochranu hesiel.	Určuje, že port sa má zablokovať po 10 neúspešných pokusoch o prihlásenie na porte.	**Príkaz**: **chsec -f /etc/security/lastlog -s username -a \ unsuccessful_login_count=10**. **Návratová hodnota**: Ak je príkaz úspešný, skript sa ukončí s hodnotou 0. Ak nie je úspešný, príkaz sa ukončí s kódom chyby 1.
164.308 (a) (5) (ii) (D) 164.312 (a) (2) (i)	Správa hesiel (A):Implementuje postupy pre vytváranie, zmenu a ochranu hesiel.	Určuje 60-sekundový časový interval na porte pre neúspešné pokusy o prihlásenie pred zakázaním portu.	**Príkaz**: **#chsec -f /etc/security/lastlog -s user –a time_last_unsuccessful_ login=60**. **Návratová hodnota**: Ak je príkaz úspešný, skript sa ukončí s hodnotou 0. Ak nie je úspešný, príkaz sa ukončí s kódom chyby 1.
164.308 (a) (5) (ii) (D) 164.312 (a) (2) (i)	Správa hesiel (A):Implementuje postupy pre vytváranie, zmenu a ochranu hesiel.	Určuje, že port sa má odomknúť 30 minút po zakázaní.	**Príkaz**: **#chsec -f /etc/security/login.cfg -s default -a loginreenable = 30**. **Návratová hodnota**: Ak je príkaz úspešný, skript sa ukončí s hodnotou 0. Ak nie je úspešný, príkaz sa ukončí s kódom chyby 1.
164.308 (a) (5) (ii) (D) 164.312 (a) (2) (i)	Správa hesiel (A):Implementuje postupy pre vytváranie, zmenu a ochranu hesiel.	Určuje 30-sekundový časový interval pre napísanie hesla.	**Príkaz**: **chsec -f /etc/security/login.cfg -s usw -a logintimeout=30**. **Návratová hodnota**: Ak je príkaz úspešný, skript sa ukončí s hodnotou 0. Ak nie je úspešný, príkaz sa ukončí s kódom chyby 1.
164.308 (a) (5) (ii) (D) 164.312 (a) (2) (i)	Správa hesiel (A):Implementuje postupy pre vytváranie, zmenu a ochranu hesiel.	Zabezpečuje, že kontá sa zablokujú po 35 dňoch nečinnosti.	**Príkaz**: **grep TMOUT= /etc/security /.profile > /dev/null 2>&1if TMOUT = (35x24x60x60){#chsec -f /etc/security/user -s user -aaccount_locked = true}**. **Návratová hodnota**: Ak príkaz nedokáže nastaviť hodnotu **account_locked** na **true**, skript sa ukončí s hodnotou 1. V opačnom prípade sa príkaz ukončí s hodnotou 0.

Tabuľka 7. Podrobnosti o pravidlách HIPAA a ich implementácii (pokračovanie)

Časti Bezpečnostného pravidla HIPAA	Špecifikácia implementácie	Implementácia aixpert	Príkazy a návratové hodnoty
164.312 (c) (1)	Implementuje politiky a postupy na ochranu informácii EPHI pred neoprávnenou úpravou alebo zničením.	Nastaviť politiky dôveryhodného vykonávania (TE) na zapnuté.	**Príkaz**: Povolí **CHKEXEC, CHKSHLIB, CHKSCRIPT, CHKKERNEXT, STOP_ON_CHKFAIL,TE=ON For example, trustchk –p TE=ON CHKEXEC = ON, CHKSHLIB,=ON, CHKSCRIPT=ON, CHKKERNEXT = ON**. **Návratová hodnota**: V prípade zlyhania sa skript ukončí s hodnotou 1.
164.312 (e) (1)	Implementuje technické bezpečnostné opatrenia na zamedzenie v neoprávnenom prístupe k informáciám EPHI odosielaným cez elektronickú komunikačnú sieť.	Určuje, či sú nainštalované sady súborov **ssh**. Ak nie sú, zobrazí sa chybové hlásenie.	**Príkaz**: **# lslpp –l | grep openssh > /dev/null 2>&1**. **Návratová hodnota**: Ak je návratový kód z tohto príkazu 0, skript sa ukončí s hodnotou 0. Ak sady súborov ssh nie sú nainštalované, skript sa ukončí s hodnotou 1 a zobrazí sa nasledujúce chybové hlásenie: Install ssh filesets for secure transmission.

Nasledujúca tabuľka uvádza podrobné informácie o niektorých funkciách bezpečnostného pravidla HIPAA, pričom pri každej funkci i sú uvedené štandardy a špecifikácie implementácie.

Tabuľka 8. Podrobnosti o funkciách a implementácii HIPAA

Funkcie HIPAA	Špecifikácia implementácie	Implementácia aixpert	Príkazy a návratové hodnoty
Zaznamenávanie chýb do protokolu	Konsoliduje záznamy o chybách z rozličných protokolov a pošle e-maily administrátorovi.	Určuje, či sa zistili chyby hardvéru. Určuje, či sa vyskytli neodstrániteľné chyby zo súboru **trcfile** v umiestnení /var/adm/ras/trcfile. Pošle chyby na adresu **root@<názov_hostiteľa>**.	**Príkaz**: **errpt -d H**. **Návratová hodnota**: Ak je príkaz úspešný, ukončí sa s hodnotou 0. Ak príkaz nie je úspešný, ukončí sa s hodnotou 1.
Podpora FPM	Zmení oprávnenia pre súbory.	Zmení oprávnenia pre súbory zo zoznamu oprávnení a súborov pomocou príkazu **fpm**.	**Príkaz**: **# fpm -1 <úroveň> -f <súbor s príkazmi>**. **Návratová hodnota**: Ak je príkaz úspešný, ukončí sa s hodnotou 0. Ak príkaz nie je úspešný, ukončí sa s hodnotou 1.
Podpora RBAC	Vytvorí užívateľov **isso**, **so** a **sa** a priradí k nim príslušné roly.	Odporučí, aby ste vytvorili užívateľov **isso**, **so** a **sa**. K užívateľom priradí príslušné roly.	**Príkaz**: **/etc/security/pscexpert/bin/RbacEnablement**.

Súvisiace informácie:

Health Insurance Portability and Accountability Act (HIPAA)

Súlad s požiadavkami organizácie NERC (North American Electric Reliability Corporation)

Organizácie North American Electric Reliability Corporation (NERC) je nezisková spoločnosť, ktorá vyvíja štandardy pre spoločnosti zaoberajúce sa výrobou a distribúciou elektrickej energie. Systém PowerSC Standard Edition obsahuje predkonfigurovaný profil NERC, ktorý poskytuje bezpečnostné štandardy, ktoré môžete použiť na ochranu kľúčových elektrických systémov.

Profil NERC dodržiava štandardy CIP (Critical Infrastructure Protection).

Profil NERC je umiestnený v /etc/security/aixpert/custom/NERC.xml. Požiadavky CIP, ktoré sú aplikované v profile NERC, môžete resetovať na predvolený stav aplikovaním profilu NERC_to_AIXDefault.xml, ktorý je umiestnený v adresári /etc/security/aixpert/custom. Tento proces nie je rovnaký ako operácia zrušenia profilu NERC.

Nasledujúca tabuľka poskytuje informácie o štandardoch CIP, ktoré sú aplikované v operačnom systéme AIX, a ako systém PowerSC Standard Edition zaobchádza so štandardmi CIP:

Tabuľka 9. Štandardy CIP pre PowerSC Standard Edition

Štandard CIP	Implementácia AIX Security Expert	Umiestnenie skriptu, ktorý modifikuje hodnotu
CIP-003-3 R5.1	Konfiguruje bezpečnostné parametre systému na zabránenie problémom odstránením atribútov SUID (set-user identification) a SGID (set-group identification) z binárnych súborov.	• /etc/security/pscexpert/bin/filepermgr • /etc/security/pscexpert/bin/rmsuidfrmrcmds
CIP-003-3 R5.1.1	Povoľuje metódu RBAC (role-based access control) vytvorením rolí systémového operátora, systémového administrátora a správcu bezpečnosti informačného systému s požadovanými oprávneniami.	/etc/security/pscexpert/bin/EnableRbac
CIP-005-3a R2.1-R2.4	Povoľuje Secure Shell (SSH) pre bezpečnostný prístup.	/etc/security/pscexpert/bin/sshstart
CIP-005-3a R2.5 CIP-007-5 R1.1	Zakazuje nasledujúce nepotrebné a nie bezpečné služby: • Démon **lpd** • Common Desktop Environment (CDE)	/etc/security/pscexpert/bin/comntrows
CIP-005-3a R2.5 CIP-007-5 R1.1	Zakazuje nasledujúce nepotrebné a nie bezpečné služby: • Démon **timed** • Démon **NTP** • Démon **rwhod** • Démon **DPID2** • Agent DHCP	/etc/security/pscexpert/bin/rctcpip

Tabuľka 9. Štandardy CIP pre PowerSC Standard Edition (pokračovanie)

Štandard CIP	Implementácia AIX Security Expert	Umiestnenie skriptu, ktorý modifikuje hodnotu
CIP-005-3a R2.5 CIP-007-5 R1.1	Zakazuje nasledujúce nepotrebné a nie bezpečné služby: • Démon **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** • Služba cmsd • Služba ttdbserver • Služba TCP echo • Služba TCP discard • Služba TCP chargen • Služba TCP daytime • Služba TCP time • Služba UDP echo • Služba UDP discard • Služba UDP chargen • Služba UDP daytime • Služba UDP time	/etc/security/pscexpert/bin/cominetdconf
CIP-005-3a R2.5 CIP-007-5 R1.1	Vynucuje požiadavku odopretia služby pre mitigation porty.	/etc/security/pscexpert/bin/tcptr_aixpert
CIP-005-3a R3 CIP-007-3a R5, R6.5 CIP-007-5 R4.4	Povoľuje auditovanie binárnych súborov na systéme.	/etc/security/pscexpert/bin/pciaudit
CIP-007-3a R3 CIP-007-5 R2.1	Zobrazuje správu na povolenie štandardu Trusted Network Connect (TNC).	/etc/security/pscexpert/bin/GeneralMsg
CIP-007-3a R4 CIP-007-5 R3.3	Udržiava integritu systému zisťovaním, odstraňovaním a ochranou proti známym typom škodlivého softvéru.	/etc/security/pscexpert/bin/manageITsecurity
CIP-007-3a R5.2.1	Povoľuje zmenu hesla pri prvom prihlásení pre všetky predvolené užívateľské kontá, ktoré nie sú uzamknuté.	/etc/security/pscexpert/bin/pwdchg
CIP-007-3a R5.2.2-R5.2.3	Uzamyká všetky predvolené užívateľské kontá.	/etc/security/pscexpert/dodv2/lockacc_rlogin
CIP-007-3a R5.3.1	Nastavuje každé heslo na minimálne 6 znakov.	/etc/security/pscexpert/bin/chusrattr

Tabuľka 9. Štandardy CIP pre PowerSC Standard Edition (pokračovanie)

Štandard CIP	Implementácia AIX Security Expert	Umiestnenie skriptu, ktorý modifikuje hodnotu
CIP-007-5 R5.5.1	Nastavuje každé heslo na minimálne 8 znakov.	/etc/security/pscexpert/bin/chusrattr
CIP-007-3a R5.3.2 CIP-007-5 R5.5.2	Nastavuje každé heslo na kombináciu abecedných, numerických a špeciálnych znakov.	/etc/security/pscexpert/bin/chusrattr
CIP-007-3a R5.3.3 CIP-007-5 R5.6	Mení každé heslo každý rok.	/etc/security/pscexpert/bin/chusrattr
CIP-007-3a R7	Zobrazuje správu na povolenie EFS (Encrypted File System).	/etc/security/pscexpert/bin/GeneralMsg
CIP-007-5 R5.7	Obmedzuje počet neúspešných pokusov o autentifikáciu.	/etc/security/pscexpert/bin/chusrattr
CIP-010-1 CIP-010-2 R2.1	Zobrazuje správu na povolenie RTC (Real Time Compliance).	/etc/security/pscexpert/bin/GeneralMsg

Súvisiace informácie:

Súlad s požiadavkami normy North American Electric Reliability Corporation

Správa funkcie Security and Compliance Automation

Spoznajte proces plánovania a nasadzovania profilov funkcie Security and Compliance Automation produktu PowerSC na skupinu systémov v súlade s akceptovanými postupmi týkajúcimi sa kontroly a súladu IT.

V súlade so zásadami súladu s nariadeniami a kontroly IT musia byť systémy s podobnými pracovnými zaťaženiami a bezpečnostnými triedami údajov spravované a nakonfigurované konzistentne. Proces plánovania a uplatnenia zásad súladu s nariadeniami v systémoch pozostáva z nasledujúcich krokov:

Identifikácia pracovných skupín systému

V súlade so zásadami súladu s nariadeniami a kontroly IT musia byť systémy s podobnými pracovnými zaťaženiami a bezpečnostnými triedami údajov spravované a nakonfigurované konzistentne. Preto musíte identifikovať všetky systémy v podobnej pracovnej skupine.

Používanie neprodukčného testovacieho systému pri úvodnom nastavení

Uplatnite príslušný profil súladu s nariadeniami PowerSC v testovacom systéme.

Pri uplatňovaní profilov súladu v operačnom systéme AIX postupujte podľa nasledujúcich príkladov.

Príklad 1: Uplatnenie profilu DoD.xml

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

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

V tomto prípade sa nevyskytli žiadne neúspešné pravidlá, čiže Failedrules=0. To znamená, že všetky pravidlá boli úspešne uplatnené a môže začať testovacia fáza. V prípade zlyhaní sa vráti podrobný výstup.

Príklad 2: Uplatnenie profilu PCI.xml so zlyhaním

```
# 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

Neúspešné uplatnenie pravidla pci_grpck je potrebné vyriešiť. Možné príčiny zlyhania sú:

- Pravidlo sa nevzťahuje na dané prostredie a musí byť odstránené.
- Vyskytol sa problém v systéme, ktorý je potrebné vyriešiť.

Vyhľadanie neúspešného pravidla

Vo väčšine prípadov nedochádza k zlyhaniu, keď aplikujete profil bezpečnosti a súladu s požiadavkami systému PowerSC. Avšak systém môže mať nevyhnutné podmienky súvisiace s inštaláciou, ktoré chýbajú, alebo sa môžu vyskytnúť iné problémy, ktoré vyžadujú pozornosť administrátora.

Príčinu zlyhania je možné zistiť pomocou nasledujúceho príkladu:

Zobrazte súbor /etc/security/aixpert/custom/PCI.xml a nájdite neúspešné pravidlo. V tomto príklade je to pravidlo pci_grpck. Spustite príkaz **fgrep**, vyhľadajte neúspešné pravidlo pci_grpck a pozrite si priradené pravidlo XML.

```
fgrep -p pci_grpck /etc/security/aixpert/custom/PCI.xml
<AIXPertEntry name="pci_grpck" function="grpck"
<AIXPertRuleType type="DLS"/
<AIXPertDescription&gt;Implementuje časti PCI Section 8.2,
Skontrolujte skupinové definície: Overuje správnosť skupinových definícií
a opraví chyby
</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
Systém skupiny užívateľov a definície hesla</AIXPertGroup
</AIXPertEntry
```

Z pravidla pci_grpck je možné vidieť príkaz /usr/sbin/grpck.

Aktualizácia neúspešného pravidla

Pri aplikácii profilu bezpečnosti a profilu súladu s požiadavkami systému PowerSC môžete zistiť chyby.

Systém môže mať chýbajúce nevyhnutné inštalačné požiadavky alebo sa môžu vyskytnúť iné problémy, ktoré vyžadujú pozornosť od administrátora. Po určení základného príkazu neúspešného pravidla preskúmajte systém, aby ste porozumeli konfiguračnému príkazu, ktorý zlyhal. Systém môže mať bezpečnostný problém. Môže to byť aj prípad, že určité pravidlo nie je aplikovateľné do prostredia systému. Potom musíte vytvoriť vlastný bezpečnostný profil.

Vytvorenie vlastného profilu konfigurácie zabezpečenia

Ak nie je nejaké pravidlo použiteľné pre špecifické prostredie systému, väčšina organizácií predpisujúcich bezpečnostné štandardy povoľuje dokumentované výnimky.

Ak chcete odstrániť pravidlo a vytvoriť vlastný súbor bezpečnostnej politiky a konfigurácie, vykonajte nasledujúce kroky:

1. Skopírujte obsah nasledujúcich súborov do jedného súboru s názvom /etc/security/aixpert/custom/<*my_security_policy*>.xml:

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

2. Upravte súbor <*my_security_policy*>.xml odstránením pravidla, ktoré nie je použiteľné, od úvodnej značky XML <AIXPertEntry name... po koncovú značku XML </AIXPertEntry.

Môžete vsunúť ďalšie konfiguračné pravidlá pre bezpečnosť. Vložte ďalšie pravidlá do schémy XML AIXPertSecurityHardening. Profily systému PowerSC nemôžete zmeniť priamo, môžete ich však prispôsobiť.

Pre väčšinu prostredí musíte vytvoriť vlastnú politiku XML. Na distribúciu zákazníckeho profilu do iných systémov musíte bezpečne skopírovať prispôsobenú politiku XML do systému, ktorý vyžaduje rovnakú konfiguráciu. Na distribúciu vlastnej politiky XML na iné systémy sa používa bezpečný protokol, ako je protokol SFTP (secure file transfer protocol), a tento profil je uložený na bezpečnom mieste /etc/security/aixpert/custom/ *<my_security_policy.xml>*/etc/security/aixpert/custom/

Prihláste sa na systém, kde musí byť vytvorený vlastný profil a spustite tento príkaz:

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

Testovanie aplikácií pomocou AIX Profile Manager

Bezpečnostné konfigurácie môžu ovplyvniť aplikácie a spôsob, ktorým sa pristupuje a riadi systém. Pred nasadením systému do produkčného prostredia je dôležité otestovať aplikácie a očakávané metódy správy systému.

Regulačné štandardy súladu s požiadavkami predpisujú konfiguráciu zabezpečenia, ktorá je prísnejšia než predpripravená konfigurácia. Pre otestovanie systému vykonajte tieto kroky:

1. Vyberte **Zobraziť a spravovať profily** z pravého panelu uvítacej stránky programu AIX Profile Manager.
2. Vyberte profil, ktorý použije šablóna pre nasadenie do systémov, ktoré budú monitorované.
3. Kliknite na **Porovnať**.
4. Vyberte riadenú skupinu alebo vyberte individuálne systémy zo skupiny a kliknite na **Pridať** na ich pridanie do zoznamu vybratých systémov.
5. Kliknite na **OK**.

Spustí sa operácia porovnávania.

Monitorovanie systémov pre trvalý súlad s požiadavkami pomocou programu AIX Profile Manager

Bezpečnostné konfigurácie môžu ovplyvniť aplikácie a spôsob, ktorým sa pristupuje a riadi systém. Keď sa nasadzuje systém do produkčného prostredia, je dôležité monitorovať aplikácie a očakávané metódy správy systému.

Ak chcete používať AIX Profile Manager na monitorovanie systému AIX, vykonajte tieto kroky:

1. Vyberte **Zobraziť a spravovať profily** z pravého panelu uvítacej stránky programu AIX Profile Manager.
2. Vyberte profil, ktorý použije šablóna pre nasadenie do systémov, ktoré budú monitorované.
3. Kliknite na **Porovnať**.
4. Vyberte riadenú skupinu alebo vyberte individuálne systémy zo skupiny a pridajte ich do vybratého poľa.
5. Kliknite na **OK**.

Spustí sa operácia porovnávania.

Konfigurácia funkcie Security and Compliance Automation softvéru PowerSC

Spoznajte proces konfigurácie softvéru PowerSC pre funkciu Security and Compliance Automation z príkazového riadka a použitím nástroja AIX Profile Manager.

Konfigurácia nastavení volieb súladu s požiadavkami systému PowerSC

Naučte sa základy funkcie automatizácie bezpečnosti a zabezpečenia súladu s požiadavkami systému PowerSC, testovať konfiguráciu na neprodukčných testovacích systémoch a plánovať a nasadzovať tieto nastavenia. Keď použijete konfiguráciu súladu s požiadavkami, tieto nastavenia zmenia viaceré konfiguračné nastavenia v operačnom systéme.

Poznámka: Niektoré štandardy a profily súladu s požiadavkami zakážu Telnet, pretože Telnet používa jednoduché textové heslá. Preto musíte mať nainštalovaný, nakonfigurovaný a funkčný Open SSH. Môžete používať ľubovoľný bezpečný spôsob komunikácie so systémom, ktorý je konfigurovaný. Tieto štandardy súladu s požiadavkami vyžadujú zakázanie prihlasovania užívateľa root. Skôr ako budete pokračovať s aplikovaním zmien konfigurácie, nakonfigurujte jedného alebo viac užívateľov iných ako root. Táto konfigurácia nezakáže užívateľa root a môžete sa prihlásiť ako užívateľ iný ako root a spustiť príkaz **su** pre získanie oprávnení užívateľa root. Otestujte, či môžete vybudovať spojenie SSH do systému, prihláste sa ako užívateľ iný ako root a spustite príkaz do root.

Na prístup ku konfiguračným profilom DoD, PCI, SOX alebo COBIT použite nasledujúci adresár:

- Profily v operačnom systéme AIX sú umiestnené v adresári /etc/security/aixpert/custom.
- Profily v Virtual I/O Server (VIOS) sú umiestnené v adresári /etc/security/aixpert/core.

Konfigurácia súladu s požiadavkami systému PowerSC z príkazového riadka

Implementujte alebo skontrolujte profil súladu s požiadavkami pomocou príkazu **pscxpert** na systéme AIX a príkazu **viosecure** na Virtual I/O Server (VIOS).

Ak chcete použiť profilu súladu s požiadavkami systému PowerSC na systéme AIX, zadajte niektorý z nasledujúcich príkazov, ktorý závisí od úrovne súladu zabezpečenia, ktorú chcete použiť.

Tabuľka 10. Príkazy PowerSC pre AIX

Príkaz	Štandard súladu
% pscxpert -f /etc/security/aixpert/custom/DoD.xml	*US Department of Defense UNIX security technical implementation guide*
% pscxpert -f /etc/security/aixpert/custom/Hipaa.xml	*Heath Insurance Portability and Accountability Act*
% pscxpert -f /etc/security/aixpert/custom/PCI.xml	*Payment card industry-Data security standard*
% pscxpert -f /etc/security/aixpert/custom/SOX-COBIT.xml	*Sarbanes-Oxley Act of 2002 – COBIT IT Governance*

Ak chcete použiť profily súladu s požiadavkami systému PowerSC na systéme VIOS, zadajte niektorý z nasledujúcich príkazov pre úroveň súladu zabezpečenia, ktorú chcete použiť.

Tabuľka 11. Príkazy PowerSC pre Virtual I/O Server

Príkaz	Štandard súladu
% viosecure -file /etc/security/aixpert/custom/DoD.xml	*US Department of Defense UNIX security technical implementation guide*
% viosecure -file /etc/security/aixpert/custom/Hipaa.xml	*Heath Insurance Portability and Accountability Act*
% viosecure -file /etc/security/aixpert/custom/PCI.xml	*Payment card industry-Data security standard*
% viosecure -file /etc/security/aixpert/custom/SOX-COBIT.xml	*Sarbanes-Oxley Act of 2002 – COBIT IT Governance*

Príkaz **pscxpert** na systéme AIX a príkaz**viosecure** v VIOS môžu zabrať nejaký čas, pretože kontrolujú alebo nastavujú celý systém a robia konfiguračné zmeny súvisiace so zabezpečením. Výstup je podobný nasledujúcemu príkladu:

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

Avšak niektoré pravidlá zlyhajú v závislosti od prostredia AIX, inštalačnej sady a predchádzajúcej konfigurácie.

Napríklad pravidlo nevyhnutnej podmienky môže zlyhať, pretože systém nemá vyžadovanú sadu inštalačných súborov. Pred nasadením profilov súladu s požiadavkami v celom dátovom centre je potrebné porozumieť každému zlyhaniu a vyriešiť ho.

Súvisiace koncepty:

“Správa funkcie Security and Compliance Automation” na strane 89
Spoznajte proces plánovania a nasadzovania profilov funkcie Security and Compliance Automation produktu PowerSC

na skupinu systémov v súlade s akceptovanými postupmi týkajúcimi sa kontroly a súladu IT.

Konfigurácia súladu s požiadavkami systému PowerSC pomocou programu AIX Profile Manager

Naučte sa ako postupovať pri konfigurácii profilov bezpečnosti a profilov súladu s požiadavkami systému PowerSC a ako nasadiť túto konfiguráciu na riadený systém AIX pomocou programu AIX Profile Manager.

Pri konfigurácii profilov bezpečnosti a profilov súladu s požiadavkami systému PowerSC pomocou programu AIX Profile Manager vykonajte tieto kroky:

1. Prihláste sa do IBM Systems Director a vyberte program AIX Profile Manager.
2. Vytvorte šablónu, ktorá je založená na jednom z profilov bezpečnosti a súladu s požiadavkami systému PowerSC, vykonaním týchto krokov:
   a. Kliknite na voľbu **Zobraziť a spravovať šablóny** z pravého panelu uvítacej stránky programu AIX Profile Manager.
   b. Kliknite na **Vytvoriť**.
   c. Kliknite na **Operačný systém** zo zoznamu **Typ šablóny**.
   d. Zadajte názov pre šablónu v poli **Názov konfiguračnej šablóny**.
   e. Kliknite na **Pokračovať > Uložiť**.
3. Vyberte profil, ktorý sa použije so šablónou, výberom **Prehľadávať** pod voľbou **Vybrať, ktorý profil sa má použiť pre túto šablónu**. Profily zobrazia tieto položky:
   - ice_DLS.xml je predvolená úroveň zabezpečenia operačného systému AIX.
   - ice_DoD.xml obsahuje pokyny STIG Ministerstva obrany USA týkajúce sa nastavení systému UNIX.
   - ice_HLS.xml je všeobecné zabezpečenie vysokej úrovne pre nastavenia AIX.
   - ice_LLS.xml je zabezpečenie nízkej úrovne pre nastavenia AIX.
   - ice_MLS.xml je zabezpečenie strednej úrovne pre nastavenia AIX.
   - ice_PCI.xml je nastavenie PCI (Payment Card Industry) pre operačný systém AIX.
   - ice_SOX.xml je nastavenie SOX alebo COBIT pre operačný systém AIX.
4. Odstráňte všetky profily z vybratého poľa.
5. Vyberte **Pridať** na presun požadovaného profilu do zoznamu vybratých profilov.
6. Kliknite na **Uložiť**.

Pre nasadenie konfigurácie na riadený systém AIX vykonajte tieto kroky:

1. Vyberte **Zobraziť a spravovať šablóny** z pravého panelu uvítacej stránky programu AIX Profile Manager.
2. Vyberte požadovanú šablónu na nasadenie.
3. Kliknite na **Nasadiť**.
4. Vyberte systémy na nasadenie profilu a kliknite na **Pridať** na presun požadovaného profilu do zoznamu vybratých profilov.
5. Kliknite na **OK** pre nasadenie šablóny konfigurácie. Systém je nakonfigurovaný v súlade s vybratou šablónou profilu.

Aby bolo nasadenie pre DoD, PCI alebo SOX úspešné, musí byť nainštalovaný systém PowerSC Standard Edition na koncovom bode systému AIX. Ak systém, ktorý je nasadzovaný, nemá nainštalovaný PowerSC, nasadzovanie zlyhá. IBM Systems Director nasadí šablónu konfigurácie na vybraté koncové body systému AIX a nakonfiguruje ich podľa požiadaviek na súlad.

Súvisiace informácie:

AIX Profile Manager

IBM Systems Director

PowerSC Real Time Compliance

Softvér PowerSC Real Time Compliance neustále monitoruje aktivované systémy AIX, aby sa zabezpečila ich konzistentná a bezpečná konfigurácia.

Funkcia PowerSC Real Time Compliance spolupracuje s funkciou PowerSC Compliance Automation a politikami AIX Security Expert za účelom upozornenia na porušenia súladu a zmenu sledovaných súborov. Keď dôjde k narušeniu politiky konfigurácie zabezpečenia systému, funkcia PowerSC Real Time Compliance pošle administrátorovi upozornenie prostredníctvom e-mailu alebo textovej správy.

Funkcia PowerSC Real Time Compliance je pasívna bezpečnostná funkcia, ktorá podporuje vopred definované alebo zmenené profily súladu zahrňujúce profily pre súlad s normami STIG Ministerstva obrany USA, Payment Card Industry Data Security Standard, Sarbanes-Oxley Act a COBIT. Poskytuje predvolený zoznam súborov, ktoré sa majú sledovať, no do tohto zoznamu môžete pridať ďalšie súbory.

Inštalácia PowerSC Real Time Compliance

Funkcia PowerSC Real Time Compliance sa inštaluje so softvérom PowerSC Standard Edition verzia 1.1.4 a novšími verziami a nie je súčasťou základného operačného systému AIX.

Postup inštalácie softvéru PowerSC Standard Edition:

1. Uistite sa, že systém, do ktorého chcete nainštalovať funkciu PowerSC Standard Edition, používa niektoré z nasledujúcich vydaní operačného systému AIX:
   - IBM AIX 6 s technologickou úrovňou 7 alebo novšie vydanie s balíkmi AIX Event Infrastructure for AIX a AIX Clusters (bos.ahafs 6.1.7.0) alebo novšie verzie
   - IBM AIX 7 s technologickou úrovňou 1 alebo novšie vydanie s balíkmi AIX Event Infrastructure for AIX a AIX Clusters (bos.ahafs 7.1.1.0) alebo novšie verzie
   - AIX, verzia 7.2 alebo novšie vydanie s balíkmi AIX Event Infrastructure for AIX a AIX Clusters (bos.ahafs 7.2.0.0) alebo novšie verzie
2. Ak chcete aktualizovať alebo nainštalovať sadu súborov funkcie PowerSC Standard Edition, nainštalujte sadu súborov powerscStd.rtc z inštalačného balíka softvéru PowerSC Standard Edition verzie 1.1.4 alebo novšej verzie.

Konfigurácia PowerSC Real Time Compliance

Môžete nakonfigurovať PowerSC Real Time Compliance na odosielanie výstrah, keď dôjde k narušeniu profilu súladu s nariadeniami alebo k zmene monitorovaného súboru. Medzi profily patria napríklad usmernenia a štandardy DoD STIG (Department of Defense Security Technical Implementation Guide), PCI DSS (Payment Card Industry Data Security Standard), Sarbanes-Oxley Act a COBIT.

PowerSC Real Time Compliance môžete konfigurovať jedným z nasledujúcich spôsobov:

- Zadajte príkaz **mkrtc**.
- Spustite SMIT zadaním nasledujúceho príkazu:

  ```
  smit RTC
  ```

Identifikácia súborov monitorovaných funkciou PowerSC Real Time Compliance

Funkcia PowerSC Real Time Compliance monitoruje na základe bezpečnostných nastavení zmeny súborov v predvolenom zozname súborov, ktorý je možné prispôsobiť pridaním alebo odstránením súborov zo zoznamu v súbore /etc/security/rtc/rtcd_policy.conf.

Existujú dve metódy, ako môžete identifikovať šablónu súladu s nariadeniami, ktorá je použitá na systéme. Prvou metódou je použitie príkazu **pscxpert**, tou druhou je použitie produktu AIX Profile Manager s produktom IBM Systems Director.

Keď identifikujete profil súladu s nariadeniami, môžete do zoznamu monitorovaných súborov pridať ďalšie súbory tým, že ich pridáte do súboru /etc/security/rtc/rtcd_policy.conf. Po uložení súboru sa zmeny prejavia okamžite a monitorovanie zmien na týchto súboroch sa spustí bez potreby reštartovať systém.

Nastavenie výstrah pre PowerSC Real Time Compliance

Notifikácie funkcie PowerSC Real Time Compliance musíte nakonfigurovať zadaním typu výstrahy a príjemcov výstrahy.

Démon rtcd, ktorý je hlavným komponentom funkcie PowerSC Real Time Compliance, získa potrebné informácie o typoch výstrah a príjemcoch z konfiguračného súboru /etc/security/rtc/rtcd.conf. Informácie v tomto súbore môžete aktualizovať v textovom editore.

Súvisiace informácie:

Formát súboru /etc/security/rtc/rtcd.conf pre funkciu Real-Time Compliance

Funkcia Trusted Boot

Funkcia Trusted Boot používa VTPM, čo je virtuálna inštancia TPMod Trusted Computing Group. VTPM sa používa na bezpečné ukladanie meraní zavádzania systému pre budúce overovanie.

Základné pojmy pre Trusted Boot

Je dôležité porozumieť integrite procesu bootovania a ako klasifikovať bootovanie ako dôveryhodné bootovanie alebo nedôveryhodné bootovanie.

Môžete nakonfigurovať maximálne 60 logických oddielov s podporou VTPM (LPAR) pre každý fyzický systém pomocou Hardware Management Console (HMC). Keď je VTPM nakonfigurovaný, je jedinečný pre každý LPAR. Keď sa VTPM používa s technológiou AIX Trusted Execution, zaisťuje bezpečnosť a zabezpečenie pre nasledujúce oddiely:

- Obraz bootovania na disku
- Celý operačný systém
- Aplikačné vrstvy

Administrátor môže prezerať dôveryhodné a nedôveryhodné systémy z centrálnej konzoly, ktorá sa inštaluje s overovačom **openpts**, ktorý je dostupný v rozširovacom balíku AIX. Konzola **openpts** riadi jeden alebo viac serverov Power Systems a monitoruje alebo atestuje dôveryhodný stav systémov AIX Profile Manager prostredníctvom dátových centier. Atestácia je proces, kde overovač zisťuje (alebo atestuje), či kolektor vykonal dôveryhodné bootovanie.

Dôveryhodný stav bootovania

O oddiele sa tvrdí, že je dôveryhodný, ak overovač úspešne atestuje integritu kolektora. Overovač je vzdialený oddiel, ktorý zisťuje, či kolektor vykonal dôveryhodné bootovanie. Kolektor je oddiel AIX, ktorý má pripojený modul VTPM (Virtual Trusted Platform Module) a nainštalovaný TSS (Trusted Software Stack). Označuje, že merania, ktoré boli zaznamenané vo VTPM sa zhodujú s množinou referencií vo vlastníctve overovača. Stav dôveryhodného bootovania označuje, že oddiel bol zavedený dôveryhodným spôsobom. Toto vyhlásenie je o integrite procesu zavedenia systému a neoznačuje aktuálnu alebo pretrvávajúcu úroveň bezpečnosti systému.

Nedôveryhodný stav bootovania

Oddiel sa dostane do nedôveryhodného stavu, ak overovač nemôže úspešne atestovať integritu procesu bootovania. Nedôveryhodný stav označuje, že niektorý aspekt procesu bootovania je nekonzistentný s referenčnými informáciami vo vlastníctve overovača. K možným príčinám neúspešnej atestácie patrí zavedenie systému z iného zavádzacieho zariadenia, bootovanie iného obrazu jadra a zmena existujúceho obrazu bootovania.

Súvisiace koncepty:

“Riešenie problémov s funkciou Trusted Boot” na strane 101
Existujú určité bežné scenáre a kroky nápravy, ktoré sú vyžadované ako pomoc pri identifikácii príčiny neúspešnej atestácie pri použití funkcie Trusted Boot.

Plánovanie dôveryhodného spustenia

Získajte informácie o konfiguráciách hardvéru a softvéru, ktoré sú vyžadované na inštaláciu dôveryhodného spustenia.

Nevyhnutné podmienky pre Trusted Boot

Inštalácia funkcie Trusted Boot zahrňuje nakonfigurovanie kolektora overovača.

Keď sa pripravujete na preinštalovanie operačného systému AIX na systéme, kde je už nainštalovaný Trusted Boot, musíte skopírovať súbor /var/tss/lib/tpm/system.data a prepísať ním súbor na tom istom umiestnení po dokončení preinštalovania. Ak neskopírujete tento súbor, musíte odstrániť virtualizovaný Trusted Platform Module z riadiacej konzoly a preinštalovať ho na tomto oddiele.

Kolektor

Ku konfiguračným požiadavkám na inštaláciu kolektora patria nasledujúce nevyhnutné podmienky:

- Hardvér POWER7, ktorý pracuje na vydaní firmvéru 740.
- Nainštalujte IBM AIX 6 s technologickou úrovňou 7 alebo nainštalujte IBM AIX 7 s technologickou úrovňou 1.
- Nainštalujte konzolu HMC (HMC) verziu 7.4 alebo novšiu.
- Nakonfigurujte oddiel s VTPM a minimálne 1 GB pamäte.
- Nainštalujte Secure Shell (SSH), najmä OpenSSH alebo ekvivalent.

Overovač

Overovač **openpts** je prístupný z rozhrania príkazového riadka a grafického užívateľského rozhrania, ktoré je navrhnuté tak, aby fungovalo na množstve rôznych platforiem. Verzia AIX overovača OpenPTS je k dispozícii v rozširovacom balíku AIX. Verzie overovača OpenPTS pre systém Linux a iné platformy sú k dispozícii prostredníctvom prevzatia z webu. Ku konfiguračným požiadavkám patria nasledujúce nevyhnutné podmienky:

- Nainštalujte SSH, najmä OpenSSH alebo ekvivalent.
- Vytvorte konektivitu siete (prostredníctvom SSH) ku kolektoru.
- Nainštalujte Java™ 1.6 alebo novší, čím získate prístup ku konzole **openpts** z grafického rozhrania.

Príprava na nápravu

Informácie o Trusted Boot, ktoré sú popísané tu, slúžia ako pomôcka pri identifikovaní situácií, ktoré by mohli vyžadovať nápravu. Nemajú vplyv na proces bootovania.

Môže nastať množstvo situácií, ktoré spôsobia zlyhanie atestácie a je ťažké predchádzať situácii, ktorú môžete zaznamenať. V závislosti od tejto situácie sa musíte rozhodnúť pre príslušný úkon. Je však dobrý zvykom pripraviť sa na niektoré vážne scenáre a mať politiku alebo pracovný tok, ktoré vám pomôžu zvládnuť takéto incidenty. Nápravy je opravný úkon, ktorý sa musí vykonať, keď atestácia nahlási, že jeden alebo viac kolektorov nie je dôveryhodných.

Napríklad, ak nastane zlyhanie atestácie následkom toho, že zavádzací obraz sa líši od referencie odkazovača, premyslite si odpovede na nasledujúce otázky:

- Ako môžete overiť, či táto hrozba je vierohodná?
- Bola vykonaná nejaká naplánovaná údržba, aktualizácia verzie AIX alebo bol nedávno nainštalovaný nový hardvér?
- Môžete sa obrátiť na administrátora, ktorý má prístup k týmto informáciám?
- Kedy bol systém naposledy zavádzaný v dôveryhodnom stave?
- Ak táto bezpečnostná hrozba vyzerá legitímne, aký úkon musíte vykonať? (Napríklad zhromaždenie protokolov z auditu, odpojenie systému od siete, vypnutie systému a upozornenie užívateľov).
- Boli zasiahnuté nejaké iné systémy, ktoré treba skontrolovať?

Súvisiace koncepty:

“Riešenie problémov s funkciou Trusted Boot” na strane 101
Existujú určité bežné scenáre a kroky nápravy, ktoré sú vyžadované ako pomoc pri identifikácii príčiny neúspešnej atestácie pri použití funkcie Trusted Boot.

Aspekty migrácie

Pred migráciou oddielu, ktorý je povolený pre virtuálny modul TPM zvážte tieto nevyhnutné podmienky.

Výhodou virtuálneho modulu TPM pred fyzickým modulom TPM je, že umožňuje presun oddielu medzi systémami, pričom virtuálny modul TPM je zachovaný. Ak chcete bezpečne migrovať logický oddiel, firmvér pred prenosom zašifruje údaje o virtuálnom module TPM. Ak chcete zabezpečiť bezpečnú migráciu, pred migráciou musia byť implementované tieto bezpečnostné opatrenia:

- Povoľte IPSEC medzi Virtual I/O Server (VIOS), ktorý vykonáva migráciu.
- Prostredníctvom konzoly HMC nastavte dôveryhodný systémový kľúč (HMC), aby ste mohli riadiť riadené systémy schopné dešifrovať údaje virtuálneho modulu TPM po migrácii. Cieľový systém migrácie musí mať rovnaký kľúč ako je kľúč zdrojového systému, aby mohol úspešne migrovať údaje.

Súvisiace informácie:

Používanie konzoly HMC

Migrácia VIOS

Inštalácia funkcie Trusted Boot

Existujú určité vyžadované hardvérové a softvérové konfigurácie, ktoré sú potrebné na inštaláciu funkcie Trusted Boot.

Súvisiace informácie:

“Inštalácia PowerSC Standard Edition” na strane 7
Pre každú špecifickú funkciu PowerSC Standard Edition musíte nainštalovať sadu súborov.

Inštalácia kolektora

Kolektor musíte nainštalovať prostredníctvom sady súborov zo základného CD AIX.

Ak chcete nainštalovať kolektor, pomocou príkazu **smit** alebo **installp** nainštalujte balíky powerscStd.vtpm a openpts.collector, ktoré sa nachádzajú na základom CD.

Inštalácia overovateľa

Komponent overovateľa OpenPTS beží v operačnom systéme AIX a na iných platformách.

Verziu AIX overovateľa možno nainštalovať zo sady súborov pomocou rozširujúceho balíka AIX. Ak chcete nainštalovať overovateľa v operačnom systéme AIX, nainštalujte balík openpts.verifier z rozširujúceho balíka AIX pomocou príkazu **smit** alebo **installp**. Takto sa nainštalujú verzie príkazového riadka aj grafického rozhrania overovateľa.

Overovateľa OpenPTS pre iné operačné systémy možno stiahnuť z Stiahnuť overovateľa Linux OpenPTS na používanie s dôveryhodným spustením AIX.

Súvisiace informácie:

Stiahnite overovateľa Linux OpenPTS na používanie s dôveryhodným spustením AIX

Konfigurácia funkcie Trusted Boot

Zistite viac o postupe pri registrácii systému a atestovaní systému pre funkciu Trusted Boot.

Registrácia systému

Naučte sa ako zaregistrovať systém u overovateľa.

Registrácia systému je proces, v ktorom sa poskytne pôvodná sada meraní overovateľovi. Táto registrácia tvorí základ pre ďalšie požiadavky na atestáciu. Ak chcete zaregistrovať systém z príkazového riadka, použite tento príkaz z overovateľa:

```
openpts -i <názov_hostiteľa>
```

Informácie o zaregistrovanom oddiele sa nachádzajú v adresári $HOME/.openpts. Počas procesu registrácie je každému novému oddielu priradený jedinečný identifikátor a informácie súvisiace so zaregistrovanými oddielmi sú uložené do adresára, ktorý zodpovedá tomuto jedinečnému identifikátoru.

Ak chcete systém zaregistrovať z grafického rozhrania, postupujte podľa týchto krokov:

1. Príkazom **/opt/ibm/openpts_gui/openpts_GUI.sh** spustite grafické rozhranie.
2. Z ponuky navigácie vyberte **Zaregistrovať**.
3. Zadajte názov hostiteľa a prihlasovacie údaje SSH systému.
4. Kliknite na **Zaregistrovať**.

Súvisiace koncepty:

"Atestácia systému"
Naučte sa postup ako atestovať systém z príkazového riadka a prostredníctvom grafického rozhrania.

Atestácia systému

Naučte sa postup ako atestovať systém z príkazového riadka a prostredníctvom grafického rozhrania.

Na dotazovanie integrity spustenia systému použite tento príkaz z overovateľa:

```
openpts <názov_hostiteľa>
```

Ak chcete atestovať systém z grafického rozhrania, postupujte podľa týchto krokov:

1. Z ponuky navigácie vyberte kategóriu.
2. Na atestáciu vyberte jeden alebo viac systémov.
3. Kliknite na **Atestovať**.

Registrácia a atestácia systému bez hesla

Požiadavka na atestáciu je odoslaná cez zabezpečené prostredie Shell (SSH). Ak chcete povoliť pripojenia SSH bez hesla, nainštalujte certifikát overovateľa v kolektore.

Ak chcete nastaviť certifikát overovateľa v systéme zhromažďovania, postupujte podľa týchto krokov :

- V overovateľovi spustite tieto príkazy:

```
ssh-keygen    # Bez frázy hesla
scp ~/.ssh/id_rsa.pub <kolektor>:/tmp
```

- V kolektore spustite tento príkaz:

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

Správa funkcie Trusted Boot

Zistite viac o postupe pri riadení výsledkov atestácie funkcie Trusted Boot.

Interpretovanie výsledkov atestácie

Naučte sa ako zobraziť a porozumieť výsledkom atestácie.

Atestácia môže mať za následok jeden z týchto stavov:

1. Požiadavka na atestáciu zlyhala: Požiadavka na atestáciu nebola úspešne dokončená. Ak chcete porozumieť možným príčinám zlyhania, pozrite si časť Riešenie problémov.
2. Integrita systému platná: Atestácia bola dokončená úspešne a spustenie systému sa zhoduje s referenčnými informáciami, ktoré vlastní overovateľ. Toto označuje úspešné dôveryhodné spustenie.
3. Integrita systému neplatná: Požiadavka na atestáciu bola dokončená, ale medzi informáciami, ktoré boli zhromaždené počas spustenia systému, a referenčnými informáciami, ktoré vlastní overovateľ, bola zistená nezhoda. Toto označuje nedôveryhodné spustenie.

Atestácia tiež hlási, či bola na kolektor použitá aktualizácia prostredníctvom tejto správy:

Aktualizácia systému dostupná: Táto správa indikuje, že v kolektore bola použitá aktualizácia a že k dispozícii je sada aktualizovaných referenčných informácií, ktoré platia pre nasledujúce spustenie. Užívateľ je pri overovaní vyzvaný, aby akceptoval alebo odmietol aktualizácie. Užívateľ sa môže napríklad rozhodnúť, že akceptuje tieto aktualizácie, ak si je vedomý, údržby, ktorá sa vyskytuje v kolektore.

Ak chcete preskúmať zlyhanie atestácie prostredníctvom grafického rozhrania, postupujte podľa týchto krokov:

1. Z ponuky navigácie vyberte kategóriu.
2. Vyberte systém na preskúmanie.
3. Kliknite dva razy na položku zodpovedajúcu systému. Zobrazí sa okno vlastností. Toto okno obsahuje informácie protokolu o zlyhanej atestácii.

Odstraňovanie systémov

Naučte sa ako odstrániť systém z databázy overovateľa.

Ak chcete odstrániť systém z databázy overovateľa, spustite tento príkaz:

```
openpts -r <názov_hostiteľa>
```

Riešenie problémov s funkciou Trusted Boot

Existujú určité bežné scenáre a kroky nápravy, ktoré sú vyžadované ako pomoc pri identifikácii príčiny neúspešnej atestácie pri použití funkcie Trusted Boot.

Príkaz **openpts** deklaruje systém ako neplatný, ak aktuálny stav zavedenia systému nevyhovuje referenčným informáciám, ktoré sú vo vlastníctve overovača. Príkaz **openpts** zisťuje možnú príčinu, prečo je integrita neplatná. Existuje niekoľko premenných v plnom zavedení systému AIX a neúspešná atestácia vyžaduje analýzu na zistenie príčinu tohto zlyhania.

Nasledujúca tabuľka uvádza niektoré bežné scenáre a kroky nápravy na identifikáciu príčiny zlyhania:

Tabuľka 12. Riešenie niektorých problémov v bežných scenároch pri zlyhaní

Príčina zlyhania	Možné príčiny zlyhania	Navrhovaná náprava

Atestácia sa nedokončila.	• Nesprávny názov hostiteľa.
	• Žiadna sieťová trasa medzi zdrojom a cieľom.
	• Nesprávne bezpečnostné prihlasovacie údaje.
		Skontrolujte pripojenie Secure Shell (SSH) pomocou nasledujúceho príkazu:
		`ssh ptsc@hostname`
		
		Ak je pripojenie SSH úspešné, skontrolujte nasledujúce príčiny neúspešnej atestácie:
		• Systém, ktorý je práve atestovaný, nemá spusteného démona **tcsd**.
		• Systém, ktorý je práve atestovaný, nebol inicializovaný príkazom **ptsc**. Tento proces sa mal vykonať automaticky počas spúšťania systému, ale skontrolujte prítomnosť adresára /var/ptsc/ na kolektore. Ak adresár /var/ptsc/ neexistuje, spustite na kolektore nasledujúci príkaz:
		`ptsc -i`

Firmvér CEC bol zmenený.	• Bola použitá aktualizácia verzie firmvéru. • LPAR bol migrovaný na systém, ktorý používa inú verziu firmvéru.	Skontrolujte úroveň firmvéru systému, ktorý hosťuje LPAR.
Prostriedky alokované pre LPAR sa zmenili.	CPU alebo pamäť alokované pre LPAR sa zmenili.	Skontrolujte profil oddielu v HMC.

Tabuľka 12. Riešenie niektorých problémov v bežných scenároch pri zlyhaní (pokračovanie)

Príčina zlyhania	Možné príčiny zlyhania	Navrhovaná náprava
Zmenil sa firmvér pre adaptéry, ktoré sú dostupné v oddiele LPAR.	Hardvérové zariadenie boli pridané na alebo odstránené z LPAR.	Skontrolujte profil oddielu v HMC.
Zoznam zariadení pripojených k LPAR sa zmenil.	Hardvérové zariadenie boli pridané na alebo odstránené z LPAR.	Skontrolujte profil oddielu v HMC.
Zmenil sa bootovací obraz, ktorý obsahuje jadro operačného systému.	• Bola aplikovaná aktualizácia AIX a overovač nevedel o tejto aktualizácii. • Bol spustený príkaz **bosboot**.	• Potvrdiť u administrátora alebo kolektora, či pred poslednou operáciou rebootovania nebola vykonaná nejaká údržba. • Skontrolujte v protokoloch na kolektore aktivity údržby.
LPAR bol bootovaný z iného zariadenia.	• Bola vykonaná registrácia bezprostredne po inštalácii siete. • Systém je nabootovaný zo zariadenia určeného na údržbu.	Zavádzacie zariadenie a príznaky môžete skontrolovať príkazom **bootinfo**. Ak bola vykonaná registrácia bezprostredne po inštalácii NIM a pred operáciou rebootovania, podrobnosti registrácie sa týkajú inštalácie siete a nie nasledujúceho bootovania disku. Túto registráciu je možné opraviť odstránením registrácie a opätovnou registráciou logického oddielu.
Bola vyvolaná ponuka bootovania SMS.		Proces bootovania musí prejsť neprerušene bez zásahu užívateľa, aby bol systém dôveryhodný. Pri vstupe do ponuky bootovania SMS dôjde k strate platnosti bootovania.
Databáza dôveryhodného vykonávania (TE) bola zmenená.	• Binárne súbory boli pridané do alebo odstránené z databázy TE. • Binárne súbory v databáze boli aktualizované.	Overte databázu spustením príkazu **trustchk**.

Súvisiace koncepty:

“Príprava na nápravu” na strane 98
Informácie o Trusted Boot, ktoré sú popísané tu, slúžia ako pomôcka pri identifikovaní situácií, ktoré by mohli vyžadovať nápravu. Nemajú vplyv na proces bootovania.

“Základné pojmy pre Trusted Boot” na strane 97
Je dôležité porozumieť integrite procesu bootovania a ako klasifikovať bootovanie ako dôveryhodné bootovanie alebo nedôveryhodné bootovanie.

Súvisiace informácie:

Používanie konzoly HMC

Trusted Firewall

Funkcia Trusted Firewall poskytuje bezpečnosť na virtualizačnej vrstve, ktorá zlepšuje výkon a účinnosť prostriedkov pri komunikácii medzi bezpečnostnými zónami odlišných virtuálnych LAN (VLAN) na tom istom serveri Power Systems. Trusted Firewall znižuje zaťaženie na externej sieti presúvaním schopnosti filtrovania paketov brány firewall, ktoré spĺňajú špecifikované pravidlá, do virtualizačnej vrstvy. Táto schopnosť filtrovania sa riadi jednoducho definovanými pravidlami sieťových filtrov, ktoré umožňujú dôveryhodnej sieťovej premávke prestupovať medzi bezpečnostnými VLAN bez toho, aby opustili virtuálne prostredie. Trusted Firewall chráni a smeruje internú sieťovú premávku medzi operačnými systémami AIX, IBM i a Linux.

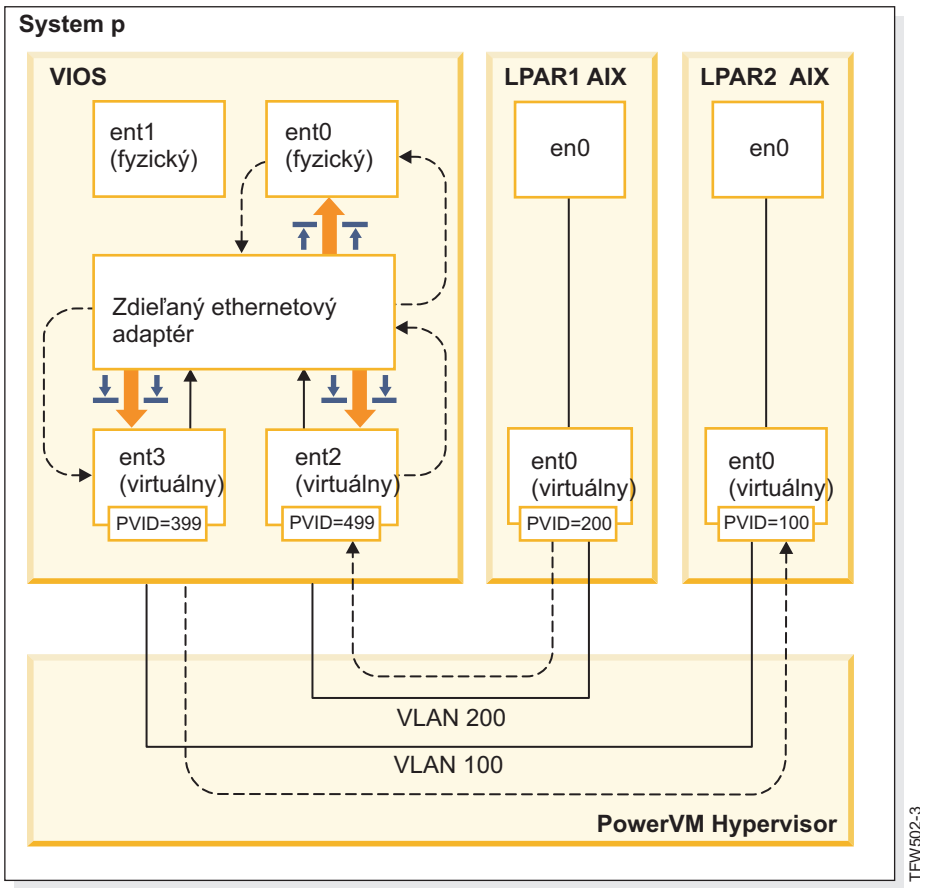
Základné pojmy pre Trusted Firewall

Existujú určité základné pojmy, ktorým treba porozumieť pri používaní funkcie Trusted Firewall.

Hardvér Power Systems je možné nakonfigurovať s viacerými virtuálnymi bezpečnostnými zónami LAN (VLAN). Užívateľom nakonfigurovaná politika, vytvorená ako pravidlo filtra funkcie Trusted Firewall, umožňuje určitej dôveryhodnej sieťovej premávke prestupovať bezpečnostné zóny VLAN a zostať pri tom interná vo virtualizačnej vrstve. Je to podobné ako uvedenie sieťovo pripojenej fyzickej brány firewall do virtualizačného prostredia, ktorá zaistí výkonovo efektívnejšiu metódu implementovania schopností brány firewall pre virtualizované dátové centrá.

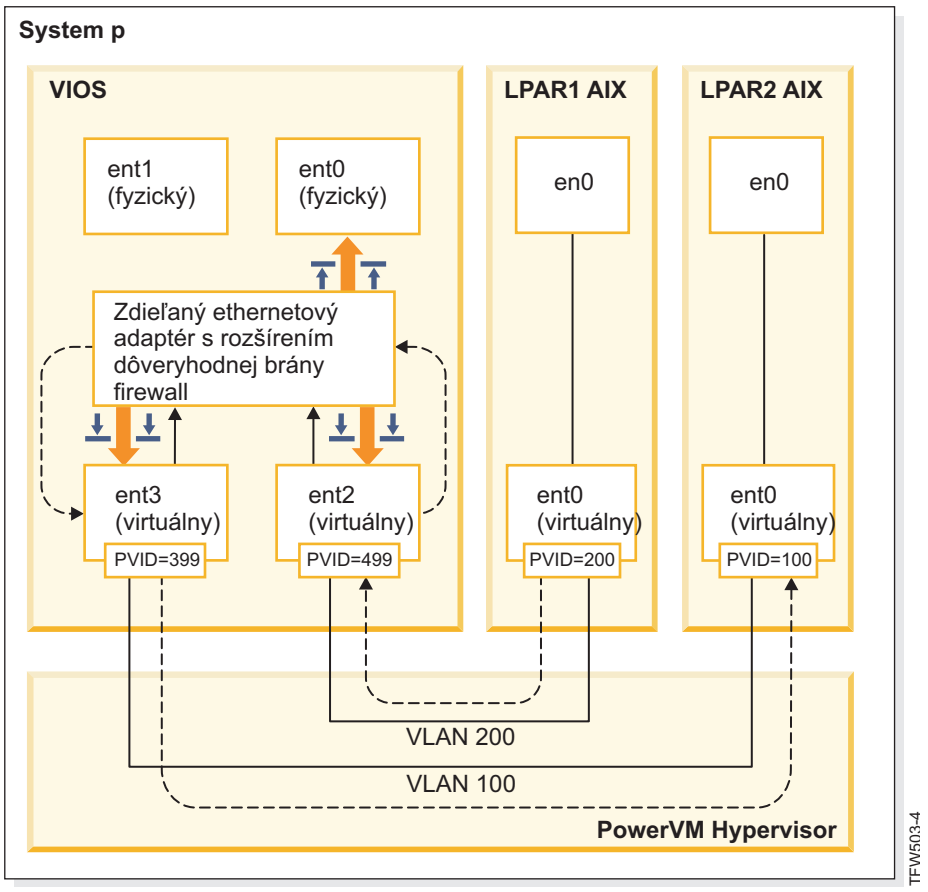
S funkciou Trusted Firewall môžete nakonfigurovať pravidlá, ktoré umožnia určitým druhom premávky porenášať sa priamo z jednej VLAN na systéme Virtual I/O Server (VIOS) na inú VLAN na tom istom systéme VIOS, pričom sa naďalej zachová vysoká úroveň bezpečnosti vďaka obmedzeniu ostatných druhov premávky. Je to konfigurovateľná brána firewall vo virtualizačnej vrstve serverov Power Systems.

Pri použití príkladu v dokumente Obrázok 1 na strane 104 je cieľom byť schopný prenášať informácie bezpečne a efektívne z LPAR1 na VLAN 200 a z LPAR2 na VLAN 100. Bez funkcie Trusted Firewall sa informácie určené pre LPAR2 z LPAR1 odosielajú von z internej siete smerovača, ktorý tieto informácie smeruje späť do LPAR2.



Obrázok 1. Príklad prenosu informácií krížom cez VLAN bez funkcie Trusted Firewall

Pomocou funkcie Trusted Firewall môžete nakonfigurovať pravidlá, ktoré umožnia odovzdávanie informácií z LPAR1 na LPAR2 bez opustenia internej siete. Táto cesta je zobrazená na Obrázok 2 na strane 105.



Obrázok 2. Príklad prenosu informácií krížom cez VLAN s funkciou Trusted Firewall

Konfiguračné pravidlá, ktoré umožňujú bezpečné odovzdávanie informácií po sieťach VLAN skracujú cestu k ich cieľu. Funkcia Trusted Firewall používa na umožnenie tejto komunikácie adaptér SEA a rozšírenie jadra SVM.

Zdieľaný ethernetový adaptér
SEA je miesto, kde začína a končí smerovanie. Keď sa zaregistruje SVM, SEA prijíma pakety a postupuje ich do SVM. Ak SVM zistí, že paket je pre LPAR na tom istom serveri Power Systems, aktualizuje hlavičku vrstvy 2 paketu. Paket sa vráti do SEA na postúpenie do konečného cieľa buď v rámci systému alebo na externej sieti.

Security Virtual Machine
SVM je miesto, kde sa aplikujú pravidlá filtrovania. Pravidlá filtrovania sú nevyhnutné na udržiavanie bezpečnosti na internej sieti. Po zaregistrovaní SVM s SEA sa pakety predtým, ako sa odošlú do externej siete, postúpia do SVM. Na základe aktívnych pravidiel filtrovania SVM určí, či paket zostáva v internej sieti alebo sa presunie do externej siete.

Inštalácia funkcie Trusted Firewall

Inštalácia funkcie PowerSC Trusted Firewall je podobná ako inštalácia funkcií PowerSC.

Nevyhnutné podmienky:

- Verzie PowerSC staršie ako 1.1.1.0 nemajú vyžadovanú sadu súborov na inštaláciu funkcie Trusted Firewall. Skontrolujte, či máte inštalačné CD PowerSC pre verziu 1.1.1.0 alebo novšiu.
- Ak chcete využívať výhody funkcie Trusted Firewall, musíte ste už pomocou konzoly HM) alebo Virtual I/O Server (VIOS) nakonfigurovať vaše virtuálne siete LAN (siete VLAN).

Trusted Firewall sa dodáva ako doplnková sada súborov na inštalačnom CD PowerSC Standard Edition. Názov súboru je powerscStd.svm.rte. Môžete pridať funkciu Trusted Firewall do existujúcej inštancie systému PowerSC verzie 1.1.0.0 alebo novšej alebo ju nainštalovať ako súčasť novej inštalácie systému PowerSC verzie 1.1.1.0 alebo novšej.

Ak chcete pridať funkciu Trusted Firewall do existujúcej inštancie systému PowerSC:

1. Musíte mať spustený VIOS, verzia 2.2.1.4 alebo novší.
2. Vložte inštalačné CD PowerSC pre verziu 1.1.1.0 alebo si prevezmite obraz inštalačného CD.
3. Použite príkaz **oem_setup_env** pre prístup typu root.
4. Pomocou príkazu **installp** alebo nástroja SMIT nainštalujte sadu súborov PowerscStd.svm.rte.

Súvisiace informácie:

"Inštalácia PowerSC Standard Edition" na strane 7
Pre každú špecifickú funkciu PowerSC Standard Edition musíte nainštalovať sadu súborov.

Konfigurácia funkcie Trusted Firewall

Po nainštalovaní funkcie Trusted Firewall sa vyžadujú ďalšie konfiguračné nastavenia.

Trusted Firewall Advisor

Funkcia Trusted Firewall Advisor analyzuje systémové prenosy z rozličných logických oddielov (oddiely LPAR) za účelom poskytnutia informácií o tom, či by funkcia Trusted Firewall zvýšila výkon systému.

Ak funkcia Trusted Firewall Advisor zaznamená veľké množstvo prenosov z rozličných virtuálnych sietí LAN (VLAN), ktoré sa nachádzajú v tom istom centrálnom elektronickom komplexe, funkcia Trusted Firewall by mohla byť prospešná pre váš systém.

Funkciu Trusted Firewall Advisor povolíte zadaním nasledujúceho príkazu:

```
vlantfw -m
```

Výsledky funkcie Trusted Firewall Advisor zobrazíte zadaním nasledujúceho príkazu:

```
vlantfw -D
```

Funkciu Trusted Firewall Advisor zakážete zadaním nasledujúceho príkazu:

```
vlantfw -M
```

Protokolovanie funkcie Trusted Firewall

Protokolovanie funkcie Trusted Firewall skompiluje zoznam ciest sieťovej premávky v rámci centrálneho elektronického komplexu. Tento zoznam uvádza filtre, ktoré funkcia Trusted Firewall používa na smerovanie premávky.

Ak funkcia Trusted Firewall Advisor zistí, že interné smerovanie prenosov zvyšuje efektivitu, protokolovanie funkcie Trusted Firewall zapíše zoznam ciest do súboru svm.log. Maximálna veľkosť súboru svm.log je obmedzená na 16 MB. Ak položky prekročia limit 16 MB, najstaršie položky za z protokolového súboru odstránia.

Ak chcete spustiť protokolovanie funkcie Trusted Firewall, zadajte nasledujúci príkaz:

```
vlantfw -l
```

Ak chcete zastaviť protokolovanie funkcie Trusted Firewall, zadajte nasledujúci príkaz:

```
vlantfw -L
```

Protokolový súbor nájdete na nasledujúcom umiestnení: /home/padmin/svm/svm.log.

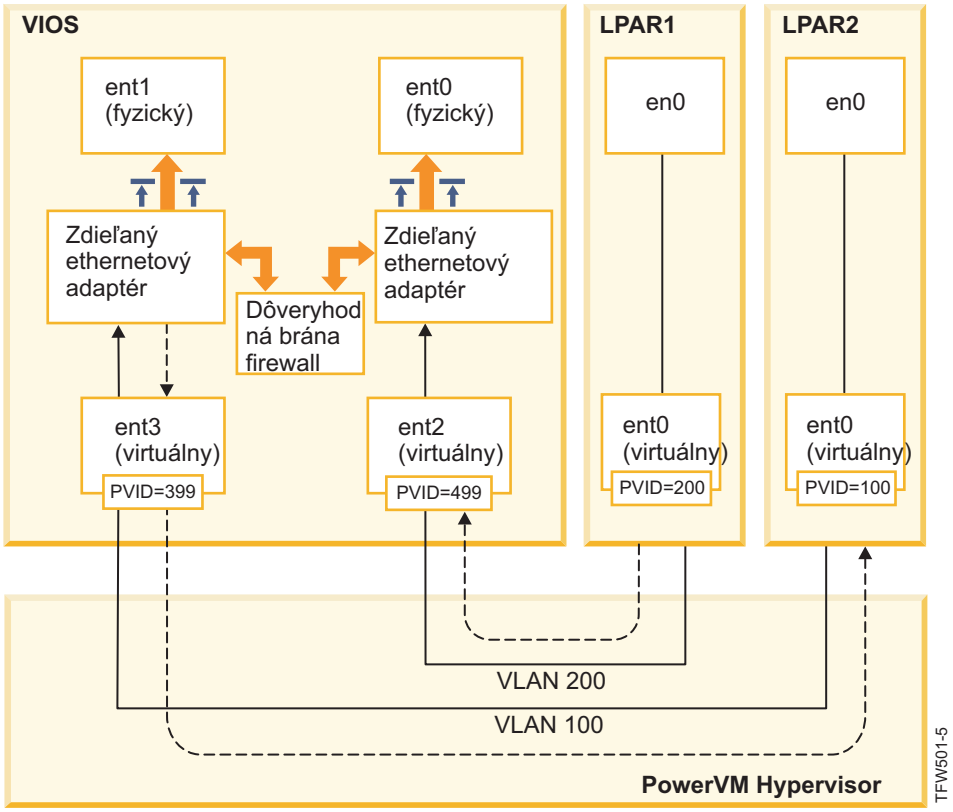
Poznámka: Príkazy na spustenie a zastavenie protokolovania funkcie Trusted Firewall môžete spustiť len vtedy, ak ste prihlásený ako užívateľ root.

Viaceré zdieľané ethernetové adaptéry

Môžete nakonfigurovať funkciu Trusted Firewall na systémoch, ktoré používajú viacero zdieľaných ethernetových adaptérov.

Niektoré konfigurácie používajú viacero SEA na rovnakom systéme Virtual I/O Server (VIOS). Viaceré SEA môžu priniesť výhody ochrany pred núdzovým prepnutím a vyrovnávaním prostriedkov. Trusted Firewall podporuje smerovanie po viacerých SEA za predpokladu, že sú na rovnakom systéme VIOS.

Obrázok 3 ukazuje prostredie používajúce viacero SEA.



Obrázok 3. Konfigurácia používajúca viacero SEA na jednom systéme VIOS

Nasledujú príklady konfigurácií viacerých SEA, ktoré sú podporované funkciou Trusted Firewall:

- Adaptéry SEA sú nakonfigurované s kmeňovými adaptérmi na rovnakom virtuálnom spínači hypervízora Power. Táto konfigurácia je podporovaná, lebo každý SEA prijíma sieťovú premávku s odlišnými ID VLAN.
- Adaptéry SEA sú nakonfigurované s kmeňovými adaptérmi na rozdielnych virtuálnych spínačoch hypervízora Power a každý kmeňový adaptér je na odlišnom ID VLAN. V tejto konfigurácii každý SEA naďalej prijíma sieťovú premávku s použitím odlišných ID VLAN.
- Adaptéry SEA sú nakonfigurované s kmeňovými adaptérmi na rozdielnych virtuálnych spínačoch hypervízora Power a na virtuálnych prepínačoch sú opakovane používané rovnaké ID VLAN. V tomto prípade má premávka pre oba adaptéry SEA rovnaké ID VLAN.

  Príkladom tejto konfigurácie je mať LPAR2 na VLAN200 s virtuálnym spínačom 10 a LPAR3 na VLAN200 s virtuálnym spínačom 20. Keďže oba oddiely LPAR a ich zodpovedajúce adaptéry SEA používajú rovnaké ID VLAN (VLAN200), oba adaptéry SEA majú prístup k paketom s týmto ID VLAN.

Nemôžete povoliť premostenie na viac ako jednom systéme VIOS. Z tohto dôvodu nie sú nasledujúce konfigurácie viacerých SEA podporované funkciou Trusted Firewall:

- Viaceré VIOS a viaceré ovládače SEA.

- Zdieľanie záťaže redundantných SEA: Kmeňové adaptéry, ktoré sú nakonfigurované na smerovanie medzi VLAN, nie je možné rozdeliť medzi servery VIOS.

Odstránenie zdieľaných ethernetových adaptérov

Kroky potrebné na odstránenie zariadení zdieľaných ethernetových adaptérov zo systému sa musia vykonať v určenom poradí.

Ak chcete odstrániť Shared Ethernet Adapter (SEA) zo systému, vykonajte nasledujúce kroky:

1. Odstráňte Security Virtual Machine, ktorý je priradený adaptéru, zadaním nasledujúceho príkazu:
   ```
   rmdev -dev svm
   ```
2. Odstráňte SEA zadaním nasledujúceho príkazu:
   ```
   rmdev -dev ID zdieľaného ethernetového adaptéra
   ```

Poznámka: Pri odstránení adaptéra SEA pred odstránením SVM môže dôjsť k zlyhaniu systému.

Vytváranie pravidiel

Môžete vytvárať pravidlá, ktoré umožnia smerovanie po sieti VLAN funkciou Trusted Firewall.

Ak chcete umožniť smerovanie funkcií Trusted Firewall, musíte vytvoriť pravidlá určujúce, ktorá komunikácia je povolená. Pri vylepšenej bezpečnosti neexistuje ani jedno pravidlo, ktoré povoľuje komunikáciu medzi všetkými sieťami VLAN na systéme. Každé povolené pripojenie vyžaduje svoje vlastné pravidlo, i keď každé pravidlo, ktoré je aktivované, umožňuje komunikáciu v oboch smeroch pre svoje špecifikované koncové body.

Keďže pravidlá sa vytvárajú deaktivujú v rozhraní Virtual I/O Server (VIOS), ďalšie informácie o príkazoch sú dostupné v kolekcii tém VIOS v Informačnom centre pre hardvér Power Systems.

Ak chcete vytvoriť pravidlo, vykonajte nasledujúce kroky:

1. Otvorte rozhranie príkazového riadka VIOS.
2. Inicializujte ovládač SVM zadaním nasledujúceho príkazu:
   ```
   mksvm
   ```
3. Spustite Trusted Firewall zadaním nasledujúceho príkazu:
   ```
   vlantfw -s
   ```
4. Ak chcete zobraziť všetky známe LPAR IP a MAC adresy, zadajte nasledujúci príkaz:
   ```
   vlantfw -d
   ```

   Budete potrebovať IP a MAC adresy logických oddielov (LPAR), pre ktoré vytvárate pravidlá.
5. Vytvorte pravidlo filtrovania na umožnenie komunikácie medzi dvomi logickými oddielmi (LPAR1 a LPAR2) zadaním niektorého z nasledujúcich príkazov (tieto príkazy je potrebné uviesť v jednom riadku):
   ```
   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
   ```

   Poznámka: Jedno pravidlo fitra umožňuje komunikáciu štandardne v oboch smeroch, v závislosti od portu a položiek protokolu. Napríklad, môžete povoliť Telnet pre LPAR1 do LPAR2 spustením nasledujúceho príkazu:
   ```
   genvfilt -v4 -a-P -z [lpar1vlanid] -Z [lpar2vlanid] -s [lpar1ipaddress] -d
       [lpar2ipaddress] -o any -p 0 -O eq -P 23
   ```
6. Ak chcete aktivovať všetky pravidlá filtrov v jadre, zadajte nasledujúci príkaz:
   ```
   mkvfilt -u
   ```

Poznámka: Týmto postupom aktivujete toto pravidlo a všetky ostatné pravidlá filtrovania, ktoré existujú na systéme.

Ďalšie príklady

Nasledujúce príklady ukazujú ďalšie pravidlá filtrovania, ktoré môžete vytvoriť pomocou funkcie Trusted Firewall.

- Ak chvcete povoliť komunikáciu Secure Shell z LPAR na VLAN 100 do LPAR na VLAN 200, zadajte nasledujúci príkaz:

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

- Ak chcete povoliť premávku medzi všetkými portami 0 - 499, zadajte nasledujúci príkaz:

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

- Ak chcete povoliť všetku premávku TCP medzi oddielmi LPAR, zadajte nasledujúci príkaz:

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

  Ak nezadáte žiadne porty alebo operácie portov, premávka môže používať všetky porty.

- Ak chcete povoliť správy ICMP medzi oddielmi LPAR, zadajte nasledujúci príkaz:

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

Súvisiace koncepty:

“Deaktivovanie pravidiel”
Môžete deaktivovať pravidlá, ktoré povoľujú krížové smerovanie VLAN vo funkcii Trusted Firewall.

Súvisiaci odkaz:

“príkaz genvfilt” na strane 150

“príkaz mkvfilt” na strane 152

“Príkaz vlantfw” na strane 170

Súvisiace informácie:

Virtual I/O Server (VIOS)

Deaktivovanie pravidiel

Môžete deaktivovať pravidlá, ktoré povoľujú krížové smerovanie VLAN vo funkcii Trusted Firewall.

Keďže pravidlá sa deaktivujú v rozhraní Virtual I/O Server (VIOS), ďalšie informácie o príkazoch a procesoch sú dostupné v kolekcii tém VIOS v Informačnom centre pre hardvér Power Systems.

Ak chcete deaktivovať pravidlo, vykonajte nasledujúce kroky:

1. Otvorte rozhranie príkazového riadka VIOS.
2. Ak chcete zobraziť všetky aktívna pravidlá filtrov, zadajte nasledujúci príkaz:

   ```
   lsvfilt -a
   ```

   Príznak **-a** môžete vynechať a zobrazia sa všetky pravidlá filtrov uložené v ODM.
3. Všimnite si identifikačné číslo pre pravidlo filtra, ktoré deaktivujete. Pre tento príklad je identifikačné číslo pravidla filtra 23.
4. Deaktivujte pravidlo filtra 23, keď je aktívne v jadre, zadaním nasledujúceho príkazu:

   ```
   rmvfilt -n 23
   ```

   Ak chcete deaktivovať všetky pravidlá filtrov v jadre, zadajte nasledujúci príkaz:

   ```
   rmvfilt -n all
   ```

Súvisiace koncepty:

“Vytváranie pravidiel” na strane 108
Môžete vytvárať pravidlá, ktoré umožnia smerovanie po sieti VLAN funkciou Trusted Firewall.

Súvisiaci odkaz:

“príkaz lsvfilt” na strane 151

“príkaz rmvfilt” na strane 169

Trusted Logging

PowerVM Trusted Logging umožňuje logickým oddielom so systémom AIX (LPAR) zapisovať do protokolových súborov, ktoré sú ložené na pripojenom oddiele Virtual I/O Server (VIOS). Údaje sa prenášajú do systému VIOS priamo cez hypervízora a nevyžaduje sa konektivita siete medzi klientskym LPAR a systémom VIOS.

Virtuálne protokoly

Administrátor Virtual I/O Server (VIOS) vytvorí a spravuje protokolové súbory a tie sa javia operačnému systému AIX ako virtuálne protokolové zariadenie v adresári /dev, podobné virtuálnym diskom alebo virtuálnemu optickému médiu.

Pri ukladaní virtuálnych protokolov sa zvyšuje úroveň dôvery v záznamoch, lebo ich nemôže meniť užívateľ s privilégiami typu root na klientskom LPAR, kde boli vygenerované. Na rovnaký klientsky LPAR môže byť pripojených viacero virtuálnych protokolových zariadení a každý protokol je v inom súbore v adresári /dev.

Funkcia Trusted Logging umožňuje zaznamenávať údaje z rozličných klientskych logických oddielov do protokolu a konsolidovať ich do jedného súborového systému, ktorý je prístupný zo systémuVIOS. Preto VIOS umožňuje jedno umiestnenie na systéme na analýzu a archivovanie protokolov. Administrátor klientskeho LPAR môže nakonfigurovať aplikácie a operačný systém AIX tak, aby sa údaje protokolov zapisovali do virtuálnych protokolových zariadení, čo je podobné zapisovaniu údajov do lokálnych súborov. Podsystém AIX Audit je možné nakonfigurovať tak, aby smeroval záznamy auditu do virtuálnych protokolov a ostatné služby AIX, napríklad syslog, pracovali so svojou existujúcou konfiguráciou a smerovali údaje do virtuálnych protokolov.

Ak chcete nakonfigurovať virtuálny protokol, administrátor VIOS musí zadať názov pre virtuálny protokol, ktorý má nasledujúce samostatné komponenty:

- Názov klienta
- Názov protokolu

Ako názvy týchto dvoch komponentov môže administrátor systému VIOS uviesť ľubovoľnú hodnotu, no názov klienta je zvyčajne rovnaký pre všetky virtuálne protokoly pripojené k danému oddielu LPAR (napríklad názov hostiteľa oddielu LPAR). Názov protokolu sa používa na identifikáciu účelu protokolu (napríklad audit alebo syslog).

Na systéme AIX LPAR, je každé virtuálne protokolové zariadenie prítomné ako dva funkčne ekvivalentné súbory v súborovom systéme /dev. Prvý súbor má názov po zariadení, napríklad /dev/vlog0 a druhý súbor má názov zlučujúci predponu vl s názvom protokolu a číslo zariadenia. Napríklad, ak virtuálne protokolové zariadenie vlog0 má názov protokolu audit, bude uvedené v súborovom systéme /dev ako vlog0 aj vlaudit0.

Súvisiace informácie:

Vytváranie virtuálnych protokolov

Zisťovanie virtuálnych protokolových zariadení

Po tom, ako administrátor VIOS vytvoril virtuálne protokolové zariadenia a pripojil ich ku klientskemu LPAR, konfigurácia klientskeho zariadenia LPAR sa musí obnoviť, aby boli zariadenia viditeľné.

Administrátor klientskeho LPAR obnoví nastavenia pomocou jednej z nasledujúcich metód:

- Rebootovanie klientaLPAR
- Spustenie príkazu **cfgmgr**

Spustite príkaz **lsdev** na zobrazenie virtuálnych protokolových zariadení. Zariadenie majú štandardne predponu vlog. Príklad výstupu príkazu **lsdev** na systéme AIX LPAR, na ktorom sa nachádzajú dve virtuálne protokolové zariadenia:

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

Vlastnosti individuálneho protokolového zariadenia skontrolujete pomocou príkazu lsattr –El <*názov zariadenia*>,ktorý vytvorí približne nasledujúci výstup:

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

Tento výstup zobrazí názov klienta, názov zariadenia a množstvo údajov protokolu, ktoré dokáže VIOS uložiť.

Virtuálny protokol ukladá dva druhy údajov:

- Údaje protokolu: Surové údaje protokolu generované aplikáciami v systéme AIX LPAR.
- Údaje o stave: Informácie o tom, kedy boli zariadenia nakonfigurované, otvorené, zatvorené a ostatné operácie, ktoré boli použité na analyzovanie aktivity protokolu.

Administrátor VIOS špecifikuje množstvo **údajov protokolu** a **údajov o stave**, ktoré možno ukladať pre každý virtuálny protokol a toto množstvo je označené atribútmi max_log_size a max_state_size. Keď množstvo uložených údajov prekročí špecifikovaný limit, staršie údaje protokolu sa prepíšu. Administrátor VIOS musí zabezpečiť, aby sa údaje protokolu zhromažďovali a archivovali pravidelne, aby sa protokoly zachovali.

Inštalácia funkcie Trusted Logging

Funkciu PowerSC Trusted Logging môžete nainštalovať pomocou rozhrania príkazového riadka alebo nástroja SMIT.

Nevyhnutné podmienky na inštaláciu funkcie Trusted Logging sú VIOS 2.2.1.0, alebo novší a IBM AIX 6 s technologickou úrovňou 7 alebo IBM AIX 7 s technologickou úrovňou 1.

Názov súboru na inštaláciu funkcie Trusted Logging je powerscStd.vlog a tento sa nachádza na inštalačnom CD PowerSC Standard Edition.

Inštalácia funkcie Trusted Logging:

1. Musíte mať spustený VIOS, verzia 2.2.1.0 alebo novší.
2. Vložte inštalačné CD PowerSC alebo si prevezmite obraz inštalačného CD.
3. Pomocou príkazu **installp** alebo nástroja SMIT nainštalujte sadu súborov powerscStd.vlog.

Súvisiace informácie:

“Inštalácia PowerSC Standard Edition” na strane 7
Pre každú špecifickú funkciu PowerSC Standard Edition musíte nainštalovať sadu súborov.

Konfigurácia funkcie Trusted Logging

Naučte sa postup ako konfigurovať dôveryhodné protokolovanie v podsystéme AIX Audit a v súbore syslog.

Konfigurácia podsystému AIX Audit

Okrem zápisu protokolov do lokálneho súborového systému možno podsystém AIX Audit konfigurovať na zápis binárnych údajov do virtuálneho protokolového zariadenia.

Poznámka: Skôr ako nakonfigurujete podsystém auditu systému AIX, musíte dokončiť postup v téme “Zisťovanie virtuálnych protokolových zariadení” na strane 111.

Ak chcete nakonfigurovať podsystém auditu systému AIX, postupujte podľa týchto pokynov:

1. Nakonfigurujte podsystém AIX Audit na protokolovanie údajov v binárnom režime (auditbin).
2. Aktivujte dôveryhodné protokolovanie pre auditovanie AIX úpravou konfiguračného súboru /etc/security/audit/config.
3. Do odseku bin: pridajte parameter virtual_log = /dev/vlog0.

   Poznámka: Pokyn je platný, ak administrátor LPAR chce, aby boli údaje auditbin zapísané do /dev/vlog0.
4. Reštartujete podsystém AIX Audit v tejto postupnosti:

   ```
   vypnutie auditu
   spustenie auditu
   ```

Správy z auditu sú okrem zápisu protokolov do lokálneho súborového systému zapísané aj do Virtual I/O Server (VIOS) prostredníctvom určeného virtuálneho protokolového zariadenia. Protokoly sú uložené pod kontrolou existujúcich parametrov bin1 a bin2 v odseku bin: konfiguračného súboru /etc/security/audit/config.

Súvisiace informácie:

Podsystém auditovania

Konfigurácia súboru syslog

Súbor syslog možno konfigurovať na zápis správ do virtuálnych protokolov pridaním pravidiel do súboru /etc/syslog.conf.

Poznámka: Skôr ako nakonfigurujete súbor /etc/syslog.conf, musíte dokončiť postup v téme “Zisťovanie virtuálnych protokolových zariadení” na strane 111.

Súbor /etc/syslog.conf môžete upraviť tak, aby sa zhodoval so správami protokolu, ktoré sú založené na týchto kritériách:

- Zariadenie
- Úroveň priority

Ak chcete použiť virtuálne protokoly pre správy syslog, súbor /etc/syslog.conf musí byť nakonfigurovaný s pravidlami na zápis požadovaných správ do príslušného virtuálneho protokolu v adresári /dev.

Napríklad ak chcete odoslať do virtuálneho protokolu vlog0 správy úrovne ladenia, ktoré vygeneruje ľubovoľné zariadenie, do súboru /etc/syslog.conf pridajte tento riadok:

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

Poznámka: Nepoužívajte zariadenia na rotáciu protokolov dostupné v démonovi syslogd pre ľubovoľný príkaz, ktorý zapisuje údaje do virtuálnych protokolov. Súbory v súborovom systéme /dev nie sú regulárne súbory a nie je možné ich premenovať alebo presunúť. Administrátor servera VIOS musí konfigurovať rotáciu virtuálnych protokolov v rámci servera VIOS.

Démon syslogd musí byť po konfigurácii reštartovaný týmto príkazom:

```
refresh -s syslogd
```

Súvisiace informácie:

syslogd Daemon

Zapisovanie údajov do virtuálnych protokolových zariadení

Ľubovoľné údaje sa zapisujú do virtuálneho protokolového zariadenia otvorením príslušného súboru v adresári /dev a zapísaním údajov do tohto súboru. Virtuálny protokol je možné otvoriť súčasne len jedným procesom.

Napríklad:

Ak chcete zapisovať správy do virtuálnych protokolových zariadení pomocou príkazu **echo**, zadajte nasledujúci príkaz:

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

Ak chcete uložiť súbory do virtuálnych protokolových zariadení pomocou príkazu **cat**, zadajte nasledujúci príkaz:

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

Maximálna veľkosť individuálneho zápisu je obmedzená na 32 KB a programy, ktoré sa pokúsia zapísať viac údajov v jednej operácii zápisu, dostanú chybu I/O (EIO). Pomocné programy rozhrania príkazového riadka (CLI), napríklad príkaz **cat**, automaticky rozdelia prenosy do 32 KB operácií zápisu.

Trusted Network Connect (TNC)

Trusted Network Connect (TNC) je súčasť skupiny funkcií Trusted Computing Group (TCG), ktorá poskytuje špecifikácie na overenie integrity koncových bodov. TNC má definovanú otvorenú architektúru riešení, ktorá pomáha administrátorom vynucovať politiky na efektívne riadenie prístupu k infraštruktúre siete.

Trusted Network Connect (TNC) má štyri komponenty:

- Server TNC
- TNC Patch Management
- Server TNC
- Odkazovač IP TNC

Základné pojmy pre Trusted Network Connect

Zistite viac o komponentoch, konfigurovaní bezpečnej komunikácie a systéme riadenia opráv pre Trusted Network Connect (TNC).

Komponenty rámca Trusted Network Connect

Zistite viac o komponentoch rámca Trusted Network Connect (TNC).

Model TNC pozostáva z nasledujúcich komponentov:

Server Trusted Network Connect (TNC)

Server Trusted Network Connect (TNC) identifikuje klientov, ktorí sa pridávajú do siete a iniciuje na nich overovanie.

Klient TNC poskytuje vyžadované informácie o úrovni sady súborov pre server na overovanie. Server zisťuje, či klient je na úrovni nakonfigurovanej administrátorom. Ak klient toto nespĺňa, server TNC upozorní administrátora o vyžadovaných nápravách.

Server TNC iniciuje overovania na klientoch, ktorí sa pokúšajú o prístup do siete. Server TNC načíta množinu identifikátorov IMV, ktoré môžu vyžadovať merania integrity od klientov a overovať ich. AIX má predvolený IMV, ktorý overuje sadu súborov a úroveň bezpečnostných opráv systémov. Server TNC je pracovný rámec, ktorý zavádza a riadi viacero modulov IMV. Pri overovaní klienta sa spolieha na to, že IMV budú vyžadovať informácie od klientov overia klientov.

TNCPM (TNC Patch Management)

Server Trusted Network Connect (TNC) sa integruje s programami Service Update Management Assistant (SUMA) a cURL, poskytujúc tak riešenie na správu opráv.

Správca opráv stiahne najnovšie servisné balíky a bezpečnostné opravy, ktoré sú dostupné vo webových lokalitách IBM ECC a Fix Central. Démon TNC Patch Management odošle najnovšie aktualizované informácie na server TNC, ktorý poskytuje východiskovú sadu súborov na overenie klientov.

Démon **tncpmd** musí bť nakonfigurovaný tak, aby spravoval položky stiahnuté cez SUMA a odosielal informácie o sadách súborov na server TNC. Tento démon sa musí spúšťať v systéme, ktorý je pripojený na internet, aby bolo možné automaticky sťahovať aktualizácie. Ak chcete používať server riadenia opráv TNC bez jeho pripojenia na Internet, môžete zaregistrovať užívateľom definovaný archív opráv so serverom riadenia opráv TNC.

Poznámka: Server TNC a démon **tncpmd** môžu byť hosťovaní na tom istom systéme.

Správa opráv sa poskytuje nasledujúcimi spôsobmi:

- pomocou rozhrania príkazového riadka (pmconf)
- pomocou démona (tncpmd2)

Zabezpečenie správy opráv pomocou rozhrania príkazového riadka (pmconf):

Pri stiahnutí úrovne servisného balíka (úroveň SP) s použitím príkazu **pmconf add** sa zavolajú programy SUMA a cURL.

Po stiahnutí úrovne servisného balíka (úroveň SP) s použitím príkazu **pmconf add** sa zavolá program SUMA na stiahnutie a registráciu úrovne SP v TNC. Okrem toho sa zavolá program cURL na stiahnutie nových alebo chýbajúcich bezpečnostných opráv.

Nasledujúce argumenty príkazu **pmconf get** poskytujú ďalšiu možnosti správy bezpečnostných opráv:

- **display-only** umožňuje užívateľovi prečítať si popis bezpečnostných nedostatkov, ktoré riešia príslušné bezpečnostné opravy pre danú úroveň SP. Bezpečnostné opravy sa nestiahnu pri použití tohto argumentu.
- **download-only** umožňuje užívateľovi stiahnuť bezpečnostné opravy do užívateľom určeného adresára bez nainštalovania týchto opráv. Neuplatnia sa žiadne opravy.

Používanie démona (tncpmd2) na účely správy opráv:

Komponent plánovača tohto démona môžete nakonfigurovať tak, aby automaticky vyhľadával aktualizácie, ktoré majú vplyv na zabezpečenie klientov TNC.

Interval sťahovania určuje, ako často má plánovač vyhľadávať nové úrovne servisných balíkov. Ak sa zistí nová úroveň servisného balíka pre technologickú úroveň (TL), ktorá je zaregistrovaná v TNC, nová úroveň servisného balíka, ako aj všetky chýbajúce alebo nové bezpečnostné opravy sa stiahnu a pridajú do archívu. Interval sťahovania môžete nastaviť pomocou príkazu **pmconf init**. Odporúčaný interval vyhľadávania aktualizácií je aspoň raz do mesiaca (43200 minút).

Interval ifix_download_interval určuje, ako často má plánovačč vyhľadávať nové bezpečnostné dočasné opravy (ifix), ktoré mohli byť zverejnené. Všetky nové bezpečnostné opravy sa stiahnu a pridajú do archívu. Odporúčaný interval sťahovania opráv ifix je raz za deň (1440 minút).

Klient Trusted Network Connect

Klient Trusted Network Connect (TNC) poskytuje informácie, ktoré vyžaduje server TNC na overovanie.

Server zisťuje, či klient je na úrovni nakonfigurovanej administrátorom. Ak klient toto nespĺňa, server TNC upozorní administrátora o vyžadovaných aktualizáciách.

Klient TNC zavedie IMC pri spustení a pomocou IMC zhromaždí vyžadované informácie.

Odkazovač IP Trusted Network Connect

Server Trusted Network Connect (TNC) môže automaticky iniciovať overovanie na klientoch, ktorí sú súčasťou siete. Odkazovač IP spustený na oddiele Virtual I/O Server (VIOS) deteguje nových klientov, ktorí sú obsluhovaní VIOS a odošle ich IP adresy na TNC. Server TNC overí klienta vo veci politiky, ktorý je definovaná.

Bezpečná komunikácia IP Trusted Network Connect

Démoni Trusted Network Connect (TNC) komunikujú cez zašifrované kanály, ktoré sú povolené v Transport Layer Security (TLS) alebo Secure Sockets Layer (SSL).

Bezpečná komunikácia slúži na zaistenie, že údaje a príkazy, ktoré prúdia v sieti, sú autentifikované a bezpečné. Každý systém musí mať vlastný kľúč a certifikát, ktorý sa vygeneruje, keď sa spustí inicializačný príkaz pre komponenty. Tento proces je pre administrátora úplne transparentný a vyžaduje menšiu účasť administrátora.

Ak chcete overiť nového klienta, je potrebné importovať certifikát klienta do databázy servera. Tento certifikát sa na začiatku označí ako nedôveryhodný a potom administrátor pomocou príkazu **psconf** zobrazí a označí certifikáty ako dôveryhodné zadaním nasledujúceho príkazu:

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

Ak chcete použiť iný kľúč, príkaz **psconf** umožňuje voľbu na importovanie certifikátu.

Ak chcete importovať certifikát zo servera, zadajte nasledujúci príkaz:

```
psconf import  -S -k<názov súboru kľúčov> -f<názov súboru kľúčov>
```

Ak chcete importovať certifikát z klienta, zadajte nasledujúci príkaz:

```
psconf import -C -k<názov súboru kľúčov> -f<názov súboru kľúčov>
```

Protokol Trusted Network Connect

Protokol Trusted Network Connect (TNC) sa používa v pracovnom rámci TNC na udržiavanie integrity siete.

TNC obsahuje špecifikácie na overovanie integrity koncových bodov. Koncové body, ktoré vyžadujú prístup, sa posudzujú na základe meraní integrity kľúčových komponentov, ktoré môžu svoje prevádzkové prostredie. Pracovný rámec TNC umožňuje administrátorom monitorovať integritu systémov v sieti. TNC je integrovaný s infraštruktúrou distribúcie opráv AIX, čo vytvára kompletné riešenie riadenia opráv.

Špecifikácie TNC musí spĺňať požiadavky architektúry systémov AIX a rad systémov POWER. Komponenty TNC slúžia na zabezpečenie komplexného riešenia riadenia opráv na operačnom systéme AIX. Táto konfigurácia umožňuje administrátorom efektívne spravovať softvérovú konfiguráciu na umiestneniach AIX. Poskytuje nástroje na overovanie úrovní opráv systémov a generovanie zostavy na klientoch, ktorí nie sú kompatibilní. Navyše sprava opráv zjednodušuje proces preberania opráv a ich inštalovania.

Moduly IMC a IMV

Server alebo klient Trusted Network Connect (TNC) interne používajú moduly Integrity measurement collector (IMC) a Integrity measurement verifier (IMV) na overovanie servera.

Tento pracovný rámec umožňuje zavedenie viacerých modulov IMC a IMV na server a klientov. Modul, ktorý vykonáva, overovanie na úrovni operačného systému (OS) a sady súborov sa štandardne dodáva s operačným systémom AIX. Na prístup k modulom, ktoré sa dodávajú s operačným systémom AIX, použite jednu z nasledujúcich ciest:

- /usr/lib/security/tnc/libfileset_imc.a: Zhromaždí informácie o úrovni a sade súborov OS, ktoré sú nainštalované z klientskeho systému a odošle ich na IMV (server TNC) na overenie.
- /usr/lib/security/tnc/libfileset_imv.a: Vyžiada informácie o úrovni a sade súborov OS z klinta a porovná ich so základnými informáciami. Aktualizuje tiež stav klienta do databázy servera TNC. Ak chcete zobraziť stav, zadajte nasledujúci príkaz:

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

Súvisiaci odkaz:

“Príkaz pscon” na strane 157

Požiadavky TNC

Aby ste mohli naplno využívať všetky funkcie každého komponentu TNC, musíte sa uistiť, že vaše prostredie splňuje aspoň minimálne požiadavky.

TNCPM (TNC Patch Management)

AIX	SUMA	OpenSSL	Poznámky
7.2 TL1	7.2.1.0	1.0.2	Dodáva sa s operačným systémom
7.2 TL0	7.2.1.0	1.0.2	Softvé SUMA/Java môže byť potrebné nainštalovať samostatne.
7.1 TL4	7.2.1.0	1.0.2	Softvé SUMA/Java môže byť potrebné nainštalovať samostatne.
7.1 TL1, TL2, TL3			Žiadna podpora pre sťahovanie úrovní servisných balíkov pre operačný systém AIX 7.2
7.1 TL0			Minimálna podporovaná úroveň vydania pre TNCPM

Konfigurácia komponentov TNC

Každý komponent Trusted Network Connect (TNC) vyžaduje isté nastavenie, aby ste ho mohli používať vo vašom prostredí.

Každý krok nasledujúceho postupu je vyžadovaný pri konfigurácii komponentov TCN. Ďalšie voliteľné kroky sú uvedené v téme

1. Identifikujte IP adresy systémov, na ktorých chcete nastaviť server TNC, server TNC Patch Management (TNCPM) a odkazujúci server IP TNC pre systém Virtual I/O Server (VIOS).
2. Nastavte server NIM (Network Installation Management). Systém, ktorý je nakonfigurovaný ako server TNCPM, je hlavný počítač NIM. Na tento systém musíte nainštalovať sadu súborov sets:bos.sysmgt.nim.master.
3. Musíte povoliť funkciu Autonomic Health Advisor (AHA) pre automatické oznámenia o nových servisných balíkoch a bezpečnostných opravách na serveri TNC. Ak funkcia AHA nie je povolená, plánovač TNC bude aktualizovať informácie na serveri TNC v určených časových intervaloch. Povolenie funkcie AHA pre automatické oznámenia:

   ```
   mkdir /aha
    /usr/sbin/mount -v ahafs  /aha /aha
   ```
4. Ak chcete inicializovať archívy opráv pre server TNC Patch Management, zadajte nasledujúci príkaz (príkaz uveďte v jednom riadku):

   ```
   pmconf init -i <interval sťahovania> -l <zoznam TL> [-A] [-P <cieľová cesta>]
   [-x <interval ifix>] [-K <kľúč ifix>]
   ```

   Príklad príkazu **pmconf**:

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

   Príkaz **init** stiahne najnovší servisný balík pre každú technologickú úroveň a sprístupní ho pre server TNC. Aktualizované servisné balíky umožňujú serveru TNC spustiť základné overenie klienta TNC a pre server na správu opráv TNC nainštalovať aktualizácie klienta TNC. Zadajte príznak **-A** na akceptovanie všetkých licenčných zmlúv pri spúšťaní aktualizácií klienta. Archívy opráv, ktoré stiahne server na správu opráv TNC, sa štandardne nachádzajú v súbore /var/tnc/tncpm/fix_repository. Pomocou príznaku **-P** zadajte iný adresár.
5. Nastavte server TNCPM. Server TNCPM môžete nastaviť na systéme NIM. Server TNCPM používa prístup cez SUMA na sťahovanie opráv z webových lokalít IBM Fix Central a ECC. Server TNCPM používa cURL na sťahovanie opráv ifix z lokality IBM Security. Ak chcete stiahnuť aktualizácie, systém musí byť pripojený na internet. Ak chcete konfigurovať server TNCPM, zadajte tento príkaz:

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

   Napríklad:

   ```
   pmconf mktncpm pmport=20000 tncserver=1.1.1.1:10000
   ```
6. Konfigurujte politiky na serveri TNC. Informácie o vytváraní politík pre overovanie klientov nájdete v téme “Vytváranie politík pre klienta Trusted Network Connect” na strane 123
7. Pomocou tohto príkazu konfigurujte klientov:

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

Napríklad:

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

8. Dokončite nastavenie komponentov TNC vykonaním voliteľných krokov pre jednotlivé komponenty.

Súvisiaci odkaz:

"Príkaz pscon" na strane 157

Súvisiace informácie:

"Inštalácia PowerSC Standard Edition" na strane 7
Pre každú špecifickú funkciu PowerSC Standard Edition musíte nainštalovať sadu súborov.

Inštalácia s NIM

IBM Fix Central

Online pomocné centrum Passport Advantage

Konfigurácia volieb pre komponenty TNC

Môžete nakonfigurovať voľby pre jednotlivé komponenty TNC.

Konfigurácia volieb pre server Trusted Network Connect (TNC)

Naučte sa nakonfigurovať server TNC.

Ak chcete konfigurovať server TNC, súbor /etc/tnccs.conf musí mať hodnotu podobnú tejto:

```
komponent = SERVER
```

Ak chcete systém konfigurovať ako server, zadajte tento príkaz:

```
psconf mkserver tncport=<port> pmserver=<ip|názov_hostiteľa[,ip2|názov_hostiteľa2..]:port>
[recheck_interval=<čas v minútach>]
```

Napríklad:

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

Poznámka: Port tncport a port pmserver musia byť nastavené na rozličné hodnoty, a ak nie je poskytnutá hodnota parametra recheck_interval, použije sa predvolená hodnota 1440 minút.

Predvolená hodnota portu 42830 sa používa pre port tncport a predvolená hodnota 38240 sa používa pre port pmserver.

Súvisiaci odkaz:

"Príkaz pscon" na strane 157

Konfigurácia ďalších volieb pre klienta TNC (Trusted Network Connect)

Zistite, ako môžete nakonfigurovať klienta TNC (Trusted Network Connect) a spoznajte vyžadované konfiguračné nastavenia.

Ak chcete konfigurovať klienta TNC, súbor /etc/tnccs.conf musí mať hodnotu podobnú tejto:

```
komponent = CLIENT
```

Ak chcete systém konfigurovať ako klienta, zadajte tento príkaz:

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

Napríklad:

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

Poznámka: Hodnota portu servera a hodnota tncport, čo je port klienta, musí byť identická.

| **Súvisiaci odkaz**:
| "Príkaz pscon" na strane 157

Konfigurácia volieb pre server TNCPM

| Server TNCPM (Trusted Network Connect Patch Manager) sa integruje s riešeniami SUMA a cURL pre poskytnutie komplexného riešenia na správu opráv.

| Server TNCPM musíte nakonfigurovať na serveri NIM (Network Installation Management), aby bolo možné aktualizovať klientov TNC.

| Ak chcete povoliť automatické stiahnutia dokumentov s analýzou bezpečnosti a dočasných opráv IBM, zadajte interval dočasných opráv. Táto funkcia poskytuje automatické oznámenie o novo publikovaných bezpečnostných dočasných opravách a priradených identifikátoroch CVE (Common Vulnerabilities and Exposures). Všetky dokumenty s analýzou bezpečnosti a dočasné opravy sú overené pred registráciou v TNC. Verejný kľúč bezpečnostného nedostatku IBM AIX, ktorý sa vyžaduje na automatické stiahnutie dočasných opráv, je k dispozícii na webovej stránke IBM AIX Security. Automatické stiahnutia servisných balíkov a dočasných opráv sú zakázané nastavením intervalu stiahnutia a intervalu dočasných opráv na 0.

| Registráciu servisných balíkov a dočasných opráv môžete aktualizovať aj manuálne. Ak chcete manuálne zaregistrovať dokument s analýzou bezpečnosti IBM s príslušnými dočasnými opravami, zadajte tento príkaz:

```
pmconf add -y <súbor dokumentu s analýzou problému> -v <súbor s podpisom>  -e  <súbor tar ifix>
```

| Ak chcete manuálne zaregistrovať samostatnú dočasnú opravu, zadajte tento príkaz:

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

| Ak chcete zaregistrovať novú technologickú úroveň a stiahnuť jej najnovší servisný balík, zadajte tento príkaz:

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

| Ak chcete stiahnuť servisný balík, ktorý nie je najaktuálnejšou verziou, alebo ak chcete stiahnuť technologickú úroveň, ktorá sa má použiť na overenie a aktualizácie klientov, zadajte tento príkaz:

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

| Ak chcete zaregistrovať servisný balík alebo archív opráv technologickej úrovne, ktorý existuje v systéme, zadajte tento príkaz:

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

| Ak chcete konfigurovať systém, aby slúžil ako server na správu opráv, zadajte tento príkaz:

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

| Príklad tohto príkazu:

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

| Server na správu opráv TNC vždy podporuje správu bezpečnostných hlásení o analýze autorizovaným programom (APAR). Ak chcete konfigurovať správu opráv TNC na správu iných typov hlásení APAR, zadajte tento príkaz:

```
pmconf add -t <zoznam_typov_APAR>
```

| V predchádzajúcom príklade je <zoznam_typov_APAR> zoznam údajov oddelených čiarkou, ktorý obsahuje tieto typy hlásení APAR:

| • HIPER
| • PE
| • Rozšírenie

Na správu archívov balíkov TNCPM Open Package môžete použiť nasledujúce príkazy:

```
pmconf add -o <názov balíka> -V <verzia> -T [installp|rqm] -D <užívateľom definovaná cesta>
pmconf delete -o <názov balíka> -V <verzia>
pmconf list -o <názov balíka> -V <verzia>
pmconf list -O [-c] [-q]
```

Balíky Open Package sa pridajú do tohto predvoleného adresára:

/var/tnc/tncpm/fix_repository/packages.

užívateľom definovaná cesta = umiestnenie balíka v systéme

Ak chcete zobraziť popisné informácie o problémoch, ktoré riešia bezpečnostné opravy pre konkrétnu úroveň servisného balíka, bez inštalácie opráv do archívu, zadajte nasledujúci príkaz:

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

Napríklad:

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

Ak chcete stiahnuť bezpečnostné opravy pre konkrétnu úroveň servisného balíka bez inštalácie opráv do archívu, zadajte nasledujúci príkaz:

```
pmconf get -p <SP> -D <cieľový adresár>
```

Poznámka: Pred spustením príkazu už musí existovať *cieľový adresár*.

Napríklad:

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

Server TNCPM podporuje príkaz **syslog** v súvislosti so sťahovaním servisných balíkov, úrovňami technológií a aktualizáciami klientov. Zariadenie je user a priorita je info. Príkladom je user.info.

Server na správu opráv TNC tiež udržiava protokol so všetkými aktualizáciami klienta v adresári /var/tnc/tncpm/log/update/<ip>/<timestamp>.

Súvisiaci odkaz:

"Príkaz pscon" na strane 157

Súvisiace informácie:

IBM AIX Security

Konfigurácia e-mailového oznámenia na serveri Trusted Network Connect

Naučte sa postup ako konfigurovať e-mailové oznámenie pre server TNC (Trusted Network Connect).

Server TNC zobrazuje úroveň opravy klienta a ak server TNC zistí, že klient nie je kompatibilný, odošle e-mail administrátorovi s výsledkom a vyžadovanou opravou.

Ak chcete konfigurovať e-mailovú adresu administrátora, zadajte tento príkaz:

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

Napríklad:

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

V predchádzajúcom príklade je e-mail pre skupinu IP *vayugrp1* a *vayugrp2* odoslaný na e-mailovú adresu abc@ibm.com.

Ak chcete e-mail odoslať na globálnu e-mailovú adresu pre skupinu IP, ktorá nemá priradenú e-mailovú adresu, zadajte tento príkaz:

```
psconf add –e <poštová_adresa>
```

Napríklad:

```
psconf add –e abc@ibm.com
```

Ak v predchádzajúcom príklade skupina IP nemá priradenú e-mailovú adresu, e-mail bude odoslaný na e-mailovú adresu abc@ibm.com. Funguje ako globálna e-mailová adresa.

Súvisiaci odkaz:

"Príkaz pscon" na strane 157

Konfigurácia odkazujúceho servera IP na serveri VIOS

Naučte sa ako konfigurovať odkazujúci server IP na serveri Virtual I/O Server (VIOS), aby sa automaticky iniciovalo overenie.

Poznámka: Pred konfiguráciou odkazujúceho servera IP musíte konfigurovať rozšírenie jadra SVM na serveri VIOS (Virtual I/O Server).

Ak chcete konfigurovať odkazujúci server TNC IP, konfiguračný súbor /etc/tnccs.conf musí mať nastavenie podobné tomuto komponent = IPREF.

Zadajte tento príkaz na konfiguráciu systému ako klienta:

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

Napríklad:

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

Hodnota portu tncserver a portu tncport, čo je port klienta, musí byť identická.

Konfigurujte odkazujúci server TNC IP v VIOS. Táto konfigurácia v VIOS spustí overenie v klientoch, ktoré sa pripájajú do siete. Na konfiguráciu odkazujúceho servera zadajte tento príkaz:

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

Napríklad:

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

Poznámka: Hodnota portu servera a portu TNC, ktorý je portom klienta, musí byť identická.

Súvisiaci odkaz:

"Príkaz pscon" na strane 157

Správa komponentov Trusted Network Connect (TNC)

Naučte sa ako spravovať TNC (Trusted Network Connect), aby ste mohli vykonávať úlohy ako pridávanie klientov, politík, protokolov, výsledkov overenia, a aktualizáciu klientov a certifikátov súvisiacich s TNC.

Prezeranie protokolov servera Trusted Network Connect

Zistite, ako prezerať protokoly servera the Trusted Network Connect (TNC).

Server TNC protokoluje výsledky overovania všetkých klientov. Ak chcete zobraziť protokol, spustite príkaz **psconf**:

```
psconf list –H –i <ip |ALL>
```

Súvisiaci odkaz:

| “Príkaz pscon” na strane 157

Vytváranie politík pre klienta Trusted Network Connect

Naučte sa ako nastaviť politiky súvisiace s klientom TNC (Trusted Network Connect).

Konzola psconf poskytuje rozhranie, ktoré je vyžadované na správu politík TNC. Každého klienta alebo skupinu klientov možno prepojiť s politikou.

Vytvoriť možno tieto politiky:

- Skupina Internet Protocol (IP) obsahuje viacero klientskych IP adries.
- Každý IP klienta môže patriť len do jednej skupiny.
- Skupina IP je prepojená so skupinou politík.
- Skupina politík obsahuje rozličné druhy politík. Napríklad politika sady súborov, ktorá určuje, aká musí byť úroveň operačného systému klienta (to jest vydanie, technologická úroveň a servisný balík). V skupine politík môže byť viacero politík sád súborov a klient, ktorý odkazuje na túto politiku, musí byť na úrovni určenej jednou z politík sád súborov.

Tieto príkazy ukazujú ako vytvoriť skupinu IP, skupinu politiky, a politiky sád súborov.

Ak chcete vytvoriť skupinu IP, zadajte tento príkaz:

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

Napríklad:

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

Poznámka: Pre skupinu musí byť uvedený minimálne jeden internetový protokol. Viaceré internetové protokoly musia byť oddelené čiarkou.

Ak chcete vytvoriť politiku sady súborov, zadajte tento príkaz:

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

Napríklad:

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

Poznámka: Informácie o zostavení musia mať formát <rel00-TL-sp>.

Ak chcete vytvoriť politiku a priradiť skupinu IP, zadajte tento príkaz:

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

Napríklad:

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

Ak chcete do politiky priradiť politiku sady súborov, zadajte tento príkaz:

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

Napríklad:

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

Ak chcete pridať politiku OpenPackage, zadajte nasledujúci príkaz:

```
pconf add -O <skupina_openpkg> <názov_openpkg:verzia>
```

Toto je príklad pridania politiky OpenPackage:

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

Ak chcete priradiť politiku OpenPackage k politike sady súborov, zadajte nasledujúci príkaz:

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

Poznámka: Ak je poskytnutých viacero politík sád súborov, systém vynúti najlepšiu zhodujúcu sa politiku v klientovi. Ak je klient napríklad na 6100-02-01 a vy spomeniete politiku sady súborov ako 7100-03-04 a 6100-02-03, v klientovi bude vynútené 6100-02-03.

Súvisiaci odkaz:

"Príkaz pscon" na strane 157

Spustenie overovania pre klienta Trusted Network Connect

Zistite, ako overiť klienta Trusted Network Connect (TNC).

Na overenie klienta použite jednu z nasledujúcich metód:

- Démon odkazovača IP na systéme Virtual I/O Server (VIOS) preposiela IP adresu na server TNC: Klientsky LPAR získa túto IP a pokúsi sa o prístup do siete. Démon odkazovača IP na systéme VIOS deteguje novú IP adresu a prepošle ju na server TNC: Server TNC iniciuje overovanie pri prijímaní novej IP adresy.
- Server TNC pravidelne overuje klienta: administrátor môže pridať klientske IP, ktoré sa majú overovať, databázy politiky TNC. Server TNC overuje klientov, ktorí sú v databáze. Opakované overovanie sa vykoná automaticky v pravidelných intervaloch s referenciou na hodnotu atribútu recheck_interval, ktorá je špecifikovaná v konfiguračnom súbore /etc/tnccs.conf.
- Administrátor iniciuje overovanie klienta manuálne: Administrátor môže iniciovať overovanie manuálne na kontrolu, či bol klient pridaný do siete, keď spustí nasledujúci príkaz:

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

Poznámka: Pre prostriedky, ktoré nie sú pripojení k systému VIOS, je možné klientov overiť a aktualizovať, keď sa pridávajú manuálne na server TNC.

Súvisiaci odkaz:

"Príkaz pscon" na strane 157

Prezeranie výsledkov overovania Trusted Network Connect

Zistite, ako prezerať výsledky overovania klienta Trusted Network Connect (TNC).

Ak chcete prezerať výsledky overovania klientov v sieti, zadajte nasledujúci príkaz:

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

Tento príkaz zobrazí všetkých klientov, ktorí majú stav **IGNORED**, **COMPLIANT** alebo **FAILED**.

- **IGNORED**: IP klienta sa ignoruje v zozname IP (t.j. tento klient môže byť vylúčený z overovania).
- **COMPLIANT**: Klient prešiel overovaním (t.j. klient spĺňa politiku).
- **FAILED**: Klient neprešiel overovaním (t.j. klient nespĺňa politiku a vyžaduje sa adrministračný zásah).

Ak chcete určiť príčinu zlyhania, spustite príkaz **psconf** s IP klienta, ktorý neuspel:

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

Súvisiaci odkaz:

"Príkaz pscon" na strane 157

Aktualizácia klienta Trusted Network Connect

Server Trusted Network Connect (TNC) overí klienta a aktualizuje databázu so stavom klienta a výsledkom overovania. Administrátor môže vidieť tieto výsledky a podniknúť krok na aktualizáciu klienta.

Ak chcete aktualizovať klienta, ktorý je na predchádzajúcej úrovni, zadajte nasledujúci príkaz:

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

| Napríklad:

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

| Príkaz **psconf** aktualizuje klienta so zostavením a inštaláciami APAR, pokiaľ nie sú nainštalované.

| Aktualizácia klienta pomocou balíkov Open Package:

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

| **Súvisiaci odkaz**:

| "Príkaz pscon" na strane 157

Správa politík na správu opráv

| Príkaz **pmconf** umožňuje konfigurovať politiky na správu opráv.

| Politiky na správu opráv poskytujú informácie, napríklad IP adresu servera TNC a časový interval na inicializáciu aktualizácie SUMA.

| Ak chcete riadiť politiku na správu opráv, zadajte tento príkaz:

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

| Napríklad:

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

| **Poznámka:** Porty pmport a tncserver musia byť odlišné.

| **Súvisiaci odkaz**:

| "príkaz pmconf" na strane 153

Import certifikátov Trusted Network Connect

| Naučte sa ako importovať certifikát a ako bezpečne vysielať údaje v sieti.

| Démony TNC (Trusted Network Connect) komunikujú cez šifrované kanály povolené cez protokol TLS (Transport Layer Security) alebo protokol SSL (Secure Sockets Layer). Tento démon zabezpečuje, že údaje a príkazy, ktoré sú transportované v sieti, sú autentifikované a bezpečné. Každý systém má vlastný kľúč a certifikát, ktoré sú vygenerované pri spustení príkazu inicializácie pre komponenty. Tento proces je administrátorovi jasný a vyžaduje od neho menej zapojenia. Keď je klient overovaný po prvý raz, jeho certifikát je importovaný do databázy servera. Certifikát je označený ako pôvodne nedôveryhodný a administrátor použije príkaz **psconf** na zobrazenie a označenie certifikátov ako dôveryhodných zadaním tohto príkazu:

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

| Ak chce administrátor použiť iný kľúč a certifikát, príkaz **psconf** poskytuje funkciu na import kľúča certifikátu.

| Ak chcete certifikát importovať zo servera, zadajte tento príkaz:

```
psconf import  -S -k <názov súboru kľúča> -f <názov súboru>
```

| Ak chcete certifikát importovať z klienta, zadajte tento príkaz:

```
psconf import -C -k <názov súboru kľúča> -f <názov súboru>
```

| **Súvisiaci odkaz**:

| "Príkaz pscon" na strane 157

Nahlasovanie servera TNC

Server Trusted Network Connect (TNC) podporuje formát CSV aj textový výstupný formát pre svoje bežné zraniteľné miesta a expozície (CVE), IBM Security Advisory, politiky servera TNC, bezpečnostnú opravu klienta TNC a registrované servisné balíky a zostavy o dočasných opravách.

Zostava CVE zobrazí všetky bežné expozície a zraniteľné pre registrované servisné balíky. Ak chcete zobraziť výsledky tejto zostavy, zadajte nasledujúci príkaz:

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

Zostava IBM Security Advisory zibrazí známe bezpečnostné zraniteľné miesta na nainštalovanom softvér IBM. Ak chcete zobraziť výsledky tejto zostavy, zadajte nasledujúci príkaz:

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

Politiky servera TNC zobrazia bezpečnostné politiky, ktoré sú vynútené na serveri TNC. Ak chcete zobraziť výsledky tejto zostavy, zadajte nasledujúci príkaz:

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

Zostava o opravách klienta TNC zobrazí nainštalované a chýbajúce dočasné opravy pre klienta TNC. Ak chcete zobraziť výsledky tejto zostavy, zadajte nasledujúci príkaz:

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

Môžete tiež spustiť zostavu, ktorá vygeneruje zoznam registrovaných servisných balíkov a súvisiacich opráv APAR a dočasných opráv. Ak chcete zobraziť výsledky tejto zostavy, zadajte nasledujúci príkaz:

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

Ak chcete zobraziť zoznam zaregistrovaných balíkov s otvoreným zdrojovým kódom, zadajte nasledujúci príkaz:

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

Súvisiaci odkaz:

"Príkaz pscon" na strane 157

Riešenie problémov s funkciou Trusted Network Connect a správou opráv

Zistite možné príčiny zlyhania a kroky na riešenie problémov s TNC a systémom riadenia opráv.

Ak chcete riešiť problémy s TNC a systémom riadenia opráv, skontrolujte konfiguračné nastavenia, ktoré sú uvedené v nasledujúcej tabuľke.

Tabuľka 13. Riešenie problémov a konfiguračné nastavenia pre TNC a systémy riadenia opráv

Problém	Riešenie
Server TNC sa nespustí alebo neodpovedá	Vykonajte nasledujúci postup: 1. Určite, či je démon servera TNC spustený zadaním príkazu: `ps –eaf | grep tnccsd` 2. Ak nie je spustený, vymažte súbor /var/tnc/.tncsock. 3. Reštartujte server. Ak sa tým problém nevyrieši, skontrolujte v konfiguračnom súbore /etc/tnccs.conf položku component = SERVER na serveri TNC.

Tabuľka 13. Riešenie problémov a konfiguračné nastavenia pre TNC a systémy riadenia opráv (pokračovanie)

Problém	Riešenie
Server riadenia opráv NC sa nespustí alebo neodpovedá	• Určite, či je démon servera riadenia opráv TNC spustený zadaním nasledujúceho príkazu: `ps –eaf | grep tncpmd` • Skontrolujte v konfiguračnom súbore /etc/tnccs.conf položku component = TNCPM na serveri riadenia opráv TNC.
Klient TNC sa nespustí alebo neodpovedá	• Určite, či je démon klienta TNC spustený zadaním nasledujúceho príkazu: `ps –eaf | grep tnccsd` • Skontrolujte v konfiguračnom súbore /etc/tnccs.conf položku component = CLIENT na klientovi TNC.
Odkazovač TNC IP nie je spustený na systéme Virtual I/O Server (VIOS)	• Určite, či je démon odkazovača TNC IP spustený zadaním nasledujúceho príkazu: `ps –eaf | grep tnccsd` • Skontrolujte v konfiguračnom súbore /etc/tnccs.conf položku component = IPREF na systéme VIOS.
Nie je možné nakonfigurovať systém súčasne ako server aj klienta TNC.	Server a klient TNC nemôžu fungovať súčasne na tom istom systéme.
Démoni sú spustení ale overenie sa nevykoná	Nie je možné protokolovať správy pre démonov. Nastavte protokol level=info v súbore /etc/tnccs.conf. Môžete analyzovať správy protokolu.

PowerSC GUI (grafické užívateľské rozhranie)

Táto časť popisuje IBM PowerSC GUI (grafické užívateľské rozhranie), ako aj informácie o inštalácii, údržbe a používaní rozhrania.

IBM PowerSC GUI zvyšuje použiteľnosť produktu PowerSC Standard Edition tým, že poskytuje alternatívu voči interakcii prostredníctvom príkazového riadka a protokolových súborov. PowerSC GUI poskytuje centralizovanú riadiacu konzolu pre vizualizáciu koncových bodov a ich stavu, použitie, zrušenie použitia alebo kontrolu úrovní súladu s nariadeniami, pre vytváranie skupín systémov za účelom použitia akcií úrovne súladu s nariadeniami a pre zobrazenie a prispôsobovanie konfiguračných profilov súladu s nariadeniami.

PowerSC GUI zahŕňa aj FIM (File Integrity Monitoring). FIM obsahuje RTC (Real Time Compliance) a TE (Trusted Execution). Pomocou PowerSC GUI, môžete konfigurovať RTC a TE, a zobraziť udalosti v reálnom čase. PowerSC GUI poskytuje aj rozsiahle schopnosti pre tvorbu výkazov a úpravu profilov.

PowerSC GUI - základné pojmy

Skôr ako začnete používať produkt PowerSC GUI, mali by ste pochopiť základné koncepty týkajúce sa zabezpečenia a zisťovania koncových bodov.

PowerSC GUI - bezpečnosť

Softvér PowerSC GUI zaručuje bezpečnosť prostredníctvom obojsmernej komunikácie medzi serverom PowerSC GUI a agentmi servera PowerSC GUI cez protokol HTTPS na každom koncovom bode so systémom AIX.

Pri procese nadviazania komunikácie cez TLS sa využívajú certifikáty, ktoré sú k dispozícii na serveri PowerSC GUI aj pre agentov PowerSC GUI. Tento proces nadviazania komunikácie cez TLS podporuje jednotnú autentifikáciu v oboch smeroch, keďže komunikáciu môže iniciovať aj agent PowerSC GUI, aj server PowerSC GUI. Agent vytvorí jednorazovú značku, čo je náhodné číslo, ktoré sa pošle na server PowerSC GUI pri prvom pripojení. Server PowerSC GUI potom uvedie túto jednorazovú značku pri každom príkaze odoslanom tomuto agentovi. Táto jednorazová značka poskytuje ďalšiu úroveň potvrdzovania pre agenta koncového bodu, ktorý spúšťa príkaz pochádzajúci z autentického servera PowerSC GUI. Koncový bod musí zabezpečiť, že zdroj volania webovej služby bude dôveryhodný. Prvotné nadviazanie spojenia a jednorazová značka zabezpečujú dôveryhodnosť komunikácie.

Všetka komunikácia medzi agentmi PowerSC GUI a serverom PowerSC GUI je šifrovaná s použitím protokolov a množín šifier, ktoré sú v súlade s bezpečnostnými požiadavkami príslušných chránených systémov. Aktuálna úroveň protokolu TLS je 1.2. Server PowerSC GUI komunikuje so všetkými agentmi PowerSC GUI a všetkými užívateľmi servera PowerSC GUI. Preto musí mať server PowerSC GUI certifikát, ktorý bude dôveryhodný pre všetky pripojenia z webových prehliadačov užívateľov. Takými sú napríklad certifikáty pochádzajúce od známej certifikačnej autority, akou je napríklad spoločnosť Verisign, alebo interne dôveryhodná certifikačná autorita.

Počas inštalácie servera PowerSC GUI vytvorí samopodpísaný certifikát na vlastné účely. Tento certifikát sa môže používať neobmedzenú dobu, no je určený len na dočasné použitie a môže byť nahradený užívateľom poskytnutým, všeobecne známym certifikátom. Pri inštalácii servera PowerSC GUI sa vytvorí aj podpisujúci certifikát, ktorý slúži na podpísanie všetkých certifikátov koncových bodov.

Inštalačný proces automaticky vytvorí súbor s verejnými kľúčmi pre každý koncový bod. Tento súbor s verejnými kľúčmi je rovnaký pre každý koncový bod a musí byť skopírovaný zo servera PowerSC GUI na každý koncový bod. Táto kombinácia certifikátov na serveri PowerSC GUI a koncových bodoch zaručuje vysokú úroveň zabezpečenia komunikácie.

Väčšiu mieru kontroly nad bezpečnosťou ponúkajú skupiny UNIX. Každý užívateľ, či už ide o užívateľa LDAP alebo lokálneho užívateľa definovaného operačným systémom, musí byť členom určenej skupiny UNIX, aby sa mohol prihlásiť do systému PowerSC GUI. Administrátor môže nastaviť alebo zmeniť členstvo v skupinách pomocou príkazu **pscuiserverctl**.

Po prihlásení sa môže stať, že budete môcť len zobrazovať informácie. Pomocou funkcie užívateľských oprávnení môžete vykonávať akcie na koncových bodoch riadených na základe členstva v skupinách UNIX. Aby ste mohli vykonávať takéto akcie, musíte byť členom skupiny UNIX s oprávnením na správu koncového bodu. Bližšie informácie nájdete v téme Určenie skupín, ktoré budú mať prístup.

Predvolene môže každý užívateľ, ktorý je členom skupiny security, spravovať každý koncový bod, ktorý je viditeľný v rozhraní PowerSC GUI. Administrátor softvéru PowerSC môže obmedziť prístup užívateľov na úrovni jednotlivých koncových bodov pomocou príkazu **setGroups.sh**.

Existuje množstvo konfiguračných príkazov, ktoré môže používať iba užívateľ s administračnými oprávneniami. Tieto zahrňujú schopnosť zmeniť globálne nastavenia pošty alebo vytvoriť nový profil. Administračné oprávnenia nastavujú skupiny UNIX a môžu byť nakonfigurované prostredníctvom príkazu **pscuiserverctl**.

Načítanie obsahu koncového bodu na stránke súladu s nariadeniami

Server PowerSC GUI a agent PowerSC GUI komunikujú s koncovým bodom, aby zistili úroveň súladu s nariadeniami.

Po spustení sa agent nepravidelne pokúša nadviazať kontakt so serverom PowerSC GUI, až kým nie je spojenie úspešné. Po vytvorení spojenia sa jednorazovo vykoná bezpečné nadviazanie spojenia agent-server. Po prvom úspešnom bezpečnom nadviazaní spojenia od agenta na server si server vytvorí doménový prvok s jedinečným identifikátorom (UID), ktorý slúži ako interné zastúpenie koncového bodu, a toto UID postúpi naspäť koncovému bodu. UID je od tohto momentu súčasťou každej komunikácie zasielanej od agenta na server. Touto akciou sa dokončí proces zisťovania. Server PowerSC GUI a koncový bod môžu zabezpečene komunikovať v oboch smeroch.

Po dokončení úvodného nadviazania spojenia alebo po reštarte agenta PowerSC GUI sa agent PowerSC GUI pokúsi určiť aktuálny stav súladu s nariadeniami na koncovom bode a aktualizuje server PowerSC GUI. Informácie o existencii koncového bodu a aktuálne informácie o súlade s nariadeniami sa načítajú ako údaje na stránke o stave súlad s nariadeniami pre PowerSC GUI. Ak sa nepodarí rozpoznať žiadne informácie o stave súladu s nariadeniami, nebude táto položka k dispozícii na stránke stavu súladu s nariadeniami.

Server PowerSC GUI obsahuje zastúpenia všetkých koncových bodov, ktoré sú automaticky vytvorené v dôsledku úvodného spojenia a komunikácie medzi agentom a serverom. Ako agent koncového bodu sleduje zmeny v stave súladu s nariadeniami na koncovom bode, sú tieto zmeny postúpené na server a tam sa uchovávajú. Všetky užívateľské interakcie z PowerSC GUI s koncovým bodom sú vykonávane prostredníctvom servera PowerSC GUI. Nedochádza k žiadnej priamej interakcii medzi užívateľským rozhraním a koncovým bodom alebo agentom koncového bodu.

Inštalácia PowerSC GUI

Agenti PowerSC GUI a komponenty servera PowerSC GUI sa inštalujú počas inštalácie softvéru PowerSC Standard Edition. Každý z nich sa inštaluje zo sád súborov installp.

Agent PowerSC GUI

Agent PowerSC GUI sa inštaluje na každý koncový bod so systémom AIX. Agent PowerSC GUI sleduje aktivity na koncovom bode a poskytuje tieto informácie serveru PowerSC GUI.

Agent PowerSC GUI taktiež spúšťa príkazy, ktoré sa odošlú z rozhrania PowerSC GUI. Všetka komunikácia medzi agentmi PowerSC GUI a serverom PowerSC GUI je šifrovaná.

Príkaz installp nainštaluje základný produkt PowerSC Standard Edition a agenta PowerSC GUI. Sada súborov powerscStd.uiAgent.rteinstallp slúži na inštaláciu agenta PowerSC GUI. Nasledujúci príklad ilustruje použitie príkazu installp na každom koncovom bode:

Poznámka: V nasledujúcom príklade sa inštalačné obrazy rozbalia do adresára /tmp/inst.images/.

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

Server PowerSC GUI

Server PowerSC GUI môže bežať na ktoromkoľvek systéme AIX. Odporúča sa vytvoriť vyhradený logický oddiel AIX, na ktorom nainštalujete alebo spustíte server PowerSC GUI.

Príkaz **installp** nainštaluje jadro produktu PowerSC Standard Edition a server PowerSC GUI. Pri inštalácii servera PowerSC GUI je použitá sada súborov powerscStd.uiServer.rte **installp**. Nasledujúci príklad ukazuje príkaz **installp** spustený na koncovom bode:

Poznámka: Inštalačné obrazy v nasledujúcom príklade sú uložené v adresári /tmp/inst.images/.

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

Požiadavky PowerSC GUI

Zoznámte sa s hardvérovými a softvérovými požiadavkami produktu PowerSC GUI.

Hardvér

- Komponenty servera PowerSC GUI by mali byť inštalované na samostatnom logickom oddiele alebo VM spustenom na AIX 7.1 na jeho vyššej verzii.
- Komponenty agenta PowerSC GUI musia byť inštalované na každom koncovom bode AIX.

Softvér

- Server PowerSC GUI vyžaduje AIX 7.1 alebo vyššiu verziu.
- Server PowerSC GUI vyžaduje, aby bol spustený démon sendmail.
- Aby sa popisy pravidiel v profiloch PowerSC GUI zobrazovali správne aj keď sú uvedené v inom jazyku než angličtina, musí byť nainštalovaná sada súborov bos.loc.utf.<LANG>.

Distribúcia bezpečnostného certifikátu verejných kľúčov na koncové body

Správcovia systému musia nasadiť bezpečnostný certifikát verejných kľúčov na všetky koncové body.

Počas inštalácie sa vytvorí súbor s verejnými kľúčmi, ktorý môžu používať všetky koncové body. Názov tohto súboru je endpointTruststore.jks. Nachádza sa v adresári /etc/security/powersc/uiServer/.

Po inštalácii musíte súbor endpointtruststore.jks umiestniť na každý koncový bod, aby sa mohol agent PowerSC GUI na koncovom bode spojiť so serverom PowerSC GUI a iniciovať proces, ktorý na koncovom bode vytvorí sklad kľúčov.

Súbor s verejnými kľúčmi môžete distribuovať niektorým z nasledujúcich postupov:

- Manuálne skopírujte súbor endpointTruststore.jks na každý koncový bod.
- Ak vo vašom prostredí využívate PowerVC (alebo iný manažér virtualizácie), môžete súbor endpointTruststore.jks vložiť do obrazu PowerVC. Pri nasadení obrazu PowerVC na koncovom bode bude nasadený aj agent PowerSC GUI a súbor s verejnými kľúčmi.

Po nasadení súboru endpointTruststore.jks ktorýmkoľvek z týchto spôsobov a po spustení koncového bodu použije agent PowerSC GUI tento súbor s verejnými kľúčmi na určenie umiestnenia, na ktorom je spustený server PowerSC GUI. Agent PowerSC GUI potom odošle serveru PowerSC GUI správu s požiadavkou o zaradenie do zoznamu dostupných a monitorovaných koncových bodov.

Manuálne kopírovanie súboru s verejnými kľúčmi na koncové body

Správcovia systému musia manuálne skopírovať súbor s verejnými kľúčmi na každý existujúci koncový bod v prostredí.

Súbor s verejnými kľúčmi je nutné skopírovať aj na každý nový pridaný koncový bod.

Poznámka: Ak máte manažéra virtualizácie údajov, napríklad PowerVC, môžete súbor s verejnými kľúčmi skopírovať na nový koncový bod vytvorením obrazu, ktorý obsahuje tak agenta PowerSC GUI, ako aj súbor s verejnými kľúčmi. Pozrite si informácie v téme "Kopírovanie súboru s verejnými kľúčmi na koncové body pomocou manažéra virtualizácie".

1. Ak chcete skopírovať súbor s verejnými kľúčmi pre koncový bod (/etc/security/powersc/uiServer/endpointTruststore.jks) do súboru /etc/security/powersc/uiAgent/endpointTruststore.jks na každom koncovom bode, spustite nasledujúci príkaz **scp**:

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

2. Spustením nasledujúcich príkazov na koncovom bode reštartujete agentov koncových bodov po inštalácii bezpečnostného certifikátu:

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

3. Kroky 1 a 2 opakujte opakujte pre každý koncový bod a pre každý nový koncový bod (pokiaľ nemáte manažéra virtualizácie údajov).

Kopírovanie súboru s verejnými kľúčmi na koncové body pomocou manažéra virtualizácie

Správcovia systému môžu použiť manažéra virtualizácie, napríklad PowerVC, na skopírovanie súboru s verejnými kľúčmi na každý nový koncový bod pomocou obrazu, ktorý obsahuje agenta PowerSC a súbor s verejnými kľúčmi.

1. skopírujte súbor s verejnými kľúčmi koncového bodu (/etc/security/powersc/uiServer/endpointTruststore.jks) do obrazu PowerVC.
2. Nasaďte obraz PowerVC na každý nový koncový bod pridaný do vášho systému.

Nastavenie užívateľských kont

Každý užívateľ, či už ide o užívateľa LDAP alebo lokálneho užívateľa definovaného operačným systémom, musí byť členom bezpečnostnej skupiny, aby sa mohol prihlásiť do systému PowerSC GUI.

Administrátor môže zmeniť toto vyžadované členstvo v skupine pomocou príkazu **pscuiserverctl**. Po prihlásení do aplikáciePowerSC GUI môže užívateľ zobraziť stav koncových bodov iba vtedy, ak je ich užívateľské konto členom skupiny UNIX s oprávnením na správu tohto koncového bodu. Administrátor môže zmeniť nastavenia užívateľských kont pre jednotlivé úrovne koncových bodov pomocou príkazu **setGroups.sh**.

Zvážte nasledujúce faktory:

- Medzi koncovými bodmi a skupinami AIX existuje vzťahy typu many-to-many:
  - Jedna skupina AIX môže byť priradená k mnohým koncovým bodom.
  - Jeden koncový bod môže byť priradený k mnohým skupinám AIX.
- Po prihlásení užívateľa do aplikácie PowerSC GUI sa na základe členstva v skupine určí, či má užívateľ oprávnenie na spúšťanie príkazov pre konkrétne koncové body, alebo či má užívateľ oprávnenia len na zobrazenie stavu koncových bodov.
  - Aby mohol užívateľ spúšťať príkazy pre konkrétny koncový bod prostredníctvom aplikácie PowerSC GUI, tento užívateľ musí patriť do niektorej zo skupín súvisiacich s týmto koncovým bodom.
  - Členstvo užívateľa v skupine sa porovná s prvou množinou skupín priradených k jednotlivým koncovým bodom. Ak sa členstvo v skupine užívateľa zhoduje so skupinami priradenými k jednotlivým koncovým bodom, užívateľ

môže spúšťať rozličné príkazy, ako sú napríklad **Apply profiles**, **Undo** a **Check** pre daný koncový bod. Ak užívateľ nie je členom žiadnej skupiny súvisiacej s koncovým bodom, tento užívateľ môže len zobraziť stav koncového bodu.

V adresári /opt/powersc/uiServer/bin/ na serveri PowerSC GUI sú k dispozícii nasledujúce skripty prostredia shell.

Tabuľka 14. Skupinové skripty prostredia shell

Skript prostredia Shell	Popis
pscuiserverctl	Určuje prihlasovaciu skupinu AIX (UNIX), do ktorej musí užívateľ patriť, aby sa mohol prihlásiť do aplikácie PowerSC GUI. Užívateľ musí byť členom iba jednej z týchto skupín.
setGroups.sh	Určuje skupiny AIX, do ktorých musí užívateľ patriť, aby mohol spúšťať príkazy pre konkrétne koncové body.

Spustenie skriptov a príkazov pre nastavenie skupín

Správcovia systému musia najprv spustiť príkaz **pscuiserverctl** a skript **setGroups** a určiť, ktoré skupiny operačných systémov sa smú prihlasovať do PowerSC GUI, vykonávať správcovské funkcie a spúšťať príkazy na konkrétnych koncových bodoch.

1. Zmeňte adresár na serveri PowerSC GUI na /opt/powersc/uiServer/bin/.
2. Spustením nasledujúceho príkazu určíte skupinu AIX, ktorej musí byť užívateľ členom, aby sa mohol prihlásiť do PowerSC GUI. Vami zadaná skupina je zapísaná v súbore /etc/security/powersc/uiServer/uiServer.conf.

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

   Tip: Pred spustením tohto príkazu môžete pomocou príkazu **groups** *username* zobraziť skupiny, v ktorých je užívateľ členom.
3. Spustením nasledujúceho príkazu určíte skupiny UNIX, ktoré majú povolenie vykonávať administračné funkcie pomocou PowerSC GUI.

   ```
   pscuiserverctl set administratorGroupList unixgrpadmin1,unixgrpadmin2
   ```
4. Spustením nasledujúceho skriptu určíte skupiny AIX, v ktorých musí byť užívateľ členom, aby mohol spúšťať príkazy na konkrétnych koncových bodoch. Musíte zadať úplné názvy hostiteľov koncových bodov. Vami zadané skupiny sa zapíšu do súboru /etc/security/powersc/uiServer/groups.txt.

   ```
   ./setGroups.sh groupname "zoznam názvov hostiteľov koncových bodov oddelených čiarkou"
   ```

   Poznámka: Pri vyhľadávaní koncových bodov sú podporované niektoré zástupné znaky. Napríklad, nasledujúcou špecifikáciou môžete špecifikovať všetky koncové body, ktorých názov sa začína na "Boston_" alebo končí na ".rs.com":
   - ./setGroups.sh groupname "Boston_*"
   - ./setGroups.sh groupname "*.rs.com"

   Tip: Jediným podporovaným zástupným znakom v tomto príklade je hviezdička (*). Môžete ju použiť len na začiatku alebo na konci reťazca.

Používanie PowerSC GUI

Prostredníctvom PowerSC GUI môžete zobraziť koncové body zistené vo vašom systéme, vytvárať prispôsobené skupiny, vytvárať prispôsobené profily, kopírovať vlastné profily na koncové body a použiť profily. Môžete tiež overiť komunikáciu medzi koncovými bodmi a serverom PowerSC GUI a zastaviť komunikáciu medzi koncovými bodmi a serverom PowerSC GUI.

Hlavná stránka PowerSC GUI obsahuje nasledujúce časti:

- Časť **Groups**: uvádza zoznam skupín definovaných vo vašom prostredí. Skupiny sú kolekcie koncových bodov zoskupené podľa ich zhodnosti. Skupina **All systems** sa vytvára automaticky zisťovaním koncových bodov vo vašom prostredí. Môžete vytvárať prispôsobené skupiny. Môžete napríklad vytvoriť skupinu koncových bodov, ktorých zhodou je HIPPA.
- Stránka **Compliance** obsahuje tri časti:
  - Horný panel zobrazuje informácie o skupine, ktorú ste vybrali v časti **Groups**. Štatistické informácie obsahujú výsledky posledných úrovní použitých na koncových bodoch vo vybratej skupine. Za vybratú skupinu môžete zobraziť percento systémových postúpení a zlyhaní, celkový počet skontrolovaných pravidiel a zistiť, ktoré pravidlá boli neúspešné.
  - Stredný panel obsahuje lištu s úlohami, pomocou ktorej môžete vykonať akcie na jednom alebo na viacerých koncových bodoch. Môžete použiť, zrušiť použitie alebo skontrolovať úroveň súladu s nariadeniami.
  - Spodný panel zobrazuje tabuľku všetkých koncových bodov alebo skupinu koncových bodov, ktoré sú dostupné vo vašom systéme. V tabuľke sú uvedené nasledujúce informácie o každom koncovom bode:
    - názov systému,
    - typ pravidla súladu s nariadeniami,
    - čas a dátum použitia pravidla súladu s nariadeniami na koncovom bode,
    - čas a dátum kontroly úrovne súladu s nariadeniami na koncovom bode,
    - stav úrovne súladu s nariadeniami,
    - počet neúspešných pravidiel na koncovom bode,
    - počet pravidiel na koncovom bode, ktoré úspešne prešli kontrolou úrovne súladu s nariadeniami.
- Stránka **Security** obsahuje dve časti:
  - Horný panel zobrazuje v reálnom čase informácie o skupine koncových bodov, ktorú ste vybrali v časti **Groups**. Za vybratú skupinu môžete zobraziť počet udalostí RTC (Real time Compliance), celkový počet udalostí TE (Trusted Execution), percento koncových bodov, ktoré majú najaktuálnejšie opravy TNC, percento koncových bodov, ktoré majú nainštalovaný Trusted Boot, percento koncových bodov, ktoré majú nainštalovaný Trusted Firewall a percento koncových bodov, ktoré majú nainštalovaný Trusted Logging.
  - Horný panel zobrazuje tabuľku systémových koncových bodov v skupine. V tabuľke sú uvedené nasledujúce informácie o každom koncovom bode:
    - názov systémového koncového bodu,
    - indikátory udalostí integrity súboru,
    - stav aktivácie RTC,
    - stav aktivácie TE,
    - stav aktuálnosti opráv TNC.
- Stránka **Reports** obsahuje zostavy súladu s nariadeniami a integrity súborov. Obsahuje prehľadové aj podrobné zostavy.
- Stránka **Profile Editor** obsahuje tri časti:
  - Horný panel má rozbaľovaciu ponuku, v ktorej sú uvedené všetky zabudované a vlastné profily.
  - Stredný panel obsahuje lištu s úlohami, pomocou ktorej môžete odstrániť profily, vytvárať nové profily a kopírovať profily na koncové body, ktoré sú súčasťou skupiny.
  - Spodný panel zobrazuje tabuľku všetkých pravidiel zahrnutých vo vybratom profile. Každá položka obsahuje nasledujúce informácie:
    - názov pravidla súladu s nariadeniami,
    - typ pravidla súladu s nariadeniami,
    - popis pravidla.

Určenie jazyka PowerSC GUI

PowerSC GUI je možné interpretovať v rozličných jazykoch.

Ak chcete vybrať jazyk rozhrania PowerSC GUI, kliknite na ikonu **Languages and Settings** na paneli s ponukami na hlavnej stránke. V ponuke sa zobrazí aktuálne zvolený jazyk rozhrania. Ak chcete zmeniť jazyk, kliknite na priradenú ikonu. Vyberte jazyk vašej relácie v zozname dostupných jazykov.

Navigácia v PowerSC GUI

V PowerSC GUI môžete nastaviť a administrovať komunikáciu medzi koncovým bodom a serverom, usporiadať a zoskupiť koncové body, monitorovať a použiť zabudované a vlastné profily a úrovne súladu s nariadeniami, monitorovať a konfigurovať bezpečnosť koncových bodov a generovať a distribuovať zostavy podľa stanoveného plánu.

1. Otvorte PowerSC GUI. Zobrazí sa domovská stránka PowerSC GUI.
2. Ak chcete administrovať komunikáciu medzi koncovými bodmi a serverom, kliknite na ikonu **Languages and Settings** na paneli s ponukami na hlavnej stránke. Po kliknutí na ikonu **Endpoint Admin** môžete overiť alebo zastaviť komunikáciu medzi koncovými bodmi a serverom PowerSC GUI. Bližšie informácie nájdete v téme "Administrácia komunikácie medzi koncovými bodmi a serverom".
3. Kliknutím na horizontálnu elipsu na navigačnom paneli na stránkach Compliance alebo Security otvoríte Group Editor. V ňom môžete vytvárať vlastné skupiny koncových bodov. Bližšie informácie nájdete v téme "Vytváranie vlastných skupín" na strane 137.
4. Ak chcete vytvárať vlastné profily súladu s nariadeniami a kopírovať profily na koncové body, kliknite na kartu **Profile Editor**. Bližšie informácie nájdete v téme "Práca s profilmi súladu" na strane 138.
5. Ak chcete monitorovať a použiť zabudované a vlastné profily a úrovne súladu s nariadeniami, kliknite na kartu **Compliance**. Bližšie informácie nájdete v téme Použitie profilov a úrovní súladu s nariadeniami.
6. Ak chcete monitorovať a konfigurovať bezpečnosť koncových bodov, kliknite na kartu **Security**. Bližšie informácie nájdete v téme Monitorovanie bezpečnosti koncových bodov.
7. Ak chcete generovať a distribuovať zostavy na vyžiadanie alebo podľa stanoveného rozvrhu, kliknite na kartu **Reports**. Bližšie informácie nájdete v téme Práca so zostavami.

Administrácia komunikácie medzi koncovými bodmi a serverom

Na stránke **Endpoint Admin** môžete overiť alebo zastaviť komunikáciu medzi koncovými bodmi a serverom PowerSC GUI. Môžete tiež overiť a generovať požiadavky na sklad kľúčov.

Overenie komunikácie medzi koncovými bodmi a serverom

Môžete overiť komunikáciu medzi zistenými koncovými bodmi a serverom PowerSC GUI.

1. Kliknite na ikonu **Languages and Settings** na paneli s ponukami na hlavnej stránke. Kliknite na **Endpoint Admin**. Otvorí sa stránka Endpoint administration.
2. V časti **Groups** vyberte skupinu s koncovými bodmi, ktoré chcete overiť. Koncové body skupiny sa zobrazia v tabuľke koncových bodov.
3. V tabuľke súladu s nariadeniami sa zobrazia všetky systémové koncové body vybratej skupiny. Zobrazené koncové body môžete filtrovať zadaním textu v poli **Filtering by text**. Zadajte v poli text, podľa ktorého chcete filtrovať, a stlačte kláves Enter. Zoznam koncových bodov vo vybratej skupine sa dynamicky vyfiltruje tak, aby boli zobrazené len riadky, ktoré obsahujú vami zadaný text.
4. Ak chcete obnoviť zobrazené informácie o stave, kliknite na **Refresh Table**.
5. Označte začiarkavacie políčko každého koncového bodu, ktorý chcete overiť.
6. Kliknite na ikonu **Verify**.
7. V stĺpcoch **Verified** a **Connectivity Diagnosis** sa zobrazí potvrdzovacia správa o platnom pripojení.

Odstránenie koncových bodov z monitorovania PowerSC GUI

Každý koncový bod je neustále monitorovaný od momentu, keď bol zistený. Ak koncový bod odstránite z vášho prostredia, musíte ho odstrániť aj zo servera PowerSC GUI.

Ak chcete odstrániť koncové body z monitorovania v PowerSC GUI, postupujte nasledovne:

1. Kliknite na ikonu **Languages and Settings** na paneli s ponukami na hlavnej stránke. Kliknite na **Endpoint Admin**. Otvorí sa stránka Endpoint administration.
2. V časti **Groups** vyberte skupinu s koncovými bodmi, ktoré chcete odstrániť. Koncové body skupiny sa zobrazia v tabuľke koncových bodov.
3. V tabuľke súladu s nariadeniami sa zobrazia všetky systémové koncové body vybratej skupiny. Zobrazené koncové body môžete filtrovať zadaním textu v poli **Filtering by text**. Zadajte v poli text, podľa ktorého chcete filtrovať, a stlačte kláves Enter. Zoznam koncových bodov vo vybratej skupine sa dynamicky vyfiltruje tak, aby boli zobrazené len riadky, ktoré obsahujú vami zadaný text.
4. Ak chcete obnoviť zobrazené informácie o stave, kliknite na **Refresh Table**.
5. Označte začiarkavacie políčko každého koncového bodu, ktorý chcete prestať monitorovať.
6. Kliknite na ikonu **Delete**.
7. V stĺpcoch **Verified Timestamp** a **Connectivity Diagnosis** sa zobrazí potvrdzovacia správa o odstránení koncového bodu.

Požiadavky na overenie a generovanie skladu kľúčov

V prípade každého koncového bodu musíte overiť, či je požiadavka na sklad kľúčov platná a ak je platná, môžete vygenerovať sklad kľúčov pre daný koncový bod.

Po prvom spustení koncového bodu použije agent PowerSC GUI pomocou súboru s verejnými kľúčmi určí, kde je spustený server PowerSC GUI. Potom agent PowerSC GUI odošle na server PowerSC GUI správu s požiadavkou o zaradenie do zoznamu dostupných, monitorovaných koncových bodov.

Na stránke **Endpoint Administrator Keystore Requests** si môžete overiť, či je požiadavka na kľúčový sklad platná a ak je platná, môžete vygenerovať sklad kľúčov pre daný koncový bod.

1. Kliknite na ikonu **Languages and Settings** na paneli s ponukami na hlavnej stránke. Kliknite na **Endpoint Admin**. Otvorí sa administračná stránka **Endpoint - All Systems**.
2. V stĺpci **System Name** je uvedený každý známy koncový bod. Kliknutím na **Keystore Requests** overíte, či sú v spracovaní nejaké požiadavky na sklad kľúčov. Otvorí sa stránka **Endpoint Admin Keystore Requests**.
3. V stĺpci **Hostname** sú uvedené požiadavky na sklad kľúčov za všetky nové alebo pridané servery. Po potvrdení, že chcete rozšíriť sklad kľúčov na konkrétny koncový bod, označte jeho začiarkavacie políčko a kliknite na **Verify**.
4. Overenie vykoná PowerVC. Zadajte v okne **PowerVC Credentials required** svoj identifikátor a heslo. Kliknite na **OK**. Ak nemáte PowerVC, vynechajte tento krok a prejdite na ďalší.

   Poznámka: Overenie je proces, ktorý pomocou rozhraní Openstack API skontroluje, či má PowerVC povedomie o novo deklarovaných koncových bodoch. Ak sa v užívateľskom prostredí nenachádza PowerVC alebo ak nebol powervcKeystoneUrl správne nakonfigurovaný pomocou pscuiserverctl, nebude môcť PowerSC overiť koncový bod.
5. Po overení sa v stĺpci **Hostname** zobrazí správa vo forme plávajúceho text. Táto správa potvrdzuje, či PowerVC rozpoznáva nový koncový bod. Na základe informácií v správe sa môžete rozhodnúť, či vygenerujete sklad kľúčov.
6. Ak chcete generovať sklad kľúčov, kliknite na **Generate Keystore**. Počas generovania skladu kľúčov v tabuľke bliká riadok koncového bodu, pre ktorý je sklad generovaný. Po dokončení sa hodnota v stĺpci **Keystore generated** zmení z **no** na **yes**.

   Poznámka: Ak ste koncový bod neoverili pomocou PowerVC, zobrazí sa správa so žiadosťou o potvrdenie, či chcete pokračovať. Ak rozpoznávate tento koncový bod a chcete generovať sklad kľúčov, kliknite na **Proceed**.

   Môže trvať niekoľko minút, kým agent PowerSC zistí, že bol sklad kľúčov vygenerovaný. Keď agent nainštaluje sklad kľúčov, bude koncový bod uvedený ako plne spravovaný koncový bod na stránkach **Endpoint Admin - all systems**, **Compliance**, **Security** a **Reports** v PowerSC GUI.
7. Ak nechcete generovať sklad kľúčov pre daný koncový bod, môžete odstrániť požiadavku. Označte začiarkavacie políčko koncového bodu, ktorý chcete odstrániť a kliknite na ikonu **Delete**.

8. V tabuľke koncových bodov sa zobrazia všetky koncové body, ktoré čakajú na overenie skladu kľúčov. Zobrazené koncové body môžete filtrovať zadaním textu v poli **Filtering by text**. Zadajte v poli text, podľa ktorého chcete filtrovať, a stlačte kláves **Enter**. Zoznam koncových bodov vo vybratej skupine sa dynamicky vyfiltruje tak, aby boli zobrazené len riadky, ktoré obsahujú vami zadaný text.
9. Ak chcete obnoviť zobrazené informácie o stave, kliknite na **Refresh Table**.

Usporiadanie a zoskupenie koncových bodov

Správcovia systému môžu koncové body usporiadať a zoskupiť podľa niektorej ich spoločnej vlastnosti. Je možné definovať vlastné skupiny, ktoré môžu obsahovať explicitne vybraté množiny koncových bodov, ktoré sú spravované prostredníctvom PowerSC GUI.

Napríklad, ak máte 3 alebo 4 prostredia, možno budete chcieť vytvoriť skupiny, ktoré obsahujú produkčné koncové body, testovacie koncové body a koncové body zabezpečenia kvality.

Predvolená skupina s názvom **All Systems** je vytvorená počas inštalácie. Táto skupina zahŕňa všetky koncové body, ktoré boli zistené vo vašom prostredí.

Vytváranie vlastných skupín

Môžete vytvoriť vlastnú skupinu s explicitne vybratým a vymenovaným zoznamom koncových bodov.

1. V časti **Groups** vyberte **Create New Group**. Otvorí sa panel **Creating New Group**. Ak potrebujete rozvinúť časť **Groups**, kliknite na horizontálnu elipsu na ľavom paneli na hlavnej stránke rozhrania.
2. Zadajte jedinečný názov novej skupiny a stlačte kláves Enter. Nová skupina sa zobrazí časti **Groups**.
3. Pridajte systémy, ktoré chcete začleniť do tejto skupiny. V zozname všetkých dostupných systémov koncových bodov **All Systems** vyberte systémy, ktoré chcete začleniť do skupiny. Kliknutím na šípku doprava presuniete všetky vybraté systémy do skupiny. Ak chcete zo skupiny odstrániť niektoré systémy koncových bodov, zvýraznite ich v zozname novej skupiny a kliknite na šípku doľava.
4. Po pridaní alebo odstránení členov skupiny uložte vykonané zmeny kliknutím na ikonu **Save** na paneli s ponukami v obsahovom paneli.
5. Kliknutím na horizontálnu elipsu sa vrátite do časti **Groups**. Zobrazí sa nový zoznam skupín.

Pridanie alebo odstránenie systémov priradených existujúcej skupine

Môžete pridať alebo odstrániť koncové body, ktoré sú priradené existujúcej skupine.

1. Kliknite v časti **Groups** na elipsu napravo od skupiny, do ktorej chcete pridať alebo z ktorej chcete odstrániť systém koncového bodu. Ak potrebujete rozvinúť časť **Groups**, kliknite na horizontálnu elipsu na ľavom paneli na hlavnej stránke rozhrania.
2. Kliknite na **Edit Group**.
3. Ak chcete do skupiny pridať systém koncového bodu, vyberte daný systém v zozname **All Systems** a kliknite na šípku doprava. Pridaný systém pribudne v zozname ***GroupName***.
4. Ak chcete odstrániť niektorý koncový bod, vyberte daný systém v zozname **Group Systems** a kliknite na šípku doľava. Odstránený systém zmizne zo zoznamu ***GroupName***.
5. Kliknite na ikonu **Save group changes** a uložte vykonané zmeny.
6. Ak chcete odstrániť niektorý systém zo skupiny, označte ho a kliknite na šípku doľava.
7. Ak chcete zrušiť svoje zmeny, kliknite na **Cancel group changes**
8. Kliknutím na elipsu **Groups** sa vrátite do časti **Groups**.

Odstránenie skupiny

Môžete odstrániť skupiny, ktoré už nie sú použiteľné.

1. Kliknite v časti **Groups** na elipsu napravo od skupiny, ktorú chcete klonovať. Ak potrebujete rozvinúť časť **Groups**, kliknite na horizontálnu elipsu na navigačnom paneli na hlavnej stránke rozhrania.

2. Kliknite na **Delete Group**. Skupina sa odstráni a zmizne zo zoznamu skupín v časti **Groups**.

Premenovanie skupiny

Môžete zmeniť názov skupiny koncových bodov.

1. Kliknite v časti **Groups** na elipsu napravo od skupiny, ktorú chcete premenovať. Ak potrebujete rozvinúť časť **Groups**, kliknite na horizontálnu elipsu na navigačnom paneli na hlavnej stránke rozhrania.
2. Kliknite na **Rename Group**. Zadajte nový názov skupiny v poli **Group name**.

Klonovanie skupiny

Klonovaním skupiny môžete vytvoriť jej duplikát s rovnakými koncovými bodmi a s novým názvom.

1. Kliknite v časti **Groups** na elipsu napravo od skupiny, ktorú chcete klonovať. Ak potrebujete rozvinúť časť **Groups**, kliknite na horizontálnu elipsu na navigačnom paneli na hlavnej stránke rozhrania.
2. Kliknite na **Clone Group**. Skupina sa skopíruje s novým názvom.

Práca s profilmi súladu

Pomocou editora profilov v aplikácii PowerSC GUI môžete zobraziť vstavané profily súladu, vytvoriť si svoje vlastné profily a skopírovať profily do koncových bodov.

Produkt PowerSC Standard Edition sa poskytuje s množinou vstavaných profilov, pomocou ktorých môžete nakonfigurovať svoje systémové koncové body, aby každý z nich vyhovoval nasledujúcim bezpečnostným štandardom:

- súlad s požiadavkami normy Payment Card Industry - Data Security Standard (PCI)
- súlad s požiadavkami normy Sarbanes-Oxley Act a COBIT (SOX-COBIT)
- súlad s požiadavkami normy STIG Ministerstva obrany USA
- súlad s požiadavkami normy Health Insurance Portability and Accountability Act (HIPAA)
- súlad s požiadavkami normy North American Electric Reliability Corporation (NERC)

Bližšie informácie o vstavaných profiloch nájdete v téme “Koncepty automatizácie bezpečnosti a súladu s nariadeniami” na strane 9.

Každý vstavaný profil obsahuje pravidlá, ktoré sa musia uplatniť na koncovom bode, aby boli splnené bezpečnostné požiadavky. Ak chcete uplatniť podmnožinu alebo inú kombináciu týchto pravidiel alebo ak si chcete prispôsobiť úrovne súladu, môžete si vytvoriť svoj vlastný profil.

Vo väčšine prípadov správcovia zvyčajne upravujú súbory s pravidlami súladu s cieľom odstrániť problémové pravidlá. Po dokončení kontrol kompatibility sa súbory s pravidlami súladu považujú za stabilné a nasadia sa na produkčné servery.

Produkt PowerSC GUI umožňuje vytváranie vlastných profilov skombinovaním pravidiel zo vstavaných profilov (alebo vlastných profilov).

Zobrazenie profilov súladu s nariadeniami

Môžete zobraziť pravidlá, ktoré sú zahrnuté v zabudovaných alebo vo vlastných profiloch.

1. Vyberte na hlavnej stránke kartu **Profile Editor**. Otvorí sa stránka **Profile Editor**.
2. Kliknite na šípku nadol a otvorte zoznam profilov. V rozbaľovacej ponuke sú uvedené dostupné profily **Built-in Profiles** a **Custom Profiles**.
3. Vyberte profil, ktorý chcete zobraziť. Zobrazí sa názov, typ a popis každého pravidla v profile. Bližšie informácie o pravidlách nájdete v téme “Koncepty automatizácie bezpečnosti a súladu s nariadeniami” na strane 9.
4. Všetky pravidlá vybratého profilu sa zobrazia v tabuľke profilov. Profily môžete filtrovať pomocou poľa **Filtering by text**. Zadajte v poli text, podľa ktorého chcete filtrovať. Zoznam pravidiel vybratého profilu sa obnoví.

Vytvorenie vlastného profilu

Môžete vytvoriť nový profil založený na existujúcom profile a potom ho prispôsobiť tak, aby obsahoval len konkrétnu množinu pravidiel.

1. Vyberte na hlavnej stránke kartu **Profile Editor**. Otvorí sa stránka **Profile Editor**.
2. Kliknite na šípku nadol a otvorte zoznam profilov. V rozbaľovacej ponuke sú uvedené dostupné profily **Built-in Profiles** a **Custom Profiles**.
3. Vyberte profil, na základe ktorého má byť vytvorený váš nový profil.
4. Kliknite na ikonu **Create New Profile**. Otvorí sa okno New Profile Name and Type.
5. V poli **Profile Name** zadajte názov nového profilu.
6. Zadajte typ v poli **Profile Type**. Vami zadaný typ zvyčajne určuje typ zabudovanej politiky, na ktorej je nový profil založený, a tiež jedinečný identifikátor. Napríklad PCIxx, SOX-COBITxy, DoDxyz, HIPAAwxyz alebo NERCabc.
7. Kliknite na **Confirm**.
8. Ak chcete do vlastného profilu pridať niektoré pravidlo, vyberte toto pravidlo v pôvodnom profile, z ktorého vlastný profil vytvárate, a potom kliknite na šípku doprava. Vybraté pravidlo bude pridané pridá do nového profilu. Tento krok opakujte pre každé ďalšie pravidlo, ktoré chcete pridať.
9. Ak chcete niektoré pravidlo odstrániť z vlastného profilu, vyberte toto pravidlo vo vlastnom profile a kliknite na šípku doľava. Vybraté pravidlo bude odstránené z nového vlastného profilu. Tento krok opakujte pre každé ďalšie pravidlo, ktoré chcete odstrániť.
10. Keď dokončíte pridávanie pravidiel, kliknite na **Save**.

Kopírovanie profilov na členy skupiny

Vlastné profily môžete kopírovať na skupinu koncových bodov. Po skopírovaní vlastného profilu na iný koncový bod je možné ho na tomto koncovom bode použiť. Tiež je možné vykonať kontrolu, ktorá overí, či použitie profilu na koncovom bode spôsobí chyby.

1. Vyberte na hlavnej stránke kartu **Profile Editor**. Otvorí sa stránka **Profile Editor**.
2. Kliknite na šípku nadol a otvorte zoznam profilov. V rozbaľovacej ponuke sú uvedené dostupné profily **Built-in Profiles** a **Custom Profiles**.
3. Vyberte profil, ktorý chcete skopírovať na členy skupiny.
4. Kliknite na ikonu **Copy Profile to Group Members**. Otvorí sa okno **Copy *profilename* to** .
5. V zozname sú uvedené všetky skupiny, ktoré ste vytvorili pre vašu organizáciu, a vedľa každej je aj príslušné začiarkavacie políčko. Označte začiarkavacie políčko každej skupiny, do ktorej chcete skopírovať vybratý profil.
6. Kliknite na **Copy**.
7. Ak chcete profil použiť alebo skontrolovať, vráťte sa na stránku **Compliance** kliknutím na kartu **Compliance**.

Odstránenie vlastného profilu

Môžete odstrániť vlastné profily.

1. Vyberte na hlavnej stránke kartu **Profile Editor**. Otvorí sa stránka **Profile Editor**.
2. Kliknite na šípku nadol a otvorte zoznam profilov. V rozbaľovacej ponuke sú uvedené dostupné profily **Built-in Profiles** a **Custom Profiles**.
3. Rozviňte zoznam **Custom Profiles**.
4. Vyberte profil, ktorý chcete odstrániť.
5. Kliknite na ikonu **Delete Profile**. Vami vybratý vlastný profil sa odstráni.

Administrácia profilov a úrovní súladu s nariadeniami

Správcovia systému môžu použiť, skontrolovať alebo zrušiť použitie zabudovaných a vlastných úrovní a profilov súladu s nariadeniami na viacerých koncových bodov.

V nasledujúcej tabuľke sú uvedené vopred definované profily a úrovne súladu s nariadeniami, ktoré podporuje PowerSC Standard Edition.

Tabuľka 15. Vopred definované profily a úrovne súladu s nariadeniami, ktoré podporuje PowerSC Standard Edition

Profily	Úrovne
Database	nízka
DoD	stredná
DoD_to_AIXDefault	vysoká
DoDv2	predvolená
DoDv2_to_AIXDefault	
HIPAA	
NERC	
NERC_to_AIXDefault	
NERCv5	
NERCv5_to_AIXDefault	
PCI	
PCI_to_AIXDefault	
PCIv3	
PCIv3_to_AIXDefault	
SOX-COBIT	

Na stránke **Compliance** v PowerSC GUI môžete vykonať nasledujúce úlohy:

- Vybrať a použiť definovaný profil alebo úroveň na jednom alebo viacerých koncových bodoch.
- Spustiť alebo zrušiť operáciu na jednom alebo viacerých koncových bodoch.
- Skontrolovať definovaný profil alebo úroveň voči aktuálnemu stavu na jednom alebo viacerých koncových bodoch. Operácia kontroly nemá za následok žiadne zmeny na koncovom bode, ale nastaví hodnotu **Checked Timestamp** tak, aby uvádzala, kedy bola kontrola naposledy vykonaná.

Použitie profilov a úrovní súladu s nariadeniami

Profil alebo úroveň súladu s nariadeniami môžete použiť na jednom alebo viacerých koncových bodoch vo vybratej skupine.

1. Vyberte na hlavnej stránke kartu **Compliance**. Otvorí sa stránka **Compliance**.
2. V časti **Groups** vyberte skupinu, ktorá obsahuje koncové body, na ktoré chcete použiť profily a úrovne súladu s nariadeniami.
3. V tabuľke súladu s nariadeniami sa zobrazia všetky systémové koncové body vybratej skupiny. Zobrazené koncové body môžete filtrovať zadaním textu v poli **Filtering by text**. Zadajte v poli text, podľa ktorého chcete filtrovať, a stlačte kláves Enter. Zoznam koncových bodov vo vybratej skupine sa dynamicky vyfiltruje tak, aby boli zobrazené len riadky, ktoré obsahujú vami zadaný text.
4. Ak chcete obnoviť zobrazené informácie o stave, kliknite na **Refresh Table**. Ak chcete nastaviť, ako často sa má tabuľka obnovovať automaticky, kliknite na **Refresh Interval**.
5. V stĺpci **Compliance Rule Type** môžete vidieť úrovne a profily, ktoré boli skopírované na súvisiaci koncový bod. Vyberte úroveň alebo profil, ktorý chcete použiť na koncovom bode. Označte súvisiace začiarkavacie políčko.
6. Krok 5 opakujte na každom koncovom bode v skupine, na ktorom chcete použiť profily a úrovne súladu s nariadeniami.
7. Kliknite na ikonu **Použiť profily**.
8. Vybraté profily a úrovne súladu s nariadeniami budú použité na každom z vybratých koncových bodov. Ak niektoré z pravidiel nie je možné použiť, považuje sa pravidlo za neúspešné. Ak je niektoré z pravidiel neúspešné, je koncový bod označený červeným pásom a v stĺpci **#Failed Rules** sa zobrazí text **Failed**.

9. V stĺpci **#Failed Rules** môžete za každý koncový bod vidieť, prečo bolo pravidlo neúspešné. Použité pravidlá môžete prispôsobovať vytvorením alebo úpravou vlastného profilu.

Zrušenie použitých úrovní súladu s nariadeniami

Môžete zrušiť použitie úrovne alebo profilu súladu s nariadeniami, ktoré boli použité na jednom alebo viacerých koncových bodov vo vybratej skupine.

Ak chcete zrušiť použitie úrovní súladu s nariadeniami, vykonajte nasledujúce kroky:

1. Vyberte na hlavnej stránke kartu **Compliance**. Otvorí sa stránka **Compliance**.
2. V časti **Groups** vyberte skupinu, ktorá obsahuje koncové body, na ktorých chcete zrušiť použitie úrovne alebo profilu súladu s nariadeniami.
3. V tabuľke súladu s nariadeniami sa zobrazia všetky koncové vo body vybratej skupine. Zobrazené koncové body môžete filtrovať zadaním textu v políčku **Filtering by text**. Zadajte v políčku text, podľa ktorého chcete filtrovať, a stlačte kláves Enter. Zoznam koncových bodov vo vybratej skupine sa dynamicky vyfiltruje tak, aby boli zobrazené len riadky, ktoré obsahujú vami zadaný text.
4. Ak chcete obnoviť zobrazené informácie o stave, kliknite na **Refresh Table**. Ak chcete nastaviť, ako často sa má tabuľka obnovovať automaticky, kliknite na **Refresh Interval**.
5. Ako zrušíte úroveň alebo profile, ktoré boli použité na koncovom bode:
   a. Označte začiarkavacie políčko kontrolného bodu.
   b. Kliknite na ikonu **Undo**.

Kontrola ostatného použitého profilu a úrovne súladu s nariadeniami

Môžete skontrolovať, aká ostatná úroveň alebo profil súladu s nariadeniami boli použité na jednom alebo viacerých koncových bodov vo vybratej skupine.

1. Vyberte na hlavnej stránke kartu **Compliance**. Otvorí sa stránka **Compliance**.
2. V časti **Groups** vyberte skupinu, ktorá obsahuje koncové body, na ktorých chcete skontrolovať profily a úrovne súladu s nariadeniami.
3. V tabuľke súladu s nariadeniami sa zobrazia všetky koncové body vo vybratej skupine. Zobrazené koncové body môžete filtrovať zadaním textu v poli **Filtering by text**. Zadajte v poli text, podľa ktorého chcete filtrovať, a stlačte kláves Enter. Zoznam koncových bodov vo vybratej skupine sa dynamicky vyfiltruje tak, aby boli zobrazené len riadky, ktoré obsahujú vami zadaný text.
4. Ak chcete obnoviť zobrazené informácie o stave, kliknite na **Refresh Table**. Ak chcete nastaviť, ako často sa má tabuľka obnovovať automaticky, kliknite na **Refresh Interval**.
5. Označte súvisiace začiarkavacie políčka vedľa systémového názvu koncového bodu, na ktorom chcete skontrolovať ostatný použitý profil alebo úroveň.
6. Krok 5 na strane 140 opakujte na každom koncovom bode, na ktorom chcete skontrolujte profily a úrovne súladu s nariadeniami.
7. Kliknite na ikonu **Skontrolovať**.
8. Na kontrolnom bode prebehne kontrola, či je možné použiť pravidlá, ktoré sú v profile súladu s nariadeniami alebo v úrovni súladu s nariadeniami. Koncové body nie sú aktualizované. Ak niektoré z pravidiel nie je možné použiť, je ich použitie považované za neúspešné. Ak niektoré pravidlo zlyhá, označí sa koncový bod červeným príznakom a v stĺpci **#Failed Rules** sa zobrazí text **Failed**.
9. V zozname **#Failed Rules** môžete pre každý označený koncový bod zobraziť správu, ktorá uvádza, prečo bolo pravidlo neúspešné. Použité pravidlá môžete prispôsobovať vytvorením vlastného profilu.

Kontrola zatiaľ nepoužitého profilu alebo úrovne súladu s nariadeniami

Môžete skontrolovať úroveň alebo profil súladu s nariadeniami, ktoré zatiaľ neboli použité na jednom alebo viacerých koncových bodov vo vybratej skupine.

1. Vyberte na hlavnej stránke kartu **Compliance**. Otvorí sa stránka **Compliance**.

2. V časti **Groups** vyberte skupinu, ktorá obsahuje koncové body, pre ktoré chcete skontrolovať účinok úrovne alebo profilu súladu s nariadeniami.
3. V tabuľke súladu s nariadeniami sa zobrazia všetky koncové body vo vybratej skupine. Zobrazené koncové body môžete filtrovať zadaním textu v políčku **Filtering by text**. Zadajte v políčku text, podľa ktorého chcete filtrovať, a stlačte kláves Enter. Zoznam koncových bodov vo vybratej skupine sa dynamicky vyfiltruje tak, aby boli zobrazené len riadky, ktoré obsahujú vami zadaný text.
4. Ak chcete obnoviť zobrazené informácie o stave, kliknite na **Refresh Table**. Ak chcete nastaviť, ako často sa má tabuľka obnovovať automaticky, kliknite na **Refresh Interval**.
5. Označte súvisiace začiarkavacie políčka vedľa systémového názvu koncového bodu, na ktorom chcete skontrolovať ostatný použitý profil alebo úroveň. Môžete vybrať viacero jeden koncových bodov.
6. Otvorte rozbaľovací zoznam **Last Checked Type**. Vyberte jednu z nasledujúcich možností:
   - **All available levels** zobrazí zoznam všetkých dostupných úrovní, ktoré môžete skontrolovať voči koncovému bodu.
   - **All available profiles** zobrazí zoznam všetkých dostupných profilov, ktoré môžete skontrolovať voči koncovému bodu.
7. Vyberte úroveň alebo profil, ktoré chcete skontrolovať voči kontrolnému bodu.
8. Kliknite na ikonu **Check**. Vrátené výsledky kontroly sa zobrazia pod koncovým bodom.

Odoslanie e-mailového oznámenia, keď dôjde k udalosti súladu s nariadeniami

Zo stránky Compliance môžete jednému alebo viacerým príjemcom odoslať e-mailové oznámenie, keď dôjde k udalosti súladu s nariadeniami.

1. Vyberte na hlavnej stránke kartu **Compliance**. Otvorí sa stránka **Compliance**.
2. Kliknite na ikonu **Email Settings** v pravom hornom rohu panela s ponukami. Otvorí sa okno **Email Settings**.
3. Označte začiarkavacie políčko **Send me emails**.
4. V textovom poli **Addresses (comma separated)** zadajte e-mailové adresy príjemcov a jednotlivé adresy oddeľujte čiarkami.

Monitorovanie bezpečnosti koncových bodov

Na stránke **Security** môžete monitorovať bezpečnosť koncových bodov v reálnom čase.

Na stránke Security je zobrazený stav koncových bodov, ktoré monitorujú RTC (Real Time Compliance) a TE (Trusted Execution).

Tak RTC, subkomponent PowerSC, ako aj TE, komponent AIX, predstavujú FIM (File Integrity Monitoring). FIM monitoruje zmeny dôležitých súborov a zabezpečuje, aby boli autorizované udalosti s dopadom na tieto súbory. Udalosti, ktoré by mohli mať dopad na bezpečnosť zahŕňajú neočakávanú zmenu povolení k súboru, aktualizáciu obsahu súboru alebo neplánovanú inštaláciu aplikácie. Tieto udalosti potrebujete identifikovať, aby ste zabezpečili dôležité súbory a aplikácie.

Stránka **Security** obsahuje monitorovanie PowerSC GUI v reálnom čase. Zobrazuje udalosti generované pri k zmene súborov, ktoré monitoruje RTC alebo TE. Tieto udalosti obsahujú podrobnosti o tom, kedy došlo k zmene obsahu súboru, kedy bol uskutočnený prístup ku koncovému bodu alebo kedy došlo k zmene konfigurácie.

Na stránke **Security** môžete vykonať nasledujúce úlohy:

- v reálnom čase zobraziť informácie o monitorovaní RTC a TE,
- konfigurovať RTC a TE pre všetky koncové body,
- zobraziť stav ďalších produktov PowerSC na koncových bodoch,
- vypnúť a zapnúť TE.

Konfigurácia produktu Real Time Compliance (RTC)

Na stránke **Security** môžete konfigurovať produkt Real Time Compliance (RTC) pre konkrétny koncový bod alebo pre skupinu koncových bodov.

1. Kliknite na elipsu napravo od koncového bodu, pre ktorý chcete upraviť konfiguráciu RTC.
2. Kliknite na **Configure RTC**. Otvorí sa okno RTC Policies Configuration.
3. Všetky dostupné konfiguračné voľby sú uvedené aj s vysvetleniami. Ak chcete zmeniť niektoré konfiguračné voľby RTC, označte alebo zrušte označenie začiarkavacích políčok zobrazených naľavo od príslušných volieb. V niektorých prípadoch sú zmeny volieb implementované až po reštarte servera.
4. Kliknite na **Save**.

Obnovenie starších konfiguračných volieb RTC (Real Time Compliance)

Môžete obnoviť staršiu konfiguráciu RTC.

1. Kliknite na tri bodky vedľa koncového bodu, pre ktorý chcete obnoviť staršiu verziu konfiguračných nastavení RTC.
2. Kliknite na položku **Rollback RTC**. Zobrazia sa časové značky pre všetky verzie konfigurácie RTC.
3. Kliknite na časovú značku verzie konfigurácie, ktorú chcete obnoviť. Obnovia sa nastavenia konfigurácie RTC z daného času.

Kopírovanie konfiguračných volieb súladu s nariadeniami v reálnom čase (RTC) na iné skupiny

Konfiguračné voľby RTC môžete skopírovať na inú skupinu koncových bodov alebo na špecifickú množinu koncových bodov.

1. Kliknite na elipsu napravo od koncového bodu, ktorého konfiguračné voľby chcete skopírovať na inú skupinu koncových bodov alebo na špecifickú množinu koncových bodov.
2. Kliknite na **Copy RTC Configuration**. Zobrazia sa všetky skupiny koncových bodov, vrátane skupiny **All Systems**.
3. Jedným z nasledujúcich postupov vyberte skupinu alebo konkrétne koncové body:
   - V zozname dostupných skupín označte začiarkavacie políčko niektorej skupiny koncových bodov. Konfiguračné voľby sa skopírujú na všetky koncové body v tejto skupine.
   - Šípkou doprava rozviňte skupinu a zobrazte zoznam všetkých koncových bodov, ktoré sa v nej nachádzajú. Označte začiarkavacie políčko každého koncového bodu v skupine, na ktorý chcete skopírovať konfiguračné voľby.
   - Rozviňte zoznam koncových bodov v skupine **All Systems**. Označte začiarkavacie políčko každého koncového bodu v skupine, na ktorý chcete skopírovať konfiguračné voľby.
4. Kliknite na **OK**. Konfiguračné voľby sa skopírujú na vybratú skupinu alebo na vybraté koncové body.

Úprava zoznamu súborov Real Time Compliance (RTC)

Môžete zobraziť a upraviť voľby monitorovania RTC pre každý súbor na koncovom bode.

1. Kliknite na elipsu napravo od koncového bodu, ktorý je hostiteľom súborov, pre ktoré chcete zobraziť a upraviť voľby monitorovania RTC.
2. Kliknite na **Edit RTC File List**. Otvorí sa stránka **RTC File List Configuration** so zoznamom všetkých adresárov a súborov na tomto koncovom bode. Značka začiarknutia na ikone priečinka pre konkrétny adresár naznačuje, že minimálne jeden z jeho súborov je monitorovaný.
3. Ak sa súbor, ktorého voľby chcete zobraziť alebo upraviť, nachádza v niektorom adresári, zobrazte dvojitým kliknutím na adresár zoznam jeho súborov. V zozname sú uvedené všetky súbory z daného adresára.
4. V stĺpcoch **Content** a **Attributes** sú uvedené voľby monitorovania pre každý súbor na koncovom bode. Ak sú na niektorom súbore monitorované zmeny obsahu, má označené začiarkavacie políčko v stĺpci **Content**. Ak sú na

niektorom súbore monitorované zmeny atribútov, má označené začiarkavacie políčko v stĺpci **Attributes**. Ak chcete upraviť voľby monitorovania, označte alebo zrušte označenie začiarkavacích políčok jedného alebo viacerých súborov na koncovom bode.

5. Kliknite na **Save**.

Obnovenie starších konfiguračných volieb monitorovania súborov RTC (Real Time Compliance)

Môžete obnoviť staršiu verziu súborov monitorovaných funkciou RTC.

1. Kliknite na tri bodky vedľa koncového bodu, pre ktorý chcete obnoviť staršiu verziu konfiguračných nastavení monitorovania súborov RTC.
2. Kliknite na položku **Rollback RTC File List**. Zobrazia sa časové značky pre všetky verzie konfigurácie monitorovaných súborov.
3. Kliknite na časovú značku verzie konfigurácie monitorovania, ktorú chcete obnoviť. Obnovia sa nastavenia konfigurácie z daného času.

Kopírovanie volieb monitorovania zoznamu súborov Real Time Compliance (RTC) na iné skupiny

Voľby monitorovania súborov RTC môžete kopírovať na ďalšie skupiny koncových bodov alebo na konkrétnu množinu koncových bodov.

1. Kliknite na elipsu napravo od koncového bodu, ktorého voľby monitorovania súborov chcete skopírovať na inú skupinu koncových bodov alebo na špecifickú množinu koncových bodov.
2. Kliknite na **Copy RTC File List**. Zobrazia sa všetky skupiny koncových bodov, vrátane skupiny **All Systems**.
3. Jedným z nasledujúcich postupov vyberte skupinu alebo konkrétne koncové body:
   - V zozname dostupných skupín označte začiarkavacie políčko niektorej skupiny koncových bodov. Voľby monitorovania zoznamu súborov sa skopírujú na všetky koncové body v tejto skupine.
   - Šípkou doprava rozviňte skupinu a zobrazte zoznam všetkých koncových bodov, ktoré sa v nej nachádzajú. Označte začiarkavacie políčko každého koncového bodu v skupine, na ktorý chcete skopírovať voľby monitorovania súborov.
   - Rozviňte zoznam koncových bodov v skupine **All Systems**. Označte začiarkavacie políčko každého koncového bodu v skupine, na ktorý chcete skopírovať konfiguračné voľby.
4. Kliknite na **OK**. Voľby monitorovania súborov sa skopírujú na vybratú skupinu alebo na vybraté koncové body.

Spustenie kontroly Real Time Compliance (RTC)

Na stránke Security môžete spustiť kontrolu súladu s nariadeniami v reálnom čase a overiť, či je koncový bod ešte v súlade s nariadeniami.

1. Kliknite na elipsu napravo od koncového bodu, pre ktorý chcete spustiť kontrolu RTC.
2. Kliknite na **Run Compliance Check**. Otvorí sa stránka **Compliance**, na ktorej blikajúci riadok kontrolovaného koncového bodu indikuje, že kontrola prebieha.
3. Ak bude použitie niektorého z pravidiel neúspešné, zobrazí sa v stĺpci **#Failed Rules** správa o tomto zlyhaní. Pomocou šípky nadol umiestnenej vľavo vedľa koncového bodu môžete zobraziť neúspešné pravidlo.

Konfigurácia produktu Trusted Execution

Na stránke **Security** môžete konfigurovať produkt Trusted Execution (TE) pre konkrétny koncový bod alebo pre skupinu koncových bodov.

1. Kliknite na elipsu napravo od koncového bodu, pre ktorý chcete upraviť konfiguračné voľby TE.
2. Kliknite na **Configure TE**. Otvorí sa okno TE Policies Configuration.
3. Všetky konfiguračné voľby TE sú uvedené aj s vysvetleniami. Ak chcete zmeniť niektoré konfiguračné voľby TE, označte alebo zrušte označenie príslušných začiarkavacích políčok. V niektorých prípadoch sú zmeny volieb implementované až po reštarte servera.

4. Kliknite na **Save**.

Kopírovanie volieb Trusted Execution (TE) na iné skupiny

Konfiguračné voľby TE môžete kopírovať na ďalšie skupiny alebo na konkrétnu množinu koncových bodov.

1. Kliknite na elipsu napravo od koncového bodu, ktorého konfiguračné voľby chcete skopírovať na inú skupinu koncových bodov alebo na špecifickú množinu koncových bodov.
2. Kliknite na **Copy TE Configuration**. Zobrazia sa všetky skupiny koncových bodov, vrátane skupiny **All Systems**.
3. Jedným z nasledujúcich postupov vyberte skupinu alebo konkrétne koncové body:
   - V zozname dostupných skupín označte začiarkavacie políčko niektorej skupiny koncových bodov. Konfiguračné voľby sa skopírujú na všetky koncové body v tejto skupine.
   - Šípkou doprava rozviňte skupinu a zobrazte zoznam všetkých koncových bodov, ktoré sa v nej nachádzajú. Označte začiarkavacie políčko každého koncového bodu v skupine, na ktorý chcete skopírovať konfiguračné voľby.
   - Rozviňte zoznam koncových bodov v skupine **All Systems**. Označte začiarkavacie políčko každého koncového bodu v skupine, na ktorý chcete skopírovať konfiguračné voľby.
4. Kliknite na **OK**. Konfiguračné voľby sa skopírujú na vybratú skupinu alebo na vybraté koncové body.

Úprava zoznamu súborov Trusted Execution (TE)

Môžete zobraziť a upraviť voľby monitorovania TE pre každý súbor na koncovom bode.

1. Kliknite na elipsu napravo od koncového bodu, ktorý je hostiteľom súborov, pre ktoré chcete zobraziť a upraviť voľby monitorovania TE.
2. Kliknite na **Edit TE File List**. Otvorí sa stránka **TE File List Configuration** so zoznamom všetkých adresárov a súborov na tomto koncovom bode. Značka začiarknutia na ikone priečinka pre konkrétny adresár naznačuje, že minimálne jeden z jeho súborov je monitorovaný.
3. Ak sa súbor, ktorého voľby chcete zobraziť alebo upraviť, nachádza v niektorom adresári, zobrazte dvojitým kliknutím zoznam jeho súborov. V zozname sú uvedené všetky súbory z daného adresára.
4. V stĺpcoch **TE** a **Volatile** sú uvedené voľby monitorovania pre každý súbor na koncovom bode. Ak sú na niektorom súbore monitorované zmeny jeho obsahu, je označené jeho začiarkavacie políčko v stĺpci **TE**. Ak sú na sobore monitorované len zmeny povolení k súboru, má označené začiarkavacie políčko v stĺpci **Volatile**. Ak chcete zmeniť voľby monitorovania, označte alebo zrušte označenie začiarkavacích políčok jedného alebo viacerých súborov na koncovom bode.
5. Kliknite na **Save**.

Kopírovanie volieb monitorovania zoznamu súborov Trusted Execution (TE) na iné skupiny

Voľby monitorovania súborov TE môžete kopírovať na ďalšie skupiny alebo na konkrétnu množinu koncových bodov.

1. Kliknite na elipsu napravo od koncového bodu, ktorého voľby monitorovania súborov chcete skopírovať na inú skupinu koncových bodov alebo na špecifickú množinu koncových bodov.
2. Kliknite na **Copy TE File List**. Zobrazia sa všetky skupiny koncových bodov, vrátane skupiny **All Systems**.
3. Jedným z nasledujúcich postupov vyberte skupinu alebo konkrétne koncové body:
   - V zozname dostupných skupín označte začiarkavacie políčko niektorej skupiny koncových bodov. Voľby monitorovania zoznamu súborov sa skopírujú na všetky koncové body v tejto skupine.
   - Šípkou doprava rozviňte skupinu a zobrazte zoznam všetkých koncových bodov, ktoré sa v nej nachádzajú. Označte začiarkavacie políčko každého koncového bodu v skupine, na ktorý chcete skopírovať voľby monitorovania súborov.
   - Rozviňte zoznam koncových bodov v skupine **All Systems**. Označte začiarkavacie políčko každého koncového bodu v skupine, na ktorý chcete skopírovať konfiguračné voľby.
4. Kliknite na **OK**. Voľby monitorovania súborov sa skopírujú na vybratú skupinu alebo na vybraté koncové body.

Zobrazenie stavu ďalších funkcií PowerSC

Na stránke Security môžete zobraziť stav funkcií PowerSC: Trusted Boot, Trusted Firewall a Trusted Logging. Môžete tiež zobraziť stav aktualizácií TNC (Trusted Network Connect) na koncovom bode.

1. Vyberte na hlavnej stránke kartu **Security**. Otvorí sa stránka **Security**.
2. Komponent TNC produktu PowerSC je určený na kontrolu a aktualizáciu bezpečnostných opráv na každom koncovom bode. Stĺpec **Up-to-date via TNC** v tabuľke koncových bodov indikuje, či je koncový bod podľa servera TNC v aktualizovanom stave. Časť **Up-to-date via TNC** na baneri riadiaceho panela ukazuje percento koncových bodov v skupine, ktoré sú v aktualizovanom stave. Ak chcete zo stránky **Security** odstrániť informácie o aktualizáciách TNC, vykonajte tieto kroky:
   a. Kliknite na ikonu **Languages and Settings** na paneli s ponukami na hlavnej stránke.
   b. Kliknite na **Sub-product usage**.
   c. Vypnite možnosť **Up to date via TNC**.
   d. Ak chcete informácie znova zobraziť, prepnite **Up to date via TNC** do stavu zapnutý.
3. Stĺpec **TB** v tabuľke koncových bodov indikuje, či je na koncovom bode dostupný PowerSC Trusted Boot. Časť **Trusted Boot** na baneri riadiaceho panela ukazuje percento koncových bodov vo vybratej skupine, na ktorých je aktivovaný PowerSC Trusted Boot. Ak chcete zo stránky **Security** odstrániť informácie o PowerSC Trusted Boot, postupujte nasledovne:
   a. Kliknite na ikonu **Languages and Settings** na paneli s ponukami na hlavnej stránke.
   b. Kliknite na **Sub-product usage**.
   c. Posuňte prepínač **Trusted Boot** do polohy vypnutý.
   d. Ak chcete informácie znova zobraziť, posuňte prepínač do polohy zapnutý.
4. Stĺpec **TF** v tabuľke koncových bodov indikuje, či je na koncovom bode dostupný PowerSC Trusted Firewall. Časť **Trusted Firewall** na baneri riadiaceho panela ukazuje percento koncových bodov vo vybratej skupine, na ktorých je aktivovaný PowerSC Trusted Firewall. Ak chcete zo stránky **Security** odstrániť informácie o produkte Trusted Firewall, postupujte nasledovne:
   a. Kliknite na ikonu **Languages and Settings** na paneli s ponukami na hlavnej stránke.
   b. Kliknite na **Sub-product usage**.
   c. Posuňte prepínač **Trusted Firewall** do polohy vypnutý.
   d. Ak chcete informácie znova zobraziť, posuňte prepínač do polohy zapnutý.
5. Stĺpec **TL** v tabuľke koncových bodov indikuje, či je na koncovom bode dostupný PowerSC Trusted Logging. Časť **Trusted Logging** na baneri riadiaceho panela ukazuje percento koncových bodov vo vybratej skupine, na ktorých je aktivovaný PowerSC Trusted Logging. Ak chcete zo stránky **Security** odstrániť informácie o produkte Trusted Firewall, postupujte nasledovne:
   a. Kliknite na ikonu **Languages and Settings** na paneli s ponukami na hlavnej stránke.
   b. Kliknite na **Sub-product usage**.
   c. Posuňte prepínač **Turusted Logging** do polohy vypnutý.
   d. Ak chcete informácie znova zobraziť, posuňte prepínač do polohy zapnutý.

Prepínanie monitorovania Trusted Execution

Monitorovanie Trusted Execution (TE) môžete prepínať do stavu zapnutý alebo vypnutý. Môžete tiež vypnúť monitorovanie TE a naplánovať jeho spustenie v závislosti na konkrétnom časovom intervale.

1. Kliknite na ikonu **Trusted Execution Toggle**.
2. V rozbaľovacej ponuke vyberte jednu z nasledujúcich možností:
   - **Turn ON for All endpoints** zapne monitorovanie TE na všetkých koncových bodoch.
   - **Turn OFF for ALL endpoints** vypne monitorovanie TE na všetkých koncových bodoch.
3. Pri vypnutí monitorovania TE sa sprístupnia možnosti nastavenia času, kedy sa má monitorovanie TE reštartovať. Môžete si vybrať jednu z nasledujúcich možností:
   - **1 Hour**

- **5 Hours**
- **1 Day**
- **1 Week**
- **Never**

4. Kliknite na **Save**.

Odoslanie e-mailového oznámenia, keď dôjde k bezpečnostnej udalosti

Zo stránky Security môžete jednému alebo viacerým príjemcom odoslať e-mailové oznámenie, keď dôjde k bezpečnostnej udalosti.

1. Vyberte na hlavnej stránke kartu **Security**. Otvorí sa stránka **Security**.
2. Kliknite na ikonu **Email Settings** v pravom rohu panela s ponukami. Otvorí sa okno **Email Settings**.
3. Označte začiarkavacie políčko **Send me emails**.
4. V poli **Addresses (comma separated)** zadajte e-mailové adresy príjemcov a jednotlivé adresy oddeľujte čiarkami.

Práca so zostavami

Na stránke Reports v grafickom užívateľskom rozhraní PowerSC môžete pristupovať k viacerým zostavám.

Dostupné sú nasledujúce zostavy:

- Zostava **Compliance Overview** je snímka informácií na vysokej úrovni, ktoré sa zobrazujú na stránke **Compliance** rozhrania.
- Zostava **Compliance Detail** je snímka informácií vysokej úrovne a podrobných informácií, ktoré sa zobrazujú na stránke **Compliance**.
- Zostava **File Integrity Overview** je snímka informácií vysokej úrovne, ktoré sa zobrazujú na stránke **Security** rozhrania.
- Zostava **File Integrity Detail** je snímka informácií vysokej úrovne a podrobných informácií, ktoré sa zobrazujú na stránke **Security**.
- **Combined Compliance and FIM**

Stránka **Reports** predvolene zobrazuje zostavy **Compliance Overview** a **File Integrity Overview** za skupinu **All Systems**. Zostavy **Compliance Detail**, **File Integrity Detail** alebo **Combined Compliance and FIM** nemajú stanovené žiadne predvolené skupiny.

Môžete vytvoriť ktorúkoľvek zostavu pre skupinu **All Systems** a pre ktorúkoľvek vami definovanú skupinu. Môžete vytvoriť zostavu pre všetky koncové body v skupine alebo pre podmnožinu koncových bodov v skupine. Keď vygenerujete zostavu, môžete naplánovať jej distribúciu ako e-mail vo formáte HTML a ako súbor CSV, jednému alebo viacerým príjemcom, s okamžitým odoslaním alebo s každodenným odosielaním.

Zoznam zostáv zobrazených na stránke **Reports** sa líši v závislosti na tom, pod akým ID užívateľa ste prihlásený. Môžete generovať len tie zostavy, ktoré spravujete pod svojím ID. Každá zostava, ktorú vygenerujete v rámci jednej relácie, sa zobrazí v zozname o spustení ďalšej relácie.

Výber skupiny pre zostavu

Každú zostavu môžete spustiť pre skupinu **All Systems** a pre ktorúkoľvek vami definovanú skupinu. Môžete spustiť zostavu pre všetky koncové body zahrnuté v skupine alebo pre podmnožinu koncových bodov v skupine.

1. Kliknite na hlavnej stránke na kartu **Reports**. Otvorí sa stránka **Reports**.
2. Kliknite na elipsu napravo od typu zostavy, ktorý chcete distribuovať.
3. Kliknite na **Change Group**.
4. Otvorí sa pole výberu so všetkými dostupnými skupinami. Vyberte prepínač vedľa skupiny, na ktorej chcete spustiť zostavu. Kliknite na **Confirm**. Spustí sa zostava a obsah hlavnej stránky sa obnoví o informácie z vybratej skupiny.

5. Ak chcete spustiť zostavu pre podmnožinu koncových bodov, rozviňte skupinu **All Systems**. Zobrazí sa zoznam všetkých dostupných koncových bodov. Označte začiarkavacie políčko vedľa každého koncového bodu, ktorý chcete zahrnúť do zostavy. Kliknutím na **Confirm** spustite zostavu.

   Poznámka: Ak chcete spustiť zostavu na konkrétnej skupine koncových bodov, môžete vytvoriť skupinu, ktorá obsahuje tieto koncové body. Vytvorenie skupiny vám ušetrí čas a budú ju môcť použiť všetci užívatelia, pretože skupiny sú globálne (môžu ich vidieť všetci užívatelia rozhrania).
6. Ak chcete vyhľadať konkrétny koncový bod, zadajte jeho názov do vyhľadávacieho textového poľa. Kliknutím na **Confirm** spustíte zostavu pre daný koncový bod.

Distribúcia zostáv prostredníctvom e-mailu

Keď nastavíte skupinu pre zostavu, môžete naplánovať distribúciu zostavy ako e-mail s HTML formátovaním a ako súbor CSV. Môžete naplánovať odoslanie e-mailu jednému alebo viacerým príjemcom, okamžite alebo každý deň.

Vloženie zostavy vo formáte CSV umožňuje príjemcom načítať údaje zostavy v tabuľkovom hárku alebo ich importovať do inej aplikácie, ktorá vie pracovať so súbormi CSV. Súbory CSV neobsahujú grafiku ani koncepty riadiacich panelov. Súbor CSV vygenerovaný z prehľadovej zostavy obsahuje v prvom riadku všetky hlavičky stĺpcov, oddelené čiarkami. Nasledujúce riadky sú zoznamom koncových bodov a hodnôt z jednotlivých stĺpcov.

Z podrobných zostáv sú generované viaceré súbory CSV. Prvý súbor CSV je formátovaný podobne ako prehľadová zostava. Za každú úroveň podrobnosti zostavy je generovaný samostatný súbor CSV. Napríklad, v prípade zostavy File Integrity Details Report budú vygenerované samostatné súbory CSV podľa nasledujúcich úrovní podrobnosti:

- **TE Configuration**
- **RTC Configuration**
- **Sub-product status**

1. Kliknite na hlavnej stránke na kartu **Reports**. Otvorí sa stránka **Reports**.
2. V zozname dostupných zostáv vyberte zostavu, ktorú chcete distribuovať. Zostava sa spustí a obnoví sa hlavná stránka.
3. Kliknite na elipsu napravo od zostavy, ktorú chcete distribuovať.
4. Kliknite na **Email Options**. Otvorí sa okno Send report by email.
5. Zadajte v poli **Addresses** e-mailové adresy všetkých príjemcov. Jednotlivé adresy oddeľte bodkočiarkami (;).
6. Zadajte popis e-mailu v poli **Subject**.
7. Vyberte jednu z nasledujúcich možností:
   - Ak chcete zaslať zostavu príjemcom každý deň, označte začiarkavacie políčko **Send every day at**. Zadajte lokálny čas (hodiny a minúty), kedy chcete e-mail odoslať. Kliknite na **Save and Close**. Zostava sa odošle každý deň v stanovenom čase.
   - Ak chcete e-mail odoslať okamžite, kliknite na **SEND IMMEDIATELY**. Zostava sa odošle a okno sa zatvorí.

Príkazy PowerSC Standard Edition

PowerSC Standard Edition poskytuje príkazy, ktoré povoľujú komunikáciu s komponentom Trusted Firewall a komponentom Trusted Network Connect prostredníctvom príkazového riadka.

príkaz chvfilt

Účel

Zmení hodnoty existujúceho pravidla filtrovania pokrývajúceho viaceré virtuálne siete LAN.

Syntax

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

Popis

Príkaz **chvfilt** umožňuje zmeniť definíciu pravidla filtrovania pokrývajúceho viaceré virtuálne siete LAN v tabuľke s pravidlami filtrovania.

Príznaky

-a Určuje akciu. Platné hodnoty:
- D (Zakázať): Blokuje premávku
- P (Povoliť): Povoľuje premávku

-c Určuje rôzne protokoly, na ktoré možno aplikovať pravidlo filtrovania. Platné hodnoty:
- udp
- icmp
- icmpv6
- tcp
- any

-d Určuje cieľovú adresu vo formáte IPv4 alebo IPv6.

-m Určuje masku zdrojovej adresy.

-M Určuje masku cieľovej adresy.

-n Určuje ID filtra v pravidle filtrovania, ktoré by sa malo upraviť.

-o Určuje zdrojový port alebo operáciu typu ICMP (Internet Control Message Protocol). Platné hodnoty:
- lt
- gt
- eq
- any

-O Určuje cieľový port alebo kódovú operáciu ICMP. Platné hodnoty:
- lt
- gt
- eq
- any

-p Určuje zdrojový port alebo typ ICMP.

-P Určuje cieľový port alebo kód ICMP.

-s Určuje zdrojovú adresu vo formáte v4 alebo v6.

-v Určuje verziu IP tabuľky s pravidlami filtrovania. Platné hodnoty sú 4 a 6.

-z Určuje ID virtuálnej siete LAN zdrojového logického oddielu.

-Z Určuje ID virtuálnej siete LAN cieľového logického oddielu.

Stav ukončenia

Tento príkaz vráti tieto výstupné hodnoty:

0 Úspešné dokončenie.

>0 Nastala chyba.

Príklady

1. Ak chcete zmeniť platné pravidlo filtrovania, ktoré existuje v jadre, príkaz zadajte takto:
   ```
   chvfilt -n 1 -v4 -a P -z 100 -Z 300 -o eq -p 23 -O lt -P 345 -c tcp
   ```
2. Keď pravidlo filtrovania (n=2) neexistuje v jadre, výstup je takýto:
   ```
   chvfilt -n 2 -v4 -a P -z 100 -Z 300 -o eq -p 23 -O lt -P 345 -c tcp
   ```

   Systém zobrazí výstup takto:
   ```
   ioctl(QUERY_FILTER) failed no filter rule err=2
   Nie je možné zmeniť pravidlo filtrovania.
   ```

---

príkaz genvfilt

Účel

Pridá pravidlo filtrovania pokrývajúce viaceré virtuálne siete LAN (VLAN) medzi logickými oddielmi na jednom serveri IBM Power Systems.

Syntax

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

Popis

Príkaz **genvfilt** pridá pravidlo filtrovania pokrývajúce viaceré virtuálne siete LAN (VLAN) medzi logickými oddielmi (LPAR) na jednom serveri IBM Power Systems.

Príznaky

-a Určuje akciu. Platné hodnoty:
- D (Zakázať): Blokuje premávku
- P (Povoliť): Povoľuje premávku

-c Určuje rôzne protokoly, na ktoré možno aplikovať pravidlo filtrovania. Platné hodnoty:
- udp
- icmp
- icmpv6
- tcp

- any

-d Určuje cieľovú adresu vo formáte v4 alebo v6.

-m Určuje masku zdrojovej adresy.

-M Určuje masku cieľovej adresy.

-o Určuje zdrojový port alebo operáciu typu ICMP (Internet Control Message Protocol). Platné hodnoty:
- lt
- gt
- eq
- any

-O Určuje cieľový port alebo kódovú operáciu ICMP. Platné hodnoty:
- lt
- gt
- eq
- any

-p Určuje zdrojový port alebo typ ICMP.

-P Určuje cieľový port alebo kód ICMP.

-s Určuje zdrojovú adresu vo formáte IPv4 alebo IPv6.

-v Určuje verziu IP tabuľky s pravidlami filtrovania. Platné hodnoty sú 4 a 6.

-z Určuje ID virtuálnej siete LAN zdrojového logického oddielu. ID virtuálnej siete LAN musí byť v rozsahu 1 až 4096.

-Z Určuje ID virtuálnej siete LAN cieľového logického oddielu. ID virtuálnej siete LAN musí byť v rozsahu 1 až 4096.

Stav ukončenia

Tento príkaz vráti tieto výstupné hodnoty:

0 Úspešné dokončenie.

>0 Nastala chyba.

Príklady

1. Ak chcete pridať pravidlo filtrovania, aby ste povolili údaje TCP zo zdrojového ID siete VLAN 100 do cieľového ID siete VLAN 200 v špecifických portoch, príkaz zadajte takto:

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

Súvisiaci odkaz:

“príkaz mkvfilt” na strane 152

“Príkaz vlantfw” na strane 170

---

príkaz lsvfilt

Účel

Vypíše zoznam pravidiel filtrovania pokrývajúcich viaceré virtuálne siete LAN z tabuľky filtrov.

Syntax

lsvfilt [**-a**]

Popis

Príkaz **lsvfilt** umožňuje vypísať zoznam pravidiel filtrovania pokrývajúcich viaceré virtuálne siete LAN a ich stav.

Príznaky

-a Vypíše len zoznam aktívnych pravidiel filtrovania.

Stav ukončenia

Tento príkaz vráti tieto výstupné hodnoty:

0 Úspešné dokončenie.

>0 Nastala chyba.

Príklady

1. Ak chcete vypísať zoznam aktívnych pravidiel filtrovania v jadre, príkaz zadajte takto:

```
lsvfilt -a
```

Súvisiace koncepty:

“Deaktivovanie pravidiel” na strane 109
Môžete deaktivovať pravidlá, ktoré povoľujú krížové smerovanie VLAN vo funkcii Trusted Firewall.

---

príkaz mkvfilt

Účel

Aktivuje pravidlá filtrovania pokrývajúce viaceré virtuálne siete LAN definované príkazom **genvfilt**.

Syntax

mkvfilt -u

Popis

Príkaz **mkvfilt** aktivuje pravidlá filtrovania pokrývajúce viaceré virtuálne siete LAN definované príkazom **genvfilt**.

Príznaky

-u Aktivuje pravidlá filtrovania v tabuľke pravidiel filtrovania.

Stav ukončenia

Tento príkaz vráti tieto výstupné hodnoty:

0 Úspešné dokončenie.

>0 Nastala chyba.

Príklady

1. Ak chcete aktivovať pravidlá filtrovania v jadre, príkaz zadajte takto:

```
mkvfilt -u
```

Súvisiaci odkaz:

“príkaz genvfilt” na strane 150

príkaz pmconf

Účel

Hlási a spravuje server TNCPM (Trusted Network Connect Patch Management) registrovaním technologických úrovní a serverov TNC pre najnovšie opravy a generovaním hlásení o stave TNCPM.

Poznámka: Server TNCPM sa môže spúšťať iba v systéme AIX verzie 7.2 s technologickou úrovňou 7100-02, aby bolo možné sťahovať metaúdaje servisných balíkov.

Syntax

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

pmconf rmtncpm

pmconf start

pmconf stop

pmconf init -i <*interval sťahovania*> **-l** <*zoznam TL*> **-A** [**-P** <*cieľová cesta*>] [**-x** <*interval ifix*>] [**-K** <*kľúč ifix*>]

pmconf add -l *zoznam_TL*

pmconf add -o <*názov balíka*> -V <*verzia*> -T [installp|rqm] -D <*užívateľom definovaná cesta*>

pmconf add -p <*Zoznam SP*> [**-U** <*užívateľom definovaná cesta SP*>]

pmconf add -p <*SP*> **-e** <*súbor ifix*>

pmconf add -y <*súbor s podpornými informáciami*> **-v** <*súbor s podpisom*> **-e**

pmconf chtncpm atribút = *hodnota*

pmconf delete -l <*zoznam TL*>

pmconf delete -o <*názov balíka*> -V <*verzia*>

pmconf delete -p <*Zoznam SP*>

pmconf delete -p <*SP*>**-e** *súbor ifix*

pmconf export -f *názov_súboru*

pmconf get -o <balík> -V <verzia> -T <installp | rpm> -D <cieľový adresár>

pmconf get -L -o <balík> -V <verzia | all> -T <installp | rpm>

pmconf get -L -p <servisný balík>

pmconf get -p <SP> -D <cieľový adresár>

pmconf hist -d

pmconf hist -u

pmconf import -f *názov_súboru_cert* **-k** *názov_súboru_kľúča*

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

pmconf list -a *SP*

pmconf list -C

pmconf list -l *SP*

pmconf list -o <*názov balíka*> -V <*verzia*>

pmconf list -o [-c] [-q]

protokol pmconf úroveň_protokolu = info | chyba | žiadny

pmconf modify -i < *interval sťahovania*>

pmconf modify -P <*cesta sťahovania*>

pmconf modify -g <*áno alebo nie na akceptovanie všetkých licencií*>

pmconf modify -t <*zoznam typu APAR*>

pmconf modify -x <*interval ifix*>

pmconf modify -K <*kľúč ifix*>

pmconf proxy display

pmconf proxy [enable=yes | no] [host=<názov_hostiteľa>] [port=<číslo_portu>]

pmconf restart

stav pmconf

Popis

Toto sú funkcie príkazu **pmconf**:

Správa archívu opráv
Registruje alebo ruší registráciu technologických úrovni; ruší registráciu serverov TNC. TNCPM vytvorí archív opráv pre každú technologickú úroveň, ktorá obsahuje najnovšie opravy, informácie **lslpp** (napríklad informácie o nainštalovaných sadách súborov alebo aktualizáciách sád súborov), a informácie o opravách zabezpečenia pre túto technologickú úroveň.

Hlásenie
Vygeneruje hlásenia o stave TNCPM.

Pomocou príkazu **pmconf** možno vykonať tieto operácie:

Položka	Popis
add	Zaregistruje novú technologickú úroveň pomocou TNCPM.
chtncpm	Zmení atribúty v súbore tnccs.conf. Aby zmeny na serveri TNCPM nadobudli účinnosť, vyžaduje sa explicitný príkaz **start**.
delete	Zruší registráciu technologickej úrovne pomocou TNCPM.
get	Zobrazí alebo stiahne informácie o dostupných bezpečnostných opravách a balíkoch Open Source.
history	Zobrazí históriu aktualizácií a stiahnutí.
list	Zobrazí informácie o TNCPM.
log	Nastaví úroveň protokolovania pre komponent TNC.
mktncpm	Vytvorí server TNCPM.
modify	Upraví atribúty tncpm.conf.
proxy	Spravuje konfiguráciu parametrov proxy servera.
rmtncpm	Odstráni server TNCPM.
start	Spustí server TNCPM.
stop	Zastaví server TNCPM.

Príznaky

Položka	Popis
-A	Akceptuje všetky licenčné zmluvy pri vykonaní aktualizácií klientov.
-a <súbor dokumentu s analýzou problému>	Určuje súbor dokumentu s analýzou problému, ktorý korešponduje s parametrom **ifix**. Ak súbor dokumentu s analýzou problému nie je poskytnutý, parameter **ifix** nie je zobrazený ako adresa CVE (common vulnerabilities and exposures) dočasnej opravy.
-a *SP*	Vygeneruje hlásenie o informáciách o bezpečnostnom hlásení o analýze autorizovaným programom (APAR) pre servisný balík. *SP* je vo formáte REL00-TL-SP (napríklad 6100-01-04 reprezentuje servisný balík 04 pre technologickú úroveň 01 a verziu 6.1).
-e <súbor ifix>	Určuje dočasné opravy, ktoré sú pridané do TNCPM.
-i *interval_sťahovania*	Určuje interval, ktorý TNCPM skontroluje, či sa v ňom nenachádza nový servisný balík pre registrované technologické úrovne. Interval je celočíselná hodnota v minútach alebo hodnota v nasledujúcom formáte: **d** (počet dní): **h** (hodiny): **m** (minúty). Podporovaný rozsah pre interval *download_interval* je 30 až 525600 minút.
-K <kľúč ifix>	Určuje verejný kľúč nástroja IBM AIX PSIRT (Product Security Incident Response Tool), ktorý umožňuje autentifikovať stiahnuté dokumenty s analýzou problému a dočasné opravy. Tento verejný kľúč možno stiahnuť zo servera verejných kľúčov PGP prostredníctvom ID **0x28BFAA12**.
-L	Určuje režim (zoznam alebo vyhľadávanie).
o *názov balíka*	Názov balíka Open Source, ktorý sa má vyhľadať alebo stiahnuť.
-P *cesta_k_archívu_opráv*	Určuje adresár sťahovania pre archívy opráv, ktoré stiahne TNCPM. Predvolený adresár je **/var/tnc/tncpm/fix_repository**.
-p *zoznam_SP*	Určuje zoznam servisných balíkov, ktoré možno stiahnuť. Zoznam je zoznam údajov oddelených čiarkou vo formáte REL00-TL-SP (napríklad 6100-01-04 reprezentuje servisný balík 04 pre technologickú úroveň 01 a verziu 6.1). Keď použijete príznak -U, zadajte len jeden SP.
-t *zoznam_typu_APAR*	Určuje typy APAR, ktoré TNCPM podporuje pre aktualizáciu klienta a zoznam serverov TNC. Bezpečnostné hlásenia APAR sú vždy podporované. zoznam_typu_APAR je zoznam údajov oddelených čiarkou a má tieto typy: HIPER, FileNet Process Engine, Enhancement.
T *typ balíka*	Určuje typ balíka Open Source, ktorý sa má vyhľadať alebo stiahnuť
-U *užívateľom_definovaný_archív_opráv*	Určuje cestu k užívateľom definovanému archívu opráv. Zadajte vydanie, technologickú úroveň a servisný balík, ktoré sú spojené s archívom opráv, ktorý je použitý na overenie a aktualizácie klientov.
-s	Vygeneruje hlásenie o registrovaných servisných balíkoch.
-l *SP*	Vygeneruje hlásenie o informáciách **lslpp** pre servisný balík. *SP* je vo formáte REL00-TL-SP (napríklad 6100-01-04 reprezentuje servisný balík 04 pre technologickú úroveň 01 a verziu 6.1).
-u	Vygeneruje hlásenie o histórii aktualizácií klienta.
V *verzia*	Verzia balíka Open Source, ktorý sa má vyhľadať alebo stiahnuť. V režime vyhľadávania (-L) môžete určiť hodnotu „all“, aby sa vyhľadali všetky dostupné verzie určeného balíka.
-d	Vygeneruje hlásenie o histórii stiahnutí servisných balíkov.
-C	Vygeneruje hlásenie o serverovom certifikáte.
-f *názov_súboru*	Určuje názov súboru certifikátu.
-k	Určuje súbor, z ktorého musí byť certifikačný kľúč prečítaný v prípade operácie importu.

-c	Zobrazí užívateľské atribúty v záznamoch oddelených dvojbodkou:
	`# názov: atribút1: atribút2: ...`
	`politika: hodnota1: hodnota2: ...`

-v <*súbor s podpisom*>	Určuje súbor s podpisom pre dokument s analýzou bezpečnostného nedostatku IBM AIX.
-y <*súbor dokumentu s analýzou problému*>	Určuje súbor dokumentu s analýzou bezpečnostného nedostatku IBM AIX.
-q	Potláča informácie hlavičky.

Položka	Popis
-x <*interval ifix*>	Určuje interval v minútach na vyhľadanie a stiahnutie nových dočasných opráv. Ak je táto hodnota nastavená na 0, automatické stiahnutie dočasných opráv a oznámenie bude zakázané. Predvolený interval je každých 24 hodín. Podporovaný rozsah pre <*interval ifix*> je 30 až 525600 minút.

Stav ukončenia

Tento príkaz vráti tieto výstupné hodnoty:

Položka	Popis
0	Príkaz bol úspešne spustený a všetky vyžadované zmeny sú vykonané.
>0	Nastala chyba. Vytlačená chybová správa obsahuje viac podrobností o type zlyhania.

Príklady

1. Ak chcete inicializovať TNCPM, zadajte tento príkaz:
   ```
   pmconf init -f 10080 -l 5300-11,6100-00
   ```
2. Ak chcete vytvoriť démona TNCPM, zadajte tento príkaz:
   ```
   mktncpm pmport=55777 tncserver=11.11.11.11:77555
   ```
3. Ak chcete spustiť server, zadajte tento príkaz:
   ```
   pmconf start
   ```
4. Ak chcete zastaviť server, zadajte tento príkaz:
   ```
   pmconf stop
   ```
5. Ak chcete zaregistrovať novú technologickú úroveň pomocou TNCPM, zadajte tento príkaz:
   ```
   pmconf add -l 6100-01
   ```
6. Ak chcete zrušiť technologickú úroveň z TNCPM, zadajte tento príkaz:
   ```
   pmconf delete -l 6100-01
   ```
7. Ak chcete zrušiť registráciu servera TNC, ktorý má IP adresu 11.11.11.11, z TNCPM, zadajte tento príkaz:
   ```
   pmconf delete -t 11.11.11.11
   ```
8. Ak chcete zaregistrovať novšiu verziu staršieho servisného balíka do TNCPM, zadajte tento príkaz:
   ```
   pmconf add -s 6100-01-04
   ```
9. Ak chcete zrušiť starší servisný balík z TNCPM, zadajte tento príkaz:
   ```
   pmconf delete -s 6100-01-04
   ```
10. Ak chcete vygenerovať hlásenie o archívoch opráv pre každú registrovanú technologickú úroveň, zadajte tento príkaz:
    ```
    pmconf list -s
    ```
11. Ak chcete vygenerovať hlásenie o informáciách **lslpp** registrovanej technologickej úrovne, zadajte tento príkaz:
    ```
    pmconf list -l 6100-01-02
    ```
12. Ak chcete vygenerovať hlásenie z histórie aktualizácií, zadajte tento príkaz:
    ```
    pmconf hist -u
    ```
13. Ak chcete vygenerovať hlásenie z histórie sťahovaní, zadajte tento príkaz:
    ```
    pmconf hist -d
    ```
14. Ak chcete vygenerovať hlásenie o serverovom certifikáte, zadajte tento príkaz:
    ```
    pmconf list -C
    ```
15. Ak chcete vygenerovať hlásenie o bezpečnostných informáciách APAR servisného balíka, zadajte tento príkaz:
    ```
    pmconf list -a 6100-01-02
    ```
16. Ak chcete importovať serverový certifikát, zadajte tento príkaz:
    ```
    pmconf import -f /tmp/server.txt -k /tmp/server-cert-key.txt
    ```
17. Ak chcete exportovať serverový certifikát, zadajte tento príkaz:

```
pmconf export -f /tmp/server.txt
```

18. Ak chcete zobraziť všetky dostupné verzie balíka Open Source ‘emacs’ vo formáte rpm, zadajte nasledujúci príkaz:

```
pmconf get -L -o emacs -V all -T rpm
```

19. Ak chcete stiahnuť verziu 4.5.1 balíka Open Source ‘lsof’ vo formáte rpm do adresára /tmp/new_lsof, zadajte nasledujúce príkazy:

```
mkdir /tmp/new_lsof
pmconf get -o lsof -V 4.5.1 -T rpm -D /tmp/new_lsof
```

20. Ak chcete zobraziť všetky dostupné verzie balíka OpenSSH vo formáte installp, zadajte nasledujúci príkaz:

```
pmconf get -o openssh -T installp -L -V all
```

21. Ak chcete zobraziť aktuálne konfiguračné nastavenia proxy servera, ktoré program použije cURL pri sťahovaní balíkov Open Source alebo bezpečnostných opráv, zadajte nasledujúci príkaz:

```
pmconf proxy display
```

22. Ak chcete zakázať konfiguráciu proxy servera, zadajte nasledujúci príkaz:

```
pmconf proxy enable=no
```

23. Ak chcete povoliť proxy server a ako hostiteľa nastaviť ‘myProxyServer’ na porte 9876, zadajte nasledujúci príkaz:

```
pmconf proxy enable=yes host=myProxyServer port=9876
```

24. Ak chcete zmeniť používaný port proxy servera, zadajte nasledujúci príkaz:

```
pmconf proxy port=1234
```

25. Ak chcete zobraziť známe bezpečnostné nedostatky, ktoré riešia bezpečnostné opravy pre úroveň servisného balíka 7100-03-02, zadajte nasledujúci príkaz:

```
 pmconf get -L -p 7100-03-02
```

26. Ak chcete stiahnuť bezpečnostné opravy pre úroveň servisného balíka 7200-00-01 do adresára /tmp/ifixes_for_7.2.0.1 bez nainštalovania týchto opráv, zadajte nasledujúce príkazy:

```
mkdir /tmp/ifixes_for_7.2.0.1
pmconf get -p 7200-00-01 -D /tmp/ifixes_for_7.2.0.1
```

Príkaz pscon

Účel

Nahlasuje a riadi server Trusted Network Connect (TNC), klienta TNC, odkazovača TNC IP (IPRef) a Service Update Management Assistant (SUMA). Riadi politiky správy sady súborov a opráv týkajúce sa integrity koncového bodu (server a klient) pri alebo po pripojení siete na ochranu siete pred hrozbami a útokmi.

Syntax

Operácie servera TNC:

psconf mkserver [**tncport=**<*port*>] **pmserver=**<*hostiteľ:port*> [tsserver=<hostiteľ>] [**recheck_interval=**<*čas_v_minútach*> | **d** (dni) : **h** (hodiny) : **m** (minúty)] [**dbpath** = <*užívateľom_definovaný_adresár*>] [**default_policy=**<*yes* | *no* >] [**clientData_interval=**<*čas_v_minútach*> | **d** (dni) : **h** (hodiny) : **m** (minúty)] [**clientDataPath=**<*úplná_cesta*>]

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

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

psconf chserver atribút = *hodnota*

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

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

psconf add { **-G** <*názov_skupiny_IP*> **ip=**[**±**]<*hostiteľ1, hostiteľ2...>* | {**-A**<*skupinaAPAR*> [**aparlist**=[**±**]*apar1, apar2...* | {**-V** <*ifixgrp*> [*ifixlist*=[+|-]*ifix1,ifix2...*]}

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

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

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

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

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

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

psconf certdel -i <*host*>

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

psconf update [-p] {-i<*hostiteľ*>| **-G** <*ipgroup*>[**-r** <*buildinfo*> | **-a** <*apar1, apar2...*> | [**-u**] **-v** <*ifix1, ifix2,...*> | **-O** <*openpkggrp1, openkggrp2,...*>}

psconf log loglevel=<info | error | none>

psconf import -C -i <*hostiteľ*> **-f** <*názov súboru*> | **–d** <*názov súboru databázy importu*>

psconf { **import -k** <*názov súboru kľúčov*> | **export**} **-S -f** <*názov súboru*>

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

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

psconf export -d <cesta k adresáru exportu>

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

psconf report -A <advisoryname>

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

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

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

psconf clientData {-l | -g} -i <*ip*|*host*>

psconf add -O <*openpkggrp*> <*openpkgname:version*>

psconf delete -O <*openpkggrp*> <*openpkgname:version*>

psconf delete -O <*openpkggrp*>

psconf delete -O ALL

psconf add -O <*openpkggrp*> fspolicy=<*fspolicy name*>

psconf report -O ALL -o TEXT

psconf add -V <*ifixgrp*> autoupdate=<yes|no>

psconf reboot -i <*host*> last one

Operácie klienta TNC:

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

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

psconf { **rmclient | status** }

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

psconf chclient atribút = *hodnota*

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

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

psconf import { **-S | -C -k** <*názov súboru kľúčov*> } **-f** <*názov súboru*>

Operácie TNC IPRef:

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

psconf { **rmipref | status**}

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

psconf chipref atribút = *hodnota*

psconf { **import -k** <*názov súboru kľúčov*> **| export** } **-R -f** <*názov súboru*>

psconf list -R

Popis

Technológia TNC je architektúra založená na otvorenom štandarde na autentifikáciu koncových bodov, manažment integrity platforiem a integráciu bezpečnostných systémov. Architektúra TNC kontrolujte koncové body (sieťových klientov a servery), či spĺňajú bezpečnostné politiky a až potom ich povolí na chránenej sieti. TNC IPRef upozorní server TNC na všetky nové IP adresy, ktoré sa detegujú na virtuálnom I/O serveri (VIOS).

SUMA pomáha odľahčiť administrátorov systému od úlohy manuálneho získavania aktualizácií údržby z webu. Ponúka flexibilné voľby, ktoré umožnia administrátorovi systému nastaviť automatizované rozhranie na preberanie opráv z webovej stránky distribúcie opráv na ich systém.

Príkaz **psconf** riadi sieťový server a klientov pridávaním alebo mazaním bezpečnostných politík ako dôveryhodných alebo nedôveryhodných, generovaním zostáv a aktualizovaním servera a klienta.

Pomocou príkazu **psconf** je možné vykonávať nasledujúce operácie:

Položka	Popis
add	Pridá politiku, klienta alebo e-mailové informácie na server TNC.
apargrp	Určuje názvy skupín APAR ako súčasť politiky sady súborov, ktoré sa použijú na overovanie klientov TNC.
aparlist	Určuje zoznam APAR, ktoré sú súčasťou skupiny APAR.
certadd	Označí certifikát ako dôveryhodný alebo nedôveryhodný.
certdel	Vymaže klientske informácie.
chclient	Zmení atribúty v súbore tnccs.conf. Na aplikovanie zmien v klientovi TNC sa vyžaduje explicitný príkaz **start**. Syntax formátu atribút=hodnota bude rovnaká ako pri príkaze **mkclient**.
chipref	Zmení atribúty v súbore tnccs.conf. Na aplikovanie zmien v IPRef sa vyžaduje explicitný príkaz **start**. Syntax formátu atribút=hodnota je rovnaká ako pri príkaze **mkipref**.
chserver	Zmení atribúty v súbore tnccs.conf. Na aplikovanie zmien na serveri TNC sa vyžaduje explicitný príkaz **start**. Syntax formátu atribút=hodnota je rovnaká ako pri príkaze **mkserver**. **Poznámka:** Atribút **dbpath** nie je možné zmeniť pomocou príkazu **chserver**. Možno ho nastaviť len počas spustenia príkazu **mkserver**.
clientData	Vytvorí snímku informácií (nainštalovaný operačný systém a sady súborov) o klientovi TNC. Cesta *clientDataPath* identifikuje miesto, kam sa uložia informácie o kolekcii snímky. Predvolené umiestnenie je adresár /var/tnc/clientData/ na serveri TNC. Cestu *clientDataPath* môžete zmeniť alebo nastaviť pomocou podpríkazu **chserver** alebo **mkserver**. Kolekciu snímky klienta TNC môžete spustiť z príkazového riadka zadaním podpríkazu **clientData** zo servera TNC. Podpríkaz **clientData**, ktorý sa spúšťa z príkazového riadka, je nezávislý od intervalu **clientData_interval**.
clientData_interval	Pomocou podpríkazu **chserver** alebo **mkserver** môžete nakonfigurovať, že sa kolekcia snímky má vykonávať v pravidelných intervaloch, a to nastavením hodnoty pre interval **clientData_interval**. Kolekcia snímky sa spustí automaticky, keď má interval **clientData_interval** inú hodnotu ako 0 (nula). Kolekcia snímky je predvolene zakázaná plánovačom. Plánovač môžete povoliť určením hodnoty pre **clientData_interval** vyššej ako alebo rovnej 30. Ak chcete zakázať plánovač, nastavte hodnotu 0 (nula) pre interval **clientData_interval**. Podporovaný rozsah pre interval **clientData_interval** je 30 až 525600 minút.
dbpath	Určuje umiestnenie databázy TNC. Predvolená hodnota je /var/tnc.
default_policy	Povolí alebo zakáže automatické overovanie klientov TNC pre dočasné opravy (ifix) a opravy APAR na rovnakej úrovni ako má klient. Nastavte hodnotu *yes*, ak chcete povoliť automatické overenie. Nastavte hodnotu *no*, ak chcete zakázať automatické overenie. Bližšie informácie o podpríkaze **default_policy** nájdete v tabuľke default_policy.
delete	Vymaže politiku alebo klientske informácie.
export	Exportuje klientsky alebo serverový certifikát alebo databázu na server TNC.
fspolicy	Určuje politiku sady súborov vydania, technologickej úrovne a servisného balíka, ktoré sa používajú na overovanie klientov TNC.
import	Importuje certifikát na klientovi alebo serveri alebo databázu na serveri TNC.
ipgroup	Určuje skupinu protokolov IP, ktorá obsahuje viaceré klientske IP adresy alebo názvy hostiteľov.
list	Zobrazí informácie o serveri TNC, klientovi TNC alebo SUMA.
log	Nastaví úroveň protokolovania pre komponenty TNC.
mkclient	Nakonfiguruje klienta TNC.
mkipref	Nakonfiguruje TNC IPRef.
mkserver	Nakonfiguruje server TNC.

Položka	Popis
Openpkggrp	Určuje názov skupiny openpkg v rámci politiky fileset používanej na overovanie klientov.
pmport	Určuje číslo portu, na ktorom načúva **pmserver**. Predvolená hodnota je 38240.
pmserver	Určuje názov hostiteľa alebo IP adresu príkazu **suma**, ktorý prevezme najnovšie servisné balíky a bezpečnostné opravy dostupné na webovej stránke IBM® ECC a webovej stránke IBM Fix Central.
reboot	Reštartuje klienta TNC identifikovaného IP adresou v premennej <*hostiteľ*>.
recheck_interval	Určuje interval v minútach, alebo formáte d (dni) : h (hodiny) : m (minúty) pre server TNC na overovanie klientov TNC. Podporovaný rozsah pre interval **recheck_interval** je 30 až 525600 minút. **Poznámka:** Nastavenie **recheck_interval=0** znamená, že plánovač nebude spúšťať overovanie klientov v pravidelných intervaloch a zaregistrovaní klienti budú overení pri spustení. V takých prípadoch je možné klienta overiť manuálne.
report	Vygeneruje zostavu, ktorá má príponu súboru .txt alebo .csv.
restart	Reštartuje klienta TNC, server TNC alebo TNC IPRef.
rmclient	Zruší konfiguráciu klienta TNC.
rmipref	Zruší konfiguráciu TNC IPRef.
rmserver	Zruší konfiguráciu servera TNC.
start	Spustí klienta TNC, server TNC alebo TNC IPRef.
status	Zobrazí stav konfigurácie TNC.
stop	Zastaví klienta TNC, server TNC alebo TNC IPRef.
tncport	Určuje číslo portu, na ktorom načúva server TNC. Predvolená hodnota je 42830.
tncserver	Určuje server TNC, ktorý overuje alebo aktualizuje klientov TNC.
tssserver	Určuje IP alebo názov hostiteľa servera Trusted Surveyor.
update	Nainštaluje opravy na klienta.
verify	Iniciuje manuálne overenie klienta.

Nasledujúca tabuľka uvádza správanie pri nastavení hodnoty *yes* alebo *no* pre podpríkaz **default_policy**:

Tabuľka 16. Výsledky príkazu default_policy

FSpolicy (politika sady súborov)	**default policy=***yes*	**default policy=***no*
Klient TNC patrí do politiky sady súborov s definovanými skupinami dočasných opráv (iFix) a opráv APAR	Predvolená politika bude nahradená opravami iFix a APAR poskytnutými v politike sady súborov.	Predvolená politika sa nepoužíva. Opravy iFix a APAR poskytované v politike sady súborov sa zohľadnia v rámci procesu overovania pre klienta TNC.
Klient TNC patrí do politiky sady súborov bez definovaných skupín iFix a APAR	Predvolená politika sa použije s opravami iFix a APAR počas overovania klienta TNC. V rámci procesu overovania sa použijú iba tie opravy iFix a APAR, ktorých úroveň sa zhoduje s úrovňou klienta TNC.	Predvolená politika sa nepoužíva.

Príznaky

Položka	Popis
-A <advisoryName>	Určuje názov poradenský názov pre zostavu.
-B <buildinfo>	Určuje informácie o zostavení na prípravu zostavy o opráve.

-c	Zobrazí atribúty užívateľa v záznamoch oddelených dvojbodkou nasledovným spôsobom:
	`# názov: atribút1: atribút2: ...`
	`politika: hodnota1: hodnota2: ...`

-C	Určuje, že operácia je pre komponent klienta.
-d *umiestnenie databázového súboru/cesta k adresáru databázy*	Určuje umiestnenie cesty k súboru pre importovanie databázy / určuje umiestnenie cesty k súboru na exportovanie databázy.
-D *rrrr-mm-dd*	Určuje dátum pre konkrétnu položku klienta v histórii protokolovania, kde *rrrr* je rok, *mm* je mesiac a *dd* je deň.
-e *id-emailu* **skupinaip=[±]***g1, g2...*	Určuje e-mailový identifikátor, za ktorým nasleduje zoznam názvov skupín IP oddelených čiarkami.
-E | FAIL | COMPLIANT | ALL |	Určuje udalosť, pre ktorú je potrebné posielať e-maily na nakonfigurovaný ID e-mailu. FAIL- Správy sa odošlú, keď stav overenia klienta je FAILED. COMPLIANT- Správy sa odošlú, keď stav overenia klienta je COMPLIANT. ALL - Správy sa odošlú pre všetky stavy overenia klienta.
-f *názov súboru*	Určuje súbor, z ktorého sa musí čítať certifikát v prípade operácie importovania alebo určuje umiestnenie, na ktorý sa musí zapísať certifikát v prípade operácie exportovania.
-F *fspolicy buildinfo*	Určuje názov politiky súborového systému, za ktorým nasledujú informácie o zostavení. Informácie a zostavení je možné poskytnúť v nasledujúcom formáte: 6100-04-01, kde 6100 predstavuje verziu 6.1, 04 je úroveň údržby a 01 je servisný balík.
-g	Spustiť podpríkaz **clientData** na určenom klientovi TNC. Tento príznak je k dispozícii iba s podpríkazom **clientData**.
-G*názov skupiny ip* **ip=[±]***ip1, ip2...*	Určuje názov skupiny IP, za ktorým nasleduje zoznam IP oddelených čiarkami.
-H	Vypíše protokol histórie.
-i *hostiteľ*	Určuje IP adresu alebo názov hostiteľa.
-I ip=[±]*ip1, ip2...* | [±] hostiteľ1,hostiteľ2...	Určuje IP/názov hostiteľa, ktorý sa musí počas overovania ignorovať.
-k *názov súboru*	Určuje súbor, z ktorého sa musí čítať kľúč certifikátu v prípade operácie importovania.
-l	Zobrazí informácie o snímke na serveri TNC pre určeného klienta TNC. Tento príznak je k dispozícii iba s podpríkazom **clientData**.
-O <openpkggrp>	Určuje názov skupiny openpkg pre politiku.
-p	Vykoná náhľad aktualizácie klienta TNC.
-P <názov politiky>	Určuje názov politiky na prípravu zostavy politiky klienta.
-q	Potlačí informácie hlavičky.
-r *informácie o zostavení*	Vygeneruje zostavu na základe informácií o zostavení. Informácie a zostavení je možné poskytnúť v nasledujúcom formáte: 6100-04-01, kde 6100 predstavuje verziu 6.1, 04 je úroveň údržby a 01 je servisný balík.
-R	Určuje, že operácia je pre komponent IPRef.
-s COMPLIANT | IGNORE | FAILED | ALL	Zobrazí klienta podľa stavu nasledovným spôsobom: **COMPLIANT** Zobrazí aktívnych klientov. **IGNORE** Zobrazí klientov, ktorí sú vylúčení z akéhokoľvek overovania. **FAILED** Zobrazí klientov, ktorých overenie zlyhalo podľa nakonfigurovanej politiky. **ALL** Zobrazí všetkých klientov bez ohľadu na ich stavy.
-S <hostiteľ>	Určuje názov hostiteľa na prípravu zostavy o bezpečnostnej oprave klienta.
-t TRUSTED | UNTRUSTED	Označí špecifikovaného klienta ako dôveryhodného alebo nedôveryhodného. **Poznámka:** Len administrátori systému môžu overovať server alebo klienta ako dôveryhodný alebo nedôveryhodný.
-T	Určuje, že klient môže akceptovať požiadavku z ľubovoľného servera TS, ktorý má platný certifikát.
-u	Odinštaluje dočasnú opravu, ktorá je nainštalovaná na klientovi TNC.

Položka	Popis
-v<*CVEid|ALL*>	Zobrazí bezpečnostné nedostatky pre zaregistrované servisné balíky.
	CVEid
	All Zobrazí všetky bezpečnostné nedostatky pre zaregistrované servisné balíky.
-v<*ifix1, ifix2,...*>	Určuje zoznam dočasných opráv oddelený čiarkami.
-V<*SkupinaIfix*>	Určuje názov skupiny dočasných opráv.
-V <*SkupinaIfix*> autoupdate=<yes|no>	Určuje, či sa majú automaticky aktualizovať opravy ifix pod určeným názvom skupiny ifix.
	Yes Automaticky aktualizuje politiku definovanú pre politiku sady súborov, keď sa prijmú nové opravy ifix na serveri TNC.
	No Určuje, že nové opravy ifix budú manuálne priradené k politike, keď budú prijaté na serveri TNC. Predvolená hodnota je No.

Výstupný stav

Tento príkaz vráti nasledujúce výstupné hodnoty:

Položka	Popis
0	Príkaz bol úspešne vykonaný a boli vykonané všetky vyžadované zmeny.
>0	Vyskytla sa chyba. Vytlačená chybová správa obsahuje ďalšie podrobnosti o type zlyhania.

Príklady

1. Ak chcete spustiť server TNC, zadajte nasledujúci príkaz:
   ```
   psconf start server
   ```
2. Ak chcete pridať politiku súborového systému s názvom 71D_latest pre zostavenie 7100-04-02, zadajte nasledujúci príkaz:
   ```
   psconf add -F 71D_latest 7100-04-02
   ```
3. Ak chcete vymazať politiku súborového systému s názvom 71D_old, zadajte nasledujúci príkaz:
   ```
   psconf delete -F 71D_old
   ```
4. Ak chcete overiť, či klient, ktorý má IP adresu 11.11.11.11,je **dôveryhodný**, zadajte nasledujúci príkaz:
   ```
   psconf certadd -i 11.11.11.11 -t TRUSTED
   ```
5. Ak chcete vymazať klienta, ktorý má IP adresu 11.11.11.11, zo servera, zadajte nasledujúci príkaz:
   ```
   psconf certdel -i 11.11.11.11
   ```
6. Ak chcete overiť informácie o klientovi, ktorý má IP adresu 11.11.11.11, zadajte nasledujúci príkaz:
   ```
   psconf verify -i 11.11.11.11
   ```
7. Ak chcete zobraziť informácie o klientovi, ktorý má IP adresu 11.11.11.11, zadajte nasledujúci príkaz:
   ```
   psconf list -i 11.11.11.11
   ```
8. Ak chcete vygenerovať správu pre klientov so stavom **COMPLIANT**, zadajte nasledujúci príkaz:
   ```
   psconf list -s CPMPLIANT -i ALL
   ```
9. Ak chcete vygenerovať zostavu pre zostavenie 7100-04-02, zadajte nasledujúci príkaz:
   ```
   psconf list -r 7100-04-02
   ```
10. Ak chcete zobraziť históriu pripojení klienta, ktorý má IP adresu 11.11.11.11, zadajte nasledujúci príkaz:
    ```
    psconf list -H -i 11.11.11.11
    ```
11. Ak chcete vymazať položku klienta, ktorý má IP adresu 11.11.11.11 z protokolu histórie, ktorý je starší ako alebo rovný 1. februáru 2009, zadajte nasledujúci príkaz:
    ```
    psconf delete -H -i 11.11.11.11 -D 2009-02-01
    ```
12. Ak chcete importovať klientsky certifikát klienta, ktorý má IP adresu 11.11.11.11, zo servera, zadajte nasledujúci príkaz:
    ```
    psconf import -C -i 11.11.11.11 -f /tmp/client.txt
    ```
13. Ak chcete exportovať certifikát z klienta, zadajte nasledujúci príkaz:

```
psconf export -S -f /tmp/server.txt
```

14. Ak chcete aktualizovať klienta, ktorý má IP adresu 11.11.11.11, na príslušnú úroveň zo servera, zadajte nasledujúci príkaz:
    ```
    psconf update -i 11.11.11.11
    ```
15. Ak chcete zobraziť stavy klienta, zadajte nasledujúci príkaz:
    ```
    psconf status
    ```
16. Ak chcete zobraziť klientsky certifikát, zadajte nasledujúci príkaz:
    ```
    psconf list -C
    ```
17. Ak chcete spustiť klienta, zadajte nasledujúci príkaz:
    ```
    psconf start client
    ```
18. Ak chcete zobraziť informácie o snímke, ktoré získal podpríkaz **clientData**, zadajte nasledujúci príkaz:
    ```
    psconf clientData -l [ip|host]
    ```
19. Ak chcete zobraziť históriu pre klienta TNC, zadajte nasledujúci príkaz:
    ```
    psconf list –H –i [ip|ALL]
    ```

Bezpečnosť

Upozornenie pre užívateľov RBAC a Trusted AIX:

Tento príkaz môže vykonávať privilegované operácie. Len privilegovaní užívatelia môžu spúšťať privilegované operácie. Bližšie informácie o autorizáciách a privilégiách nájdete v Databáze privilegovaných príkazov v časti Bezpečnosť. Zoznam privilégií a autorizácií spojených s týmto príkazom nájdete v informáciách o príkaze **lssecattr** alebo podpríkaze **getcmdattr**

Príkaz pscuiserverctl

Účel

Umožňuje nastaviť voľby servera PowerSC GUI.

Syntax

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]

Príznaky

-r Reštartuje server PowerSC GUI po uplatnení hodnoty parametra.

set
Nastaví alebo získa hodnotu voľby servera PowerSC GUI.

Parametre

httpPort *httpPortno*
Zobraziť alebo nastaviť predvolený port používaný softvérom PowerSC GUI.

httpsPort *httpsPortno*
Zobraziť alebo nastaviť predvolený zabezpečený port používaný softvérom PowerSC GUI.

administratorGroupList *unixgrp1,unixgrp2,...*
Zobraziť alebo nastaviť skupiny systému UNIX, ktoré môžu vykonávať administračné úkony pomocou softvéru PowerSC GUI.

logonGroupList *unixgrp1,unixgrp2,...*
Zobraziť alebo určiť skupiny systému UNIX, ktoré sa môžu prihlásiť do prostredia PowerSC GUI.

powervcKeystoneUrl *powervcKeystoneurl*
Zobraziť alebo nastaviť adresu URL servera skladu kľúčov PowerVC.

QRadarSyslogResponseEnabled on | off
Zobraziť aktuálne nastavenie zaznamenávania do protokolu Syslog z aplikácie PowerSC GUI alebo nastaviť zaznamenávanie do protokolu Syslog na hodnotu on alebo off.

tncServer *tncserver.abc.com*
Zobraziť alebo určiť názov hostiteľa servera TNC. Ak zmeníte názov hostiteľa servera TNC, musíte reštartovať server PowerSC GUI.

Výstupný stav

Tento príkaz vráti nasledujúce výstupné hodnoty:

0 Úspešné dokončenie.

>0 Vyskytla sa chyba.

Príklady

1. Zobrazenie aktuálne nastaveného predvoleného portu používaného aplikáciou PowerSC GUI:
   ```
   pscuiserverctl set httpPort
   ```
2. Nastavenie predvoleného portu pre aplikáciu PowerSC GUI:
   ```
   pscuiserverctl set httpPort 80
   ```
3. Zobrazenie aktuálne nastaveného predvoleného zabezpečeného portu používaného aplikáciou PowerSC GUI:
   ```
   pscuiserverctl set httpsPort
   ```
4. Nastavenie predvoleného zabezpečeného portu pre aplikáciu PowerSC GUI:
   ```
   pscuiserverctl set httpsPort 483
   ```
5. Zobrazenie skupín systému UNIX, ktoré môžu vykonávať administračné úkony v aplikácii PowerSC GUI:
   ```
   pscuiserverctl set administratorGroupList
   ```
6. Nastavenie skupín systému UNIX, ktoré môžu vykonávať administračné úkony v aplikácii PowerSC GUI:
   ```
   pscuiserverctl set administratorGroupList securitygroup1,admingrp1
   ```
7. Zobrazenie skupín systému UNIX, ktoré sa môžu prihlásiť do aplikácie PowerSC GUI:
   ```
   pscuiserverctl set logonGroupList
   ```
8. Nastavenie skupín systému UNIX, ktoré sa môžu prihlásiť do aplikácie PowerSC GUI:
   ```
   pscuiserverctl set logonGroupList unixgroup1,unixgrp2
   ```
9. Zobrazenie adresy URL servera skladu kľúčov PowerVC:
   ```
   pscuiserverctl set powervcKeystoneUrl
   ```
10. Nastavenie adresy URL servera skladu kľúčov PowerVC:
    ```
    pscuiserverctl set powervcKeystoneUrl https://powervc/server/example/
    ```
11. Zobrazenie, či je povolené alebo zakázané zaznamenávanie do protokolu Syslog z aplikácie PowerSC GUI:

```
pscuiserverctl set QRadarSyslogResponseEnabled
```

12. Povolenie alebo zakázanie zaznamenávania do protokolu Syslog z aplikácie PowerSC GUI:

```
pscuiserverctl set QRadarSyslogResponseEnabled on
pscuiserverctl set QRadarSyslogResponseEnabled off
```

13. Zobrazenie názvu hostiteľa servera TNC:

```
pscuiserverctl set tncServer
```

14. Nastavenie názvu hostiteľa servera TNC:

```
pscuiserverctl set tncServer tncserver.abc.com
```

15. Po nastavení názvu hostiteľa servera TNC je potrebné reštartovať aplikáciu PowerSC GUI. Reštartovanie aplikácie PowerSC GUI:

```
pscuiserverctl -r set tncServer tncs1.rs.com
```

Príkaz pscxpert

Účel

Pomáha správcovi systému pri nastavovaní konfigurácie zabezpečenia.

Syntax

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

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

pscxpert -f Profil [**-p**] [**-r**|**-R**]

pscxpert -u [**-p**]

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

pscxpert -t

pscxpert -l <Úroveň> [**-p**] <**-a** *Súbor1* | **-n** *Súbor2* | **-a** *Súbor3* **-n** *Súbor4*>

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

pscxpert -d

Popis

Príkaz **pscxpert** nastavuje rozličné konfiguračné nastavenia systému s cieľom povoliť určenú úroveň zabezpečenia.

Spustením príkazu **pscxpert** s príznakom **-l** môžete rýchlo uplatniť nastavenia bezpečnosti bez toho, že by užívateľ musel nakonfigurovať jednotlivé nastavenia. Napríklad, ak spustíte príkaz **pscxpert -l high**, v systéme sa automaticky uplatnia všetky nastavenia zabezpečenia vysokej úrovne. Ak však príkaz **pscxpert -l** spustíte spolu s príznakmi **-n** a **-a**, nastavenia zabezpečenia sa uložia do súboru určeného parametrom *Súbor*. Príznak **-f** potom uplatní nové konfiguračné nastavenia.

Po výbere prvotných nastavení sa zobrazí ponuka uvádzajúca všetky konfiguračné voľby zabezpečenia súvisiace s vybratou úrovňou zabezpečenia. Tieto voľby môžete akceptovať ako celok alebo ich môžete individuálne povoliť alebo zakázať. Po vykonaní sekundárnych zmien bude príkaz **pscxpert** pokračovať v uplatňovaní nastavení zabezpečenia v počítačovom systéme.

Príkaz **pscxpert** spustite ako užívateľ root cieľového systému Virtual I/O Server. Ak nie ste prihlásený ako užívateľ root cieľového systému Virtual I/O Server, pred spustením tohto príkazu spustite príkaz **oem_setup_env**.

Keď príkaz **pscxpert** spustíte vtedy, keď beží iná inštancia príkazu **pscxpert**, príkaz **pscxpert** sa ukončí s chybovým hlásením.

Poznámka: Po významných zmenách v systéme, napríklad po inštalácii alebo inovovaní softvéru, znova spustite príkaz **pscxpert**. Ak nevyberiete konkrétnu položku konfigurácie zabezpečenia pri opätovnom spustení príkazu **pscxpert**, daná položka konfigurácie sa vynechá.

Príznaky

Položka	Popis
-a	Nastavenia so súvisiacimi voľbami úrovne zabezpečenia sa zapíšu do určeného súboru v skrátenom tvare.
-c	Skontroluje nastavenia zabezpečenia v porovnaní s predtým uplatnenou množinou pravidiel. Ak kontrola pravidla zlyhá, skontrolujú sa aj predchádzajúce verzie pravidla. V tomto procese sa bude pokračovať, kým kontrola nebude úspešná alebo kým sa neskontrolujú všetky výskyty neúspešného pravidla v súbore /etc/security/aixpert/core/appliedaixpert.xml. Túto kontrolu môžete spustiť pre ľubovoľný predvolený alebo vlastný profil.
-d	Zobrazí definíciu typu dokumentu (DTD).
-f	Uplatní nastavenia zabezpečenia poskytnuté v určenom súbore *Profil*. Profily sa nachádzajú v adresári /etc/security/aixpert/custom. Dostupné profily zahrňujú nasledujúce štandardné profily: **DataBase.xml** Tento súbor obsahuje požadované predvolené nastavenia databázy. **DoD.xml** Tento súbor obsahuje požadované nastavenia pre STIG (Security Technical Implementation Guide) Ministerstva obrany USA. **DoD_to_AIXDefault.xml** Tento profil obnoví predvolené nastavenia systému AIX. **DoDv2.xml** Tento súbor obsahuje požadované nastavenia pre verziu 2 normy STIG (Security Technical Implementation Guide) Ministerstva obrany USA. **DoDv2_to_AIXDefault.xml** Tento profil obnoví predvolené nastavenia systému AIX. **Hipaa.xml** Tento súbor obsahuje požadované nastavenia pre normu HIPAA (Health Insurance Portability and Accountability Act). **NERC.xml** Tento súbor obsahuje požadované nastavenia pre normu NERC (North American Electric Reliability Corporation). **NERC_to_AIXDefault.xml** Tento profil obnoví predvolené nastavenia systému AIX z nastavení pre NERC. **PCI.xml** Tento súbor obsahuje požadované nastavenia pre normu PCI DSS (Payment Card Industry Data Security Standard). **PCIv3.xml** Tento súbor obsahuje požadované nastavenia pre normu PCI DSS (Payment Card Industry Data Security Standard) verzie 3. **PCI_to_AIXDefault.xml** Tento profil obnoví predvolené nastavenia systému AIX. **PCIv3_to_AIXDefault.xml** Tento profil obnoví predvolené nastavenia systému AIX. **SOX-COBIT.xml** Tento súbor obsahuje požadované nastavenia pre Sarbanes-Oxley Act a COBIT.

Položka	Popis
	Môžete tiež vytvoriť svoje vlastné profily v tom istom adresári a uplatniť ich na nastavenia, a to premenovaním alebo úpravou existujúcich súborov XML. Napríklad, zadaním nasledujúceho príkazu uplatníte profil HIPAA vo vašom systéme: `pscxpert -f /etc/security/aixpert/custom/Hipaa.xml` Keď uvediete príznak **-f**, nastavenia zabezpečenia sa konzistentne uplatnia v jednotlivých systémoch bezpečným prenosom a uplatnením súboru **appliedaixpert.xml** v týchto systémoch. Všetky úspešne uplatnené pravidlá sa zapíšu do súboru /etc/security/aixpert/core/appliedaixpert.xml a príslušné pravidlá akcie undo sa zapíšu do súboru /etc/security/aixpert/core/undo.xml.
-l	Nastaví určenú úroveň nastavení zabezpečenia systému. Tento príznak má nasledujúce voľby: **h|high** Určuje voľby zabezpečenia vysokej úrovne. **m|medium** Určuje voľby zabezpečenia strednej úrovne. **l|low** Určuje voľby zabezpečenia nízkej úrovne. **d|default** Určuje voľby zabezpečenia na úrovni štandardov systému AIX. **s|sox-cobit** Určuje voľby zabezpečenia v súlade so zákonom Sarbanes-Oxley Act a COBIT. Ak uvediete voľbu **-l** aj **-n**, nastavenia zabezpečenia sa neuplatnia v systéme, iba sa zapíšu do určeného súboru. Všetky úspešne uplatnené pravidlá sa zapíšu do súboru /etc/security/aixpert/core/appliedaixpert.xml a príslušné pravidlá akcie undo sa zapíšu do súboru /etc/security/aixpert/core/undo.xml. **Upozornenie:** Keď uvediete príznak **d|default**, tento príznak môže prepísať nakonfigurované nastavenia zabezpečenia, ktoré ste predtým nastavili pomocou príkazu **pscxpert** alebo nezávisle, a obnoví tradičnú otvorenú konfiguráciu systému.
-n	Zapíše nastavenia s príslušnými voľbami úrovne zabezpečenia do určeného súboru.
-p	Určuje, že sa má zobraziť podrobný výstup z bezpečnostných pravidiel. Príznak **-p** zapíše pravidlá spracované v podsystéme auditu, ak je povolená voľba **auditing**. Túto voľbu môžete použiť spolu s príznakmi **-l**, **-u**, **-c** a **-f**. Príznak **-p** povolí podrobný výstup do terminálu aj súboru aixpert.log.
-P	Akceptuje názov profilu ako vstup. Táto voľba sa používa spolu s príznakom **-c**. Príznaky **-c** a **-P** slúžia na kontrolu kompatibility systému s príslušným profilom.
-r	Zapíše existujúce nastavenia systému do súboru /etc/security/aixpert/check_report.txt. Tento výstup môžete použiť v správach z auditu zabezpečenia a súladu. Táto správa popisuje každé nastavenie, vzťah nastavenia k požiadavke súladu s regulačnými nariadeniami a informácie o úspešnosti kontroly. **Poznámka:** • Príznak -r podporuje operáciu uplatnenia iba pre profily. Nepodporuje operáciu uplatnenia pre úrovne. • Voľba -r zobrazí celú správu (jeden alebo viacero riadkov) pre pravidlo.
-R	Vráti rovnaký výstup ako príznak **-r**. Okrem toho tento príznak pripojí aj popis skriptu alebo programu pravidla používaného na implementáciu konfiguračného nastavenia. **Poznámka:** • Príznak -R podporuje operáciu uplatnenia iba pre profily. Nepodporuje operáciu uplatnenia pre úrovne.
-t	Zobrazí typ profilu uplatneného v systéme.
-u	Zruší uplatnené nastavenia zabezpečenia. **Poznámka:** • Pomocou prízknaku **-u** nemôžete zrušiť uplatnenie profilov DoD, DoDv2, NERC, PCI a PCIv3. Tieto profily môžete odstrániť uplatnením profilu končiaceho _AIXDefault.xml. Napríklad, ak chcete odstrániť profil NERC.xml, musíte uplatniť profil NERC_to_AIXDefault.xml. • Zmeny v systéme vykonané operáciou uplatnenia sa stratia po vykonaní operácie zrušenia. Obnovia sa nastavenia spred operácie uplatnenia.

Parametre

Položka	Popis
Súbor	Výstupný súbor, do ktorého sa majú uložiť nastavenia zabezpečenia. Na prístup k tomuto súboru sa vyžadujú oprávnenia užívateľa root.
Úroveň	Vlastná úroveň, ktorá sa má overiť vzhľadom na predtým uplatnené nastavenia.
Profil	Názov súboru profilu poskytujúceho pravidlá súladu pre systém. Na prístup k tomuto súboru sa vyžadujú oprávnenia užívateľa root.

Bezpečnosť

Príkaz **pscxpert** môže spustiť iba užívateľ root.

Príklady

1. Zápis všetkých bezpečnostných volieb vysokej úrovne do výstupného súboru:

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

   Po spustení tohto súboru môžete upraviť výstupný a konkrétne bezpečnostné roly môžete zakázať uzavretím týchto položiek do štandardného reťazca komentára XML <-- označuje začiatok komentára a -\> označuje jeho koniec).
2. Uplatnenie nastavení zabezpečenia z konfiguračného súboru STIG Ministerstva obrany USA:

   ```
   pscxpert -f /etc/security/aixpert/custom/DoD.xml
   ```
3. Uplatnenie nastavení zabezpečenia z konfiguračného súboru HIPAA:

   ```
   pscxpert -f /etc/security/aixpert/custom/Hipaa.xml
   ```
4. Kontrola nastavení zabezpečenia systému a zapísanie neúspešných pravidiel do podsystému auditu:

   ```
   pscxpert -c -p
   ```
5. Kontrola vlastnej úrovne nastavení zabezpečenia pre profil NERC v systéme a zapísanie neúspešných pravidiel do podsystému auditu:

   ```
   pscxpert -c -p -l NERC
   ```
6. Vygenerovanie zostáv a ich zápis do súboru /etc/security/aixpert/check_report.txt:

   ```
   pscxpert -c -r
   ```

Umiestnenie

Položka	Popis
/usr/sbin/pscxpert	Obsahuje príkaz **pscxpert**.

Súbory

Položka	Popis
/etc/security/aixpert/log/aixpert.log	Obsahuje protokol zo sledovania uplatnených nastavení zabezpečenia. Tento súbor nepoužíva štandard syslog. Príkaz **pscxpert** zapisuje priamo do súboru, má oprávnenia na čítanie a zápis a vyžaduje oprávnenia užívateľa root.
/etc/security/aixpert/log/firstboot.log	Obsahuje protokol zo sledovania nastavení zabezpečenia, ktoré boli uplatnené počas prvého zavedenia systému s inštaláciou Secure by Default (SbD).
/etc/security/aixpert/core/undo.xml	Obsahuje zoznam nastavení zabezpečenia, ktoré nemožno zrušiť, vo formáte XML.

príkaz rmvfilt

Účel

Odstráni pravidlá filtra virtuálneho kríženia LAN pre tabuľku filtrov.

Syntax

rmvfilt -n [**fid|all>**]

Popis

Príkaz **rmvfilt** sa používa na odstránenie pravidiel filtra virtuálneho kríženia LAN pre tabuľku filtrov.

Príznaky

-n Určuje ID pravidla filtra, ktoré sa odstráni. Voľba **all** sa používa na odstránenie všetkých pravidiel filtrov.

Výstupný stav

Tento príkaz vráti nasledujúce výstupné hodnoty:

0 Úspešné dokončenie.

>0 Vyskytla sa chyba.

Príklady

1. Ak chcete odstrániť všetky pravidlá filtra alebo deaktivovať všetky pravidlá filtra v jadre, zadajte príkaz takto:

```
rmvfilt -n all
```

Súvisiace koncepty:

"Deaktivovanie pravidiel" na strane 109
Môžete deaktivovať pravidlá, ktoré povoľujú krížové smerovanie VLAN vo funkcii Trusted Firewall.

Príkaz vlantfw

Účel

Zobrazí alebo vymaže informácie o mapovaní IP a Media Access Control (MAC) a riadi funkciu mapovania.

Syntax

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

Popis

Príkaz **vlantfw** zobrazí alebo vymaže položky mapovania IP a MAC. Poskytuje tiež možnosť spúšťať alebo zastavovať zariadenie na protokolovanie Trusted Firewall.

Príznaky

-d Zobrazí všetky informácie o mapovaní IP.

-D Zobrazí zhromaždené údaje o pripojení.

-E Zobrazí údaje o pripojení medzi logickými oddielmi (LPAR) na rôznych centrálnych procesorových komplexoch.

-f Odstráni všetky informácie o mapovaní IP.

-F Vymaže pamäť cache údajov o pripojení.

-G Zobrazí pravidlá filtrov, ktoré možno nakonfigurovať na smerovanie premávky interne s použitím funkcie Trusted Firewall.

-l Zobrazí údaje o pripojení medzi oddielmi LPAR, ktoré sú priradené rôznym ID VLAN, ale zdieľajú rovnaké centrálne procesorové komplexy.

-l Spustí zariadenie na protokolovanie Trusted Firewall.

-L Zastaví zariadenie na protokolovanie Trusted Firewall a presmeruje obsah súboru sledovania do súboru /home/padmin/svm/svm.log.

-m Povolí monitorovanie Trusted Firewall.

-M Zakáže monitorovanie Trusted Firewall.

-q Dotazuje stav bezpečného virtuálneho počítača.

-s Spustí Trusted Firewall.

-t Zastaví Trusted Firewall.

Parametre

-N *celé číslo*
Zobrazí pravidlo filtra, ktoré zodpovedá celému číslu, ktoré je zadané.

Výstupný stav

Tento príkaz vráti nasledujúce výstupné hodnoty:

0 Úspešné dokončenie.

>0 Vyskytla sa chyba.

Príklady

1. Ak chcete zobraziť všetky mapovania IP, zadajte príkaz takto:
   ```
   vlantfw -d
   ```
2. Ak chcete odstrániť všetky mapovania IP, zadajte príkaz takto:
   ```
   vlantfw -f
   ```
3. Ak chcete spustiť funkciu protokolovania Trusted Firewall, zadajte príkaz takto:
   ```
   vlantfw -l
   ```
4. Ak chcete skontrolovať stav bezpečného virtuálneho počítača, zadajte príkaz takto:
   ```
   vlantfw -q
   ```
5. Ak chcete spustiť dôveryhodný firewall, zadajte príkaz takto:
   ```
   vlantfw -s
   ```
6. Ak chcete zastaviť dôveryhodný firewall, zadajte príkaz takto:
   ```
   vlantfw -t
   ```
7. Ak chcete zobraziť zodpovedajúce pravidlá, ktoré možno použiť na generovanie filtrov, ktoré smerujú premávku v rámci centrálneho procesorového komplexu, zadajte príkaz nasledovne:
   ```
   vlantfw -G
   ```

Súvisiaci odkaz:

“príkaz genvfilt” na strane 150

Vyhlásenia

Tieto informácie sa vzťahujú na produkty a služby ponúkané v USA.

Produkty, služby alebo súčasti popisované v tomto dokumente nemusí spoločnosť IBM ponúkať v iných krajinách. Informácie o produktoch a službách, ktoré sú k dispozícii vo vašej krajine, vám poskytne miestny zástupca spoločnosti IBM. Žiadny odkaz na produkt, program alebo službu spoločnosti IBM neznamená ani nenaznačuje, že je možné použiť len tento produkt, program alebo službu spoločnosti IBM. Namiesto nich je možné použiť ľubovoľný funkčne rovnocenný produkt, program alebo službu, ktoré neporušujú žiadne právo duševného vlastníctva spoločnosti IBM. Je však na zodpovednosti užívateľa zhodnotiť a overiť si funkčnosť ľubovoľného produktu, programu alebo služby nepochádzajúcich od spoločnosti IBM.

Spoločnosť IBM môže mať patenty alebo prihlášky patentov čakajúce na spracovanie, ktoré sa týkajú predmetu tohto dokumentu. Získaním tohto dokumentu nezískavate licenciu na tieto patenty. Otázky týkajúce sa licencií môžete posielať písomne na adresu:

IBM Director of Licensing
IBM Corporation
North Castle Drive, MD-NC119
Armonk, NY 10504-1785
USA

V prípade otázok týkajúcich sa licencie na dvojbajtové informácie (DBCS) kontaktujte oddelenie intelektuálneho vlastníctva spoločnosti IBM Intellectual Property Department vo vašej krajine alebo ich pošlite písomne na adresu:

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

SPOLOČNOSŤ INTERNATIONAL BUSINESS MACHINES POSKYTUJE TÚTO PUBLIKÁCIU „TAK, AKO JE“, BEZ AKÝCHKOĽVEK VÝSLOVNÝCH ALEBO MLČKY PREDPOKLADANÝCH ZÁRUK VRÁTANE, ALE BEZ OBMEDZENIA NA, PREDPOKLADANÝCH ZÁRUK NEPORUŠENIA PRÁV, PREDAJNOSTI ALEBO VHODNOSTI NA KONKRÉTNY ÚČEL. Niektoré štáty nepovoľujú zrieknutie sa výslovných, ani mlčky predpokladaných záruk pri konkrétnych transakciách, preto sa na vás toto vyhlásenie nemusí vzťahovať.

Tieto informácie môžu obsahovať technické nepresnosti alebo tlačové chyby. Informácie uvedené v tomto dokumente podliehajú pravidelným zmenám. Tieto zmeny budú zapracované do nových vydaní publikácie. Spoločnosť IBM môže kedykoľvek a bez prechádzajúceho upozornenia vykonať vylepšenia alebo zmeny v produktoch alebo programoch popísaných v tejto publikácii.

Akékoľvek odkazy na iné webové stránky než stránky spoločnosti IBM sa v tejto publikácii poskytujú len pre vaše pohodlie a v žiadnom prípade sa nemôžu chápať ako prejav súhlasu s obsahom týchto webových stránok. Materiály na týchto webových stránkach nie sú súčasťou materiálov k tomuto produktu spoločnosti IBM a ich použitie je výhradne na vaše vlastné riziko.

Spoločnosť IBM môže ľubovoľné vami poskytnuté informácie použiť alebo rozširovať spôsobom, ktorý uzná za vhodný, bez toho, aby jej tým vznikli akékoľvek záväzky voči vám.

Držitelia licencií na tento program, ktorí chcú získať informácie o tomto programe na účely povolenia: (i) výmeny informácií medzi nezávisle vytvorenými programami a inými programami (vrátane tohto programu) a (ii) vzájomného využívania vymenených informácií, by mali kontaktovať:

IBM Director of Licensing
IBM Corporation
North Castle Drive, MD-NC119
Armonk, NY 10504-1785
USA

Takéto informácie môžu byť dostupné (v súlade s príslušnými podmienkami používania, čo v niektorých prípadoch zahŕňa zaplatenie poplatku).

Spoločnosť IBM poskytuje licenčný program popísaný v tomto dokumente a všetky dostupné súvisiace licenčné materiály na základe podmienok zmluvy IBM Customer Agreement, zmluvy IBM International Program License Agreement alebo akejkoľvek rovnocennej zmluvy uzatvorenej medzi nami.

Údaje o výkone a príklady použitia uvedené v tomto dokumente slúžia výhradne na ilustratívne účely. Skutočný výkon sa môže líšiť v závislosti od konkrétnych konfigurácií a prevádzkových podmienok.

Informácie o produktoch od iných spoločností ako IBM boli získané od dodávateľov týchto produktov, z nimi publikovaných oznámení alebo z iných verejne dostupných zdrojov. Spoločnosť IBM tieto produkty netestovala a nemôže potvrdiť presnosť vyhlásení týkajúcich sa ich výkonu, kompatibility ani iných vyhlásení súvisiacich s produktmi nepochádzajúcimi od spoločnosti IBM. Otázky týkajúce sa schopností produktov, ktoré nepochádzajú od spoločnosti IBM, by ste mali adresovať dodávateľom týchto produktov.

Všetky vyhlásenia týkajúce sa budúceho smerovania alebo zámerov spoločnosti IBM môžu byť bez upozornenia zmenené alebo zrušené a predstavujú len ciele a zámery.

Všetky uvedené ceny stanovené spoločnosťou IBM predstavujú odporúčané maloobchodné ceny IBM, sú aktuálne a môžu sa zmeniť bez predchádzajúceho upozornenia. Ceny u jednotlivých predajcov sa môžu líšiť.

Tieto informácie sú určené len na účely plánovania. Tu uvedené informácie sa môžu zmeniť pred uvedením popisovaných produktov.

Tieto informácie obsahujú príklady údajov a zostáv, aké sa používajú v bežnej podnikovej praxi. V záujme čo najvyššej názornosti tieto príklady obsahujú mená osôb, názvy spoločností, pobočiek a produktov. . Všetky tieto mená a názvy sú fiktívne a akákoľvek podobnosť s menami, názvami a adresami skutočných ľudí alebo firiem je celkom náhodná.

LICENCIA NA AUTORSKÉ PRÁVA:

Tieto informácie obsahujú vzorové aplikačné programy v zdrojovom jazyku, ktoré demonštrujú programovacie techniky v rozličných operačných platformách. Tieto vzorové programy môžete kopírovať, upravovať a distribuovať za účelom vývoja, používania, podpory predaja alebo distribuovania aplikačných programov vyhovujúcich aplikačnému programovému rozhraniu operačnej platformy, pre ktorú boli tieto vzorové programy napísané, a to v akejkoľvek forme a bez toho, že by vám tým vznikol finančný záväzok voči spoločnosti IBM. Tieto vzorové programy neboli dôkladne testované za všetkých podmienok. Spoločnosť IBM preto nemôže zaručiť ani predpokladať spoľahlivosť, prevádzkyschopnosť alebo funkčnosť týchto programov. Tieto vzorové programy sa poskytujú „TAK, AKO SÚ“ bez záruky akéhokoľvek druhu. Spoločnosť IBM nebude niesť zodpovednosť za žiadne škody, ktoré vzniknú v dôsledku používania týchto vzorových programov.

Každá kópia alebo ľubovoľná časť týchto vzorových programov alebo ľubovoľných odvodených diel musí obsahovať nasledujúce vyhlásenie o autorských právach:

© (názov vašej spoločnosti) (rok).

Časti tohto kódu sú odvodené zo Vzorových programov spoločnosti IBM Corp.

© Copyright IBM Corp. _uveďte rok alebo roky_.

Hľadiská politiky ochrany osobných údajov

V softvérových produktoch IBM vrátane riešení SaaS (Software as a Service) („Ponuky softvéru“) sa môžu používať objekty cookie a iné technológie s cieľom zhromažďovať informácie o používaní produktu, zlepšiť skúsenosti koncových užívateľov, prispôsobiť komunikáciu s koncovými užívateľmi a iné účely. Vo väčšine prípadov tieto Ponuky softvéru nezhromažďujú žiadne informácie umožňujúce identifikáciu osôb. Niektoré Ponuky softvéru vám môžu umožňovať zhromažďovanie informácií umožňujúcich identifikáciu osôb. Ak táto Ponuka softvéru používa objekty cookie s cieľom zhromažďovať informácie umožňujúce identifikáciu osôb, nižšie nájdete podrobné informácie o tom, ako táto ponuka používa objekty cookie.

Táto Ponuka softvéru nepoužíva objekty cookie alebo iné technológie s cieľom zhromažďovať informácie umožňujúce identifikáciu osôb.

Ak nasadené konfigurácie tejto Ponuky softvéru umožňujú vám ako zákazníkovi zhromažďovať informácie umožňujúce identifikáciu osôb od koncových užívateľov prostredníctvom objektov cookie alebo iných technológií, mali by ste požiadať o právnu pomoc v súvislosti s právnymi predpismi, ktoré sa vzťahujú na takéto zhromažďovanie údajov vrátane požiadaviek týkajúcich sa upozornenia na toto zhromažďovanie informácií a súhlasu s ním.

Bližšie informácie o používaní rozličných technológií vrátane objektov cookie na tieto účely nájdete v dokumente Zásady ochrany osobných údajov spoločnosti IBM na adrese http://www.ibm.com/privacy a Vyhlásenie o online ochrane osobných údajov IBM na adrese http://www.ibm.com/privacy/details v časti s názvom „Objekty cookie, Web Beacon a iné technológie“ a v dokumente „Vyhlásenie o ochrane osobných údajov v softvérových produktoch a ponukách SaaS spoločnosti IBM“ na adrese http://www.ibm.com/software/info/product-privacy.

Ochranné známky

IBM, logo IBM a ibm.com sú ochranné známky alebo registrované ochranné známky spoločnosti International Business Machines Corp., zaregistrované v mnohých krajinách. Ďalšie názvy produktov a služieb môžu byť ochranné známky spoločnosti IBM alebo iných spoločností. Aktuálny zoznam ochranných známok spoločnosti IBM je k dispozícii na stránke Informácie o autorských právach a ochranných známkach na adrese www.ibm.com/legal/copytrade.shtml.

Linux je registrovaná ochranná známka Linusa Torvaldsa v Spojených štátoch alebo iných krajinách.

Java a všetky ochranné známky a logá súvisiace so značkou Java sú ochranné známky alebo registrované ochranné známky spoločnosti Oracle alebo jej pridružených spoločností.

Index

A

AIX syslog 113
Aktualizácia klienta TNC 124
Aktualizácia neúspešného pravidla 90
Aspekty migrácie 99
Atestácia systému 100

B

bezpečná komunikácia 116
bezpečnosť
    PowerSC
        Real-Time Compliance 95

C

cURL 115, 117

D

Dôveryhodné spustenie 97, 99, 100, 101

E

e-mailové oznámenie 121

F

funkcia
    PowerSC Real Time Compliance 95

G

grafické užívateľské rozhranie
    agent 130
    bezpečnosť 129
    inštalácia 130
    obnovenie RTC so staršou časovou značkou 143
    obnovenie súborov RTC z predchádzajúcej konfigurácie monitorovania 144
    profily súladu 138
    určenie skupín koncových bodov 132

H

hardvérové a softvérové požiadavky 5

I

importovať certifikáty 116
Importovať certifikáty 125
inštalácia 118
Inštalácia 7
Inštalácia funkcie Trusted Boot 99
Inštalácia kolektora 99
Inštalácia overovateľa 99
Inštalácia PowerSC Standard Edition 7
Interpretovanie výsledkov atestácie 100

K

Klient TNC 116
Klientske politiky 123
Komponenty 115
Konfigurácia 119
Konfigurácia funkcie Security and Compliance Automation softvéru PowerSC 91
Konfigurácia funkcie Trusted Boot 99
Konfigurácia funkcie Trusted Logging 112, 113
Konfigurácia klienta 119
Konfigurácia servera 119
Konfigurácia servera na správu opráv 120

M

Moduly IMC a IMV 117
Monitorovanie systémov pre trvalý súlad s požiadavkami 91

N

Nástroj na hlásenie a správu pre TNCPM
    použitie príkazu pmconf 153
Nástroj na nahlasovanie a správu pre TNC, SUMA
    použitie príkazu psconf 157
Nevyhnutné podmienky 98

O

Odkazovač IP 116
Odkazujúci server IP na serveri VIOS 122
Odstraňovanie systémov 101
Overenie klienta 124

P

Plánovanie 97
pmconf 116
Podsystém AIX Audit 112
PowerSC 10, 81, 89, 91
    Real-Time Compliance 95
    Trusted Firewall
        deaktivovanie pravidiel 109
        inštalácia 105
        konfigurovanie 106
        konfigurovanie s viacerými SEA 107
        odstránenie adaptérov SEA 108
        vytváranie pravidiel 108
    Trusted Logging
        inštalácia 112
PowerSC Standard Edition 5, 7
prehľad 5, 115
Prezeranie protokolov 122
Prezeranie virtuálnych protokolových zariadení 111
Prezeranie výsledkov overovania 124
príkaz genvfilt 150
príkaz chvfilt 149

príkaz lsvfilt 151
príkaz mkvfilt 152
príkaz pmconf 153
Príkaz pscon 157
príkaz pscuiserverctl 164
príkaz pscxpert 166
príkaz rmvfilt 169
príkaz vlantfw 170
Príkazy
  genvfilt 150
  chvfilt 149
  lsvfilt 151
  mkvfilt 152
  pscuiserverctl 164
  rmvfilt 169
  vlantfw 170
Príprava na nápravu 98
Protokol 117

R

Real-Time Compliance 95
registrácia systému 99
riešenie problémov 101
Riešenie problémov s funkciou TNC a správou opráv 126
Rozhranie GUI
  jazyk 135
  klonovanie skupín koncových bodov 138
  komunikácia medzi koncovými bodmi a serverom 135
  koncový bod 130
  Konfigurácia RTC 143
  konfigurácia TE 144
  kontrola profilov súladu s nariadeniami 141
  kopírovanie konfiguračných volieb RTC na skupiny 143, 145
  kopírovanie profilov na koncové body 139
  kopírovanie TE volieb monitorovania zoznamu súborov na iné skupiny 145
  kopírovanie volieb monitorovania zoznamu súborov RTC na iné skupiny 144
  monitorovanie bezpečnosti koncových bodov 142
  navigácia 135
  odstraňovanie koncových bodov 136
  odstránenie skupín koncových bodov 137
  odstránenie vlastných profilov 139
  overenie komunikácie medzi koncovými bodmi a serverom 135
  overenie požiadaviek na sklad kľúčov 136
  oznámenie o bezpečnostnej udalosti 147
  oznámenie o udalosti súladu s nariadeniami 142
  použitie 133
  použitie profilov súladu s nariadeniami 140
  požiadavky 131
  požiadavky na generovanie sklad kľúčov 136
  premenovanie skupiny koncových bodov 138
  prepínanie monitorovania TE 146
  pridanie koncových bodov do skupiny 137
  server 131
  spustenie bezpečnostných certifikátov 132
  spustenie kontroly RTC 144
  spustenie skupinových skriptov 133
  úprava zoznamu súborov RTC 143
  úprava zoznamu súborov TE 145
  úvod 129
  vlastné skupiny koncových bodov 137
  vytváranie bezpečnostných certifikátov 131
  vytváranie profilov súladu s nariadeniami 139
  zobrazenie profilov súladu s nariadeniami 138
  zobraziť stav produktov PowerSC 146
Rozhranie GUI *(pokračovanie)*
  zoskupenie koncových bodov 137
  zrušenie použitia profilov súladu s nariadeniami 141

S

Server 115
server Trusted Network Connect 121
Server Trusted Network Connect 122
SOX a COBIT 81
Správa automatizácie bezpečnosti a súladu s požiadavkami 90
Správa automatizácie bezpečnosti a zabezpečenia súladu s požiadavkami 90, 91
Správa funkcie Security and Compliance Automation 89
Správa funkcie Trusted Boot 100
Správa komponentov TNC 122
správa opráv 116
Správa opráv 115, 116, 117
Správa politík 125
SUMA 115, 116, 117
Súlad s predpismi STIG Ministerstva obrany USA 10

T

Testovanie aplikácií 91
TNC 126
Trusted Boot 97, 98, 99, 100, 101
Trusted Firewall 103
  deaktivovanie pravidiel 109
  inštalácia 105
  konfigurovanie 106
    viaceré SEA 107
  odstránenie
    adaptéry SEA 108
  vytváranie pravidiel 108
Trusted Logging 111, 113
  inštalácia 112
Trusted Logging - prehľad 111
Trusted network Connect 124
Trusted Network Connect 115, 116, 117, 118, 119, 120, 122, 123, 124, 125
Trusted Network Connect and Patch management 115

V

virtuálne protokoly 111
Vyhľadanie neúspešného pravidla 90

Z

Zapisovanie údajov do virtuálnych protokolových zariadení 113
základné pojmy 115
Základné pojmy pre Trusted Boot 97
Základné pojmy pre Trusted Firewall 103
zostavy
  distribúcia 148
  práca s 147
  výber skupiny pre zostavu 147

Vytlačené v USA