IBM PowerSC

Standard Edition

Verzia 1.1.3

PowerSC Standard Edition

IBM PowerSC

Standard Edition

Verzia 1.1.3

PowerSC Standard Edition

Poznámka

Pred použitím týchto informácií a produktu, ktoré podporujú, si prečítajte informácie v časti “Vyhlásenia” na strane 45.

Toto vydanie sa zvzťahuje na produkt IBM PowerSC, verzia 1.1.3, a na všetky následné vydania a modifikácie, pokiaľ v nových vydaniach nebude uvedené inak.

Obsah

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 použité systémy s certifikáciou kvality ISO 9000.

IBM PowerSC Standard Edition 1.1.3

IBM® PowerSC Standard Edition obsahuje funkcie Trusted Boot, Trusted Firewall, Trusted Logging, Trusted Network Connect a Patch management a Security and Compliance Automation.

Novinky v produkte PowerSC Standard Edition 1.1.3

Prečítajte si o nových alebo výrazne zmenených informáciách v kolekcii tém PowerSC Standard Edition, verzia 1.1.3.

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

December 2013

- Aktualizovať systémové požiadavky v dokumente “PowerSC Standard Edition 1.1.3 - základné pojmy”.
- Identifikovaná vyžadovaná náhrada súborov Trusted Boot pri preinštalovaní operačného systému AIX v dokumente “Nevyhnutné podmienky pre Trusted Boot” na strane 5.
- Pridané informácie o funkcii monitorovania Trusted Firewall v dokumente “Monitorovanie funkcie Trusted Firewall” na strane 12.
- Pridané informácie o funkcii protokolovania Trusted Firewall v dokumente “Protokolovanie funkcie Trusted Firewall” na strane 12.
- Pridaná téma “Inštalácia funkcie Trusted Logging” na strane 17.
- Pridané informácie aktualizáciách dočasnej opravy pre Trusted Network Connect v dokumente “Konfigurácia servera na správu záplat” na strane 22.
- Pridané informácie o nahlasovaní servera Trusted Network Connect v dokumente “Nahlasovanie servera TNC” na strane 27.
- Pridané informácie o inštalácii overovača Trusted Network Connect v dokumente “Inštalácia overovateľa” na strane 6.
- Pridané príkazy Trusted Firewall v dokumente “Príkazy PowerSC Standard Edition” na strane 29.
- Premenovaný príkaz **tscpmconsole** na príkaz **pmconf** a pridané informácie o ňom v dokumente “príkaz pmconf” na strane 33.
- Premenovaný príkaz **tscconsole** na príkaz **psconf** a pridané informácie o ňom v dokumente “Príkaz pscon” na strane 36.
- Aktualizované aktualizácia o voľbách pre príkaz **vlantfw** v dokumente “Príkaz vlantfw” na strane 42.

November 2012

Aktualizované informácie v téme “Trusted Network Connect a Patch management” na strane 19.

Máj 2012

Pridaná dokumentácia pre novú funkciu pre “Trusted Firewall” na strane 9.

PowerSC Standard Edition 1.1.3 - 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	• POWER5 • POWER6 • POWER7
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 • VIOS, verzia 2.2.1.4 alebo novší	• POWER6 • POWER7 • 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	• POWER5 • POWER6 • POWER7
Trusted Network Connect a Patch Management	Overí, či všetky systémy AIX vo virtuálnom prostredí sú na špecifikovanej úrovni softvéru a úrovni záplat 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 záplata, ktorá má vplyv na systém.	• AIX 5.3 • AIX 6.1 • AIX 7.1 Klient Trusted Network Connect vyžaduje jeden z nasledujúcich komponentov: • AIX 6.1 s 6100-06 alebo novší • Systém konzoly AIX, verzia 7.1 Service Update Management Assistant (SUMA) v prostredí SUMA na správu záplat	• POWER5 • POWER6 • POWER7

Inštalácia PowerSC Standard Edition 1.1.3

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

Tieto sady súborov sú k dispozícii pre PowerSC Standard Edition:

- powerscExp.ice: Nainštalovaná v systémoch AIX, ktoré vyžadujú funkciu Security and Compliance Automation v PowerSC Standard Edition.

- powerscStd.vtpm: Nainštalovaná v systémoch AIX, ktoré vyžadujú funkciu Trusted Boot v PowerSC Standard Edition.
- powerscStd.vlog: Nainštalovaná v systémoch AIX, ktoré vyžadujú funkciu Trusted Logging v PowerSC Standard Edition.
- powerscStd.tnc_pm: Nainštalovaná v systéme AIX, verzia 6.1 s technologickou úrovňou 6100-06 alebo vyššom, alebo v konzolovom systéme AIX, verzia 7.1 SUMA (Service Update Management Assistant) v rámci prostredia SUMA pre správu záplat.
- powerscStd.svm: Nainštalovaná v systémoch AIX, ktoré by mohli profitovať z funkcie smerovania v PowerSC Standard Edition.

Inštalovať PowerSC Standard Edition prostredníctvom jedného z týchto 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**.

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 1.1.3 - základné pojmy” na strane 1
Tento prehľad súčasti PowerSC Standard Edition vysvetľuje funkcie, komponenty a hardvérovú podporu týkajúcu sa súčasti PowerSC Standard Edition.

“Inštalácia funkcie Trusted Boot” na strane 6
Existujú určité vyžadované hardvérové a softvérové konfigurácie, ktoré sú potrebné na inštaláciu funkcie Trusted Boot.

“Inštalácia Trusted Network Connect” na strane 21
Inštalácia komponentov TNC (Trusted Network Connect) vyžaduje, aby ste vykonali určité kroky.

Súvisiace úlohy:

“Inštalácia funkcie Trusted Firewall” na strane 11
Inštalácia funkcie PowerSC Trusted Firewall je podobná ako inštalácia funkcií PowerSC.

“Inštalácia funkcie Trusted Logging” na strane 17
Funkciu PowerSC Trusted Logging môžete nainštalovať pomocou rozhrania príkazového riadka alebo nástroja SMIT.

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 Konzola správy hardvéru (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 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 8
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? (Navrhuje sa napríklad zhromažďovať protokoly auditu, odpojiť systém od siete, vypnúť systém a upozorniť užívateľov).

- Boli zasiahnuté nejaké iné systémy, ktoré treba skontrolovať?

Súvisiace koncepty:

“Riešenie problémov s funkciou Trusted Boot” na strane 8
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 1.1.3” na strane 2
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

Konfigurovanie 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
  ```

Riadenie 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 2. 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 2. 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 5
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 4
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.

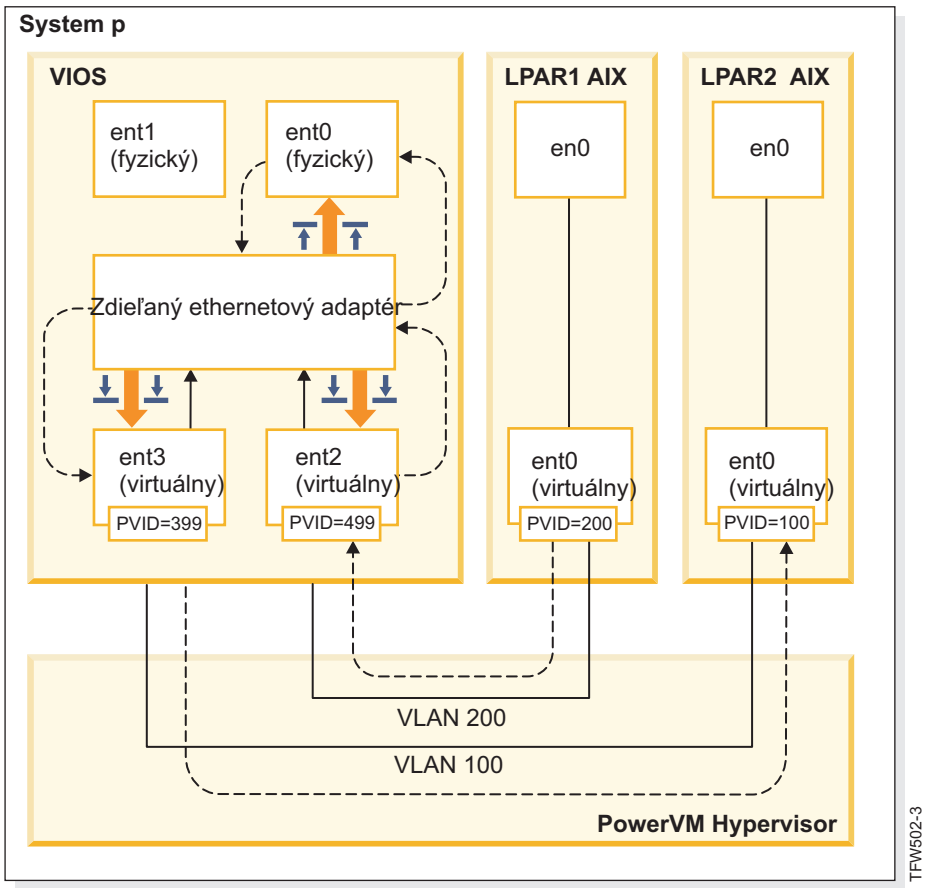
Základné pojmy pre Trusted Firewall

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.

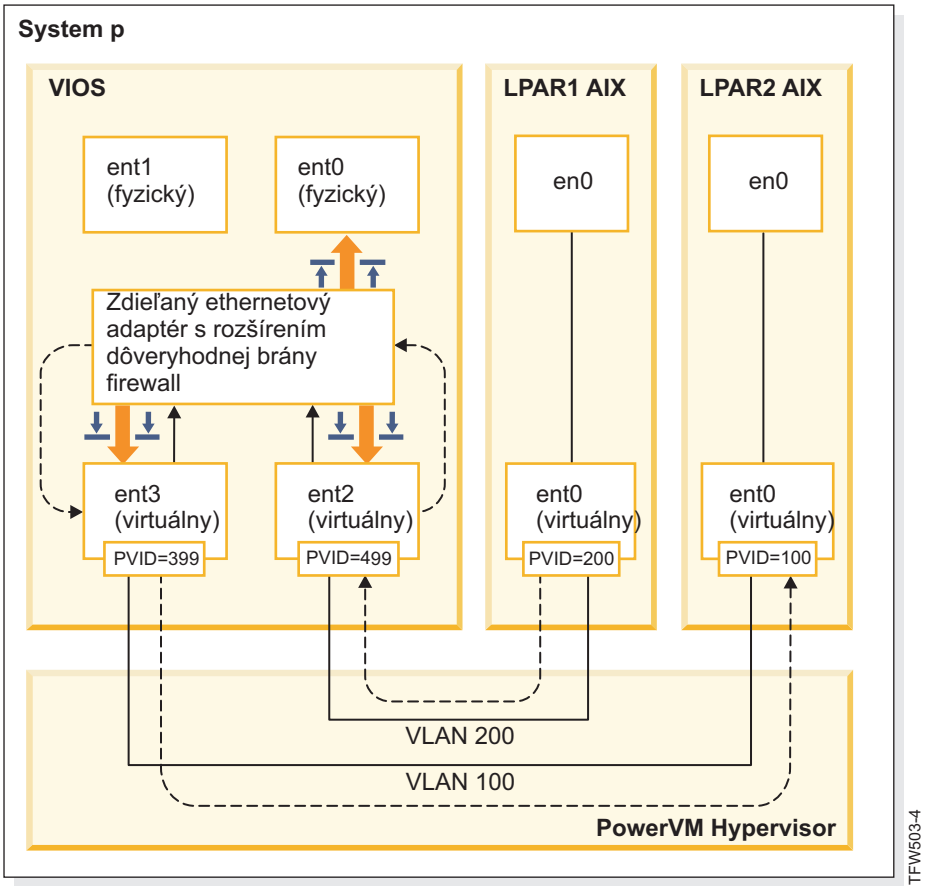
S funkciou Trusted Firewall môžete nakonfigurovať pravidlá, ktoré umožnia určitým druhom premávky porenášať sa priamo z jednej VLAN na systéme Virtual I/O Server (VIOS) na inú VLAN na tom istom systéme VIOS, pričom sa naďalej zachová vysoká úroveň bezpečnosti vďaka obmedzeniu ostatných druhov premávky.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

Pri použití príkladu v dokumente Obrázok 1 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 11.



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 1.1.3" na strane 2
Pre každú špecifickú funkciu PowerSC Standard Edition musíte nainštalovať sadu súborov.

Konfigurovanie funkcie Trusted Firewall

Po nainštalovaní funkcie Trusted Firewall sa vyžadujú ďalšie konfiguračné nastavenia.

Monitorovanie funkcie Trusted Firewall

Monitorovanie funkcie Trusted Firewall analyzuje systémovú premávku z rozličných logických oddielov (LPAR), čím poskytuje užitočné informácie na určenie, či funkcia Trusted Firewall zlepšuje výkon systému.

Ak funkcia monitorovania Trusted Firewall zaznamená výrazný objem premávky z rôznych virtuálnych sietí LAN (sietí VLAN), ktoré sú na tom istom, centrálnom elektronickom komplexe, povolenie funkcie Trusted Firewall by malo vášmu systému prospieť.

Ak chcete povoliť monitorovanie Trusted Firewall, zadajte nasledujúci príkaz:

```
vlantfw -m
```

Ak chcete zobraziť výsledky monitorovania funkcie Trusted Firewall, zadajte nasledujúci príkaz:

```
vlantfw -D
```

Ak chcete zakázať monitorovanie Trusted Firewall, zadajte nasledujúci príkaz:

```
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.

Keď monitorovanie funkcie Trusted Firewall zistí, že smerovaním premávky interne sa zlepšuje efektivita, protokolovanie funkcie Trusted Firewall udržiava zoznam ciest v súbore svm.log. Limit veľkosti súboru svm.log je 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
```

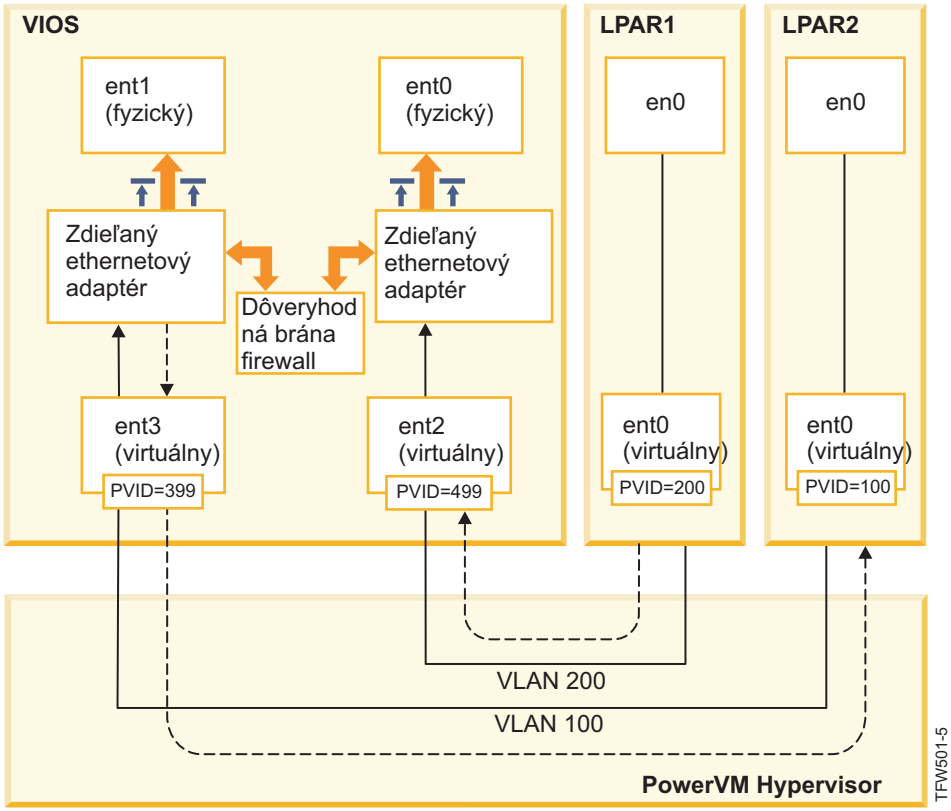
Protokolový súbor nájdete na nasledujúcom umiestnení: /home/padmin/svm/svm.log.

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 filtra, ktoré umožní komunikáciu medzi dvoma oddielmi LPAR (LPAR1 a LPAR2) zadaním jedného z nasledujúcich príkazov:
   - `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 30

“príkaz mkvfilt” na strane 32

“Príkaz vlantfw” na strane 42

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 14
Môžete vytvárať pravidlá, ktoré umožnia smerovanie po sieti VLAN funkciou Trusted Firewall.

Súvisiaci odkaz:

“príkaz lsvfilt” na strane 31

“príkaz rmvfilt” na strane 41

Trusted Logging

Funkcia PowerVM Trusted logging umožňuje systémom AIX LPAR zapisovať do protokolových súborov, ktoré sú uložené na pripojenom systéme 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 konsolidovanie údajov protokolu z viacerých klientskych LPAR do jedného súborového systému, ktorý je dostupný zo systému VIOS. 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

Názvy dvoch komponentov, ktoré môže nastaviť administrátor VIOS na ľubovoľnú hodnotu, ale názov klienta je väčšinou rovnaký pre všetky virtuálne protokoly, ktoré sú pripojené k danému LPAR (napríklad názov hostiteľa 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

Detegovanie 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 1.1.3” na strane 2
Pre každú špecifickú funkciu PowerSC Standard Edition musíte nainštalovať sadu súborov.

Konfigurácia dôveryhodného protokolovania

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 budete konfigurovať podsystém AIX Audit musíte dokončiť procedúru v “Detegovanie virtuálnych protokolových zariadení” na strane 16.

Ak chcete konfigurovať podsystém AIX Audit, postupujte podľa týchto krokov:

1. Konfigurujte 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 budete konfigurovať súbor /etc/syslog.conf musíte dokončiť procedúru v “Detegovanie virtuálnych protokolových zariadení” na strane 16.

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 a Patch management

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

Základné pojmy pre Trusted Network Connect

Zistite viac o komponentoch, konfigurovaní bezpečnej komunikácie a systéme riadenia záplat 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:

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 záplat 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.

Riadenie záplat:

Server TNC sa integruje so SUMA a vytvára riešenie na správu záplat.

AIX SUMA prevezme najnovšie servisné balíky a bezpečnostné opravy dostupné na webovej stránke IBM ECC a Fix Central. TNC a démon na správu záplat automaticky doručí najnovšie aktualizované informácie na server TNC, ktorý slúži ako základná sada súborov na overovanie klientov.

Démon **tncpmd** musí byť nakonfigurovaný tak, aby spravoval preberania SUMA a automaticky doručoval informácie o sade súborov na server TNC. Tento démon musí byť hosťovaný na systéme, ktorý je pripojený na Internet, aby bol schopný preberať aktualizácie automaticky. Ak chcete používať server riadenia záplat TNC bez jeho pripojenia na Internet, môžete zaregistrovať užívateľom definovaný archív opráv so serverom riadenia záplat TNC.

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

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 záplat AIX, čo vytvára kompletné riešenie riadenia záplat.

Špecifikácie TNC musí spĺňať požiadavky architektúry systémov AIX a Rodina produktov POWER. Komponenty TNC slúžia na zabezpečenie komplexného riešenia riadenia záplat na operačnom systéme AIX. Táto konfigurácia umožňuje administrátorom efektívne spravovať softvérovú konfiguráciu na umiestneniach AIX. Poskytuje nástroje na overovanie úrovní záplat systémov a generovanie zostavy na klientoch, ktorí nie sú kompatibilní. Navyše sprava záplat zjednodušuje proces preberania záplat 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 36

Inštalácia Trusted Network Connect

Inštalácia komponentov TNC (Trusted Network Connect) vyžaduje, aby ste vykonali určité kroky.

Ak chcete konfigurovať nastavenie na používanie komponentov TNC, postupujte podľa týchto krokov:

1. Identifikujte IP adresy systémov na nastavenie servera TNC, servera TNCPM (Trusted Network Connect and Patch Management) a odkazujúceho servera TNC IP pre Virtual I/O Server (VIOS).

   Poznámka: Server TNC nemožno konfigurovať ako klienta TNC.
2. Nastavte server NIM (Network Installation Management). Systém, ktorý je nakonfigurovaný ako server je hlavný počítač NIM a v klientskom systéme musia byť nainštalované sady súborov sets:bos.sysmgt.nim.master.
3. Konfigurujte server TNCPM. Táto konfigurácia môže byť nastavená v systéme NIM. Server TNCPM používa SUMA na stiahnutie záplat z webových stránok IBM Fix Central a ECC. 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
   ```
4. Konfigurujte politiky na serveri TNC. Ak chcete vytvoriť politiky na overenie klientov, pozrite si “Vytváranie politík pre klienta Trusted Network Connect” na strane 25.
5. 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.
6. Pomocou tohto príkazu konfigurujte klientov:

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

   Napríklad:

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

Súvisiaci odkaz:

“Príkaz pscon” na strane 36

Súvisiace informácie:

“Inštalácia PowerSC Standard Edition 1.1.3” na strane 2
Pre každú špecifickú funkciu PowerSC Standard Edition musíte nainštalovať sadu súborov.
Inštalácia s NIM

IBM Fix Central

Online pomocné centrum Passport Advantage

Konfigurácia Trusted Network Connect a správy záplat

TNC (Trusted Network Connect) musíte konfigurovať ako démon na správu záplat. Server TNC sa integruje so SUMA s cieľom poskytnúť komplexné riešenie pre správu záplat.

Konfigurácia servera Trusted Network Connect

Naučte sa ako konfigurovať 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 42 830 minút sa použije pre port tncport a predvolená hodnota 38 240 minút sa použije pre port pmserver.

Súvisiaci odkaz:

"Príkaz pscon" na strane 36

Konfigurácia klienta Trusted Network Connect

Naučte sa postup ako konfigurovať klienta TNC (Trusted Network Connect) a konfiguračné nastavenia vyžadované na nastavenie.

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 36

Konfigurácia servera na správu záplat

Naučte sa konfigurovať systém ako server na správu záplat.

Server na správu záplat TNC (Trusted Network Connect) musí byť nakonfigurovaný na serveri NIM (Network Installation Management), aby bolo možné aktualizovať klientov TNC.

Ak chcete inicializovať archívy opráv pre správu záplat TNC, zadajte tento príkaz:

```
pmconf init -i <interval sťahovania> -l <zoznam TL> [-A] [-P <cesta sťahovania>][-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 záplat TNC nainštalovať aktualizácie klienta TNC. Zadajte príznak **-A** na akceptovanie všetkých licenčných zmlúv pri

spúšťaní aktualizácií klienta. Archívy opráv, ktoré stiahne server na správu záplat TNC, sa štandardne nachádzajú v súbore /var/tnc/tncpm/fix_repository. Pomocou príznaku **-P** zadajte iný adresár.

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 záplat, 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 záplat TNC vždy podporuje správu bezpečnostných hlásení o analýze autorizovaným programom (APAR). Ak chcete konfigurovať správu záplat 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

Server na správu záplat TNC podporuje **syslog** na stiahnutie aktualizácií servisného balíka, technologickej úrovne a klienta. Zariadenie je užívateľ a priorita je info. Napríklad: užívateľ.info.

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

Súvisiaci odkaz:

"Príkaz pscon" na strane 36

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 záplaty 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 36

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.

Súvisiaci odkaz:

"Príkaz pscon" na strane 36

Riadenie Trusted Network Connect a správy záplat

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 36

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
```

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 36

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:

  ```
  tncconsole 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 36

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 36

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.

Súvisiaci odkaz:

"Príkaz pscon" na strane 36

Riadenie politík na správu záplat

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

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

| Ak chcete riadiť politiku na správu záplat, 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 33

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 36

| 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 zostáv APAR a dočasných opráv. Ak chcete zobraziť výsledky tejto zostavy, zadajte nasledujúci príkaz:

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

Súvisiaci odkaz:

“Príkaz pscon” na strane 36

Riešenie problémov s Trusted Network Connect a riadením záplat

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

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

Tabuľka 3. Riešenie problémov a konfiguračné nastavenia pre TNC a systémy riadenia záplat

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.
Server riadenia záplat NC sa nespustí alebo neodpovedá	• Určite, či je démon servera riadenia záplat TNC spustený zadaním nasledujúceho príkazu: `ps –eaf | grep tncpmd` • Skontrolujte v konfiguračnom súbore /etc/tnccs.conf položku component = TNCPM na serveri riadenia záplat 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.

Tabuľka 3. Riešenie problémov a konfiguračné nastavenia pre TNC a systémy riadenia záplat (pokračovanie)

Problém	Riešenie
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.

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 32

“Príkaz vlantfw” na strane 42

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 15
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 30

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 musí byť spustený len v systéme AIX verzia 7.1 s technologickou úrovňou 7100-02, aby bolo možné sťahovať metaúdaje servisného balíka.

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** <*cesta sťahovania*>] [**-x** <*ifix interval*>] [**-K** <*ifix*
| *kľúč*>]

pmconf add -l *zoznam_TL*

pmconf add -p <*Zoznam SP*> [**-U** <*užívateľom definovaná cesta SP*>]

| **pmconf add -p** <*SP*> **-e** <*súbor ifix*>

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

pmconf delete -l *zoznam_TL*

pmconf delete -p <*Zoznam SP*>

| **pmconf delete -p** <*SP*>**-e** *súbor ifix*

pmconf list -s [**-c**] [**-q**]

pmconf list -l *SP*

pmconf list -C

pmconf list -a *SP*

pmconf hist -u

pmconf hist -d

pmconf import -f *názov_súboru_cert* **-k** *názov_súboru_kľúča*

pmconf export -f *názov_súboru*

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 delete -l <*zoznam TL*>

pmconf restart

stav pmconf

protokol pmconf úroveň_protokolu = info | chyba | žiadny

pmconf chtncpm atribút = *hodnota*

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.
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.
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.
-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, ktorá reprezentuje minúty alebo ktorá je v tomto formáte: **d** (počet dní): **h** (hodiny): **m** (minúty).
-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**.
-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.
-P *cesta_k_archívu_opráv*	Určuje adresár sťahovania pre archívy opráv, ktoré stiahne TNCPM. Predvolený adresár je **/var/tnc/tncpm/fix_repository**.
-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.
-d	Vygeneruje hlásenie o histórii stiahnutí servisných balíkov.
-C	Vygeneruje hlásenie o serverovom certifikáte.
-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).
-f *názov_súboru*	Určuje názov súboru certifikátu.
-k *názov_súboru_kľúča*	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.
-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.

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
    ```

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 záplat 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=**<*host*:*port*> [tsserver=<host>] [**recheck_interval=**<*čas_v_minútach*> | **d** (dni) : **h** (hodiny) : **m** (minúty)] [**dbpath** = <*užívateľom definovaný adresár*>]

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

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

psconf chserver atribút = *hodnota*

psconf add -F <*FSPolicyname*> -r <*buildinfo*> [**apargrp=** [**±**]<*apargrp1, apargrp2..* >] [*ifixgrp*=[+|-]<*ifixgrp1*,*ifixgrp2...*>]

| **psconf add** { **-G** <*ipgroupname*> **ip=**[**±**]<*host1, host2...*> | {**-A**<*apargrp*> [**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**< *host* >| **-G** <*ipgroup*> [**-r** <*buildinfo*> | **-a** <*apar1, apar2...*> | [**-u**] **-v** <*ifix1*, *ifix2*,...>}

| **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*>} [**-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>**

| 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**.
dbpath	Určuje umiestnenie databázy TNC. Predvolená hodnota je /var/tnc.
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.

Položka	Popis
log	Nastaví úroveň protokolovania pre komponenty TNC.
mkclient	Nakonfiguruje klienta TNC.
mkipref	Nakonfiguruje TNC IPRef.
mkserver	Nakonfiguruje server TNC.
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.
recheck_interval	Určuje interval v minútach, alebo formáte d (dni) : h (hodiny) : m (minúty) pre server TNC na overovanie klientov TNC. **Poznámka:** Hodnota **recheck_interval=0** znamená, že plánovač neinicioval overovanie klientov v pravidelných intervaloch a zaregistrovaní klienti sa automaticky overia počas spúšťania. 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 záplaty na klienta.
verify	Iniciuje manuálne overenie klienta.

Príznaky

Položka	Popis
-A <advisoryName>	Určuje názov poradenský názov pre zostavu.
-B <buildinfo>	Určuje informácie o zostavení na prípravu zostavy o záplate.

-c	Zobrazí atribúty užívateľa v záznamoch oddelených dvojbodkou nasledovným spôsobom:
	`# name: atribút1: atribút2: ...`
	`policy: 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 ID e-mailu, za ktorým nasleduje zoznam názvov skupín IP oddelených čiarkou.
-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 COMPLAINT. 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 *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.

Položka	Popis
-k *názov súboru*	Určuje súbor, z ktorého sa musí čítať kľúč certifikátu v prípade operácie importovania.
-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.
-v	Určuje zoznam dočasných opráv oddelený čiarkami.
-V	Určuje názov skupiny dočasných opráv.

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 zostavu pre klientov, ktorí sú v stave **COMPLAINT**, 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
    ```

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 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 15
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.

-I 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 30

Vyhlásenia

Tieto informácie boli vyvinuté pre produkty a služby ponúkané v USA.

Spoločnosť IBM nemusí poskytovať produkty, služby alebo komponenty zmienené v tomto dokumente vo všetkých krajinách. Informácie o produktoch a službách, aktuálne dostupných vo vašej krajine, môžete získať od zástupcu spoločnosti IBM. Žiadne odkazy na produkt, program alebo službu spoločnosti IBM neznamenajú, ani z nich nevyplýva, že musí byť použitý len tento produkt, program alebo služba spoločnosti IBM. Môžete použiť ľubovoľný funkčne ekvivalentný produkt, program alebo službu, ktoré neporušujú práva duševného vlastníctva IBM. Za posúdenie a overenie funkčnosti akéhokoľvek produktu, programu alebo služby, ktorý alebo ktorú nedodáva spoločnosť IBM, je však zodpovedný sám používateľ.

Spoločnosť IBM môže byť držiteľom patentov alebo čakateľom na udelenie patentov pre predmet tohto dokumentu. Poskytnutie tohto dokumentu vás neoprávňuje k ničomu, čo súvisí s týmito patentmi. Dotazy týkajúce sa licencií môžete adresovať na :

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
U.S.A.

V prípade otázok týkajúcich sa licencií vzťahujúcich sa na sadu dvojbajtových znakov (DBCS), kontaktujte oddelenie duševného vlastníctva spoločnosti IBM vo vašej krajine, alebo ich písomne pošlite na adresu:

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

Nasledujúci odsek sa nevzťahuje na Veľkú Britániu ani na žiadnu inú krajinu, kde sú takéto ustanovenia v rozpore so všeobecne záväznými právnymi predpismi: SPOLOČNOSŤ INTERNATIONAL BUSINESS MACHINES CORPORATION POSKYTUJE TÚTO PUBLIKÁCIU „TAK, AKO JE“, BEZ AKEJKOĽVEK ZÁRUKY, ČI UŽ VÝSLOVNEJ ALEBO MLČKY PREDPOKLADAEJ, VRÁTANE, ALE BEZ OBMEDZENIA NA, ZÁRUKY PREDAJNOSTI, VHODNOSTI NA KONKRÉTNY ÚČEL A NEPORUŠENIA PRÁV. Niektoré štáty pri určitých transakciách nepovoľujú takéto zrieknutie sa výslovných alebo mlčky predpokladaných záruk, toto vyhlásenie sa vás teda nemusí netýkať.

Je možné, že v tejto publikácii sa vyskytujú technické nepresnosti alebo typografické chyby. V tu uvedených informáciách sa pravidelne vykonávajú zmeny; tieto zmeny budú zapracované do nových vydaní tejto publikácie. IBM môže kedykoľvek bez ohlásenia urobiť vylepšenia a/alebo zmeny v produktoch alebo programoch opísaných v tejto publikácii.

Všetky odkazy na webové stránky iných spoločností ako IBM uvedené v týchto informáciách sa poskytujú len pre vaše pohodlie a v žiadnom prípade nepredstavujú súhlas s obsahom týchto webových stránok. Informácie uvedené na týchto webových stránkach nie sú súčasťou materiálov pre tento produkt IBM a používanie týchto webových stránok je na vašu vlastnú zodpovednosť.

IBM môže použiť alebo distribuovať informácie, ktoré poskytnete, ľubovoľným spôsobom, ktorý bude považovať za vhodný, bez toho, že jej vznikli akékoľvek záväzky voči vám.

Držitelia licencií tohto programu, ktorí si želajú mať informácie o tomto programe kvôli povoleniu: (i) výmeny informácií medzi nezávisle vytvorenými programami a inými programami (vrátane tohto programu) a (ii) spoločného používania vymenených informácií by mali kontaktovať:

IBM Corporation
Dept. LRAS/Bldg. 903
11501 Burnet Road
Austin, TX 78758-3400
USA

Za primeraných podmienok, v niektorých prípadoch i za poplatok, môže spoločnosť IBM takéto informácie poskytnúť.

The Licenčný program spomínaný v tomto dokumente a všetky pre tento program dostupné licenčné materiály poskytuje spoločnosť IBM podľa podmienok zmluvy IBM Customer Agreement, IBM International Program License Agreement alebo ľubovoľnej ekvivalentnej zmluvy medzi nami.

Všetky údaje o výkone uvedené v tomto dokumente boli získané v laboratórnom prostredí. Z tohto dôvodu sa môžu výsledky získané v iných prevádzkových podmienkach výrazne odlišovať od tu uvedených údajov. Niektoré merania sa mohli robiť na systémoch, ktoré boli ešte vo vývoji, a nie je teda záruka, že výsledky týchto meraní budú zodpovedať výsledkom, ktoré vykazujú bežne dostupné systémy. Navyše, niektoré hodnoty mohli byť odhadnuté extrapoláciou. Skutočné výsledky môžu byť odlišné. Užívatelia týchto dokumentov by si mali overiť príslušné údaje pre svoje konkrétne prostredie.

Informácie týkajúce sa produktov iných spoločností ako IBM boli získané od dodávateľov týchto produktov, z ich publikovaných oznámení alebo iných verejne prístupných zdrojov. Spoločnosť IBM tieto produkty netestovala a nemôže potvrdiť presnosť ich výkonu, kompatibilitu ani iné parametre týkajúce sa produktov nepochádzajúcich od IBM. Otázky o schopnostiach produktov nepochádzajúcich od IBM adresujte dodávateľom týchto produktov.

Všetky vyhlásenia týkajúce sa budúceho smerovania spoločnosti IBM sa môžu zmeniť bez predchádzajúceho upozornenia a reprezentujú iba ciele spoločnosti IBM.

Všetky uvedené ceny IBM sú aktuálne odporúčané maloobchodné ceny spoločnosti IBM a môžu sa zmeniť bez predchádzajúceho upozornenia. Ceny predajcov môžu byť iné.

Tieto informácie slúžia len na plánovacie účely. Tu uvedené informácie môžu byť pred sprístupnením opisovaných produktov zmenené.

Tieto informácie obsahujú príklady údajov a hlásení používaných v každodenných obchodných operáciách. Aby boli tieto príklady čo najvernejšou ilustráciou skutočnosti, obsahujú mená osôb a názvy spoločností, značiek a výrobkov. Všetky tieto mená a názvy sú fiktívne a akákoľvek podobnosť s menami, názvami a adresami skutočných ľudí alebo podnikov je celkom náhodná.

LICENCIA NA AUTORSKÉ PRÁVA:

Tieto informácie obsahujú vzorové aplikačné programy v zdrojovom jazyku, ktoré ilustrujú programovacie techniky na rozličných operačných platformách. Tieto vzorové programy môžete kopírovať, upravovať a distribuovať v ľubovoľnej forme bez poplatkov spoločnosti IBM, ak tieto programy využijete na vývoj, používanie, marketing alebo distribúciu aplikačných programov vyhovujúcich rozhraniu aplikačného programovania pre platformu operačného systému, pre ktorú boli tieto vzorové programy napísané. Tieto programy neboli detailne testované vo všetkých prevádzkových podmienkach. IBM preto nemôže zaručiť spoľahlivosť, servisovateľnosť ani fungovanie týchto programov. Tieto vzorové programy sa poskytujú "TAK, AKO SÚ", bez záruky akéhokoľvek druhu. Spoločnosť IBM nebude zodpovedná za žiadne škody vyplývajúce z používania týchto vzorových programov.

Každá kópia alebo akákoľvek časť týchto vzorových programov alebo akéhokoľvek z nich odvodeného diela musí obsahovať nasledovnú deklaráciu autorských práv:

© (názov vašej firmy) (rok). Časti tohto kódu sú odvodené od vzorových programov IBM Corp. © Copyright IBM Corp. _zadajte rok alebo roky_.

Ak si prezeráte elektronickú kópiu týchto informácií, nemusia byť zobrazené fotografie ani farebné ilustrácie.

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 pomôcť pri zhromažďovaní 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 subjektov. Aktuálny zoznam ochranných známok spoločnosti IBM nájdete 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 USA alebo iných krajinách.

Java a všetky s ňou súvisiace ochranné známky a logá sú ochranné známky alebo registrované ochranné známky spoločnosti Oracle alebo jej pridružených spoločností.

Index

T

V

Z

Vytlačené v USA