IBM PowerSC

Standard Edition

verze 1.1.3

PowerSC Standard Edition

IBM PowerSC

Standard Edition

verze 1.1.3

PowerSC Standard Edition

Poznámka

Před použitím těchto informací a popisovaného produktu si přečtěte informace obsažené v oddílu “Poznámky” na stránce 47.

Toto vydání se vztahuje na modul IBM PowerSC verze 1.1.3 a na všechny následné verze a modifikace, není-li v nových vydáních uvedeno jinak.

Obsah

O této příručce

Tento dokument obsahuje úplné informace o zabezpečení souborů, systémů a sítí pro administrátory systémů.

Zvýrazňování

V tomto dokumentu se používají následující zvýrazňovací konvence:

Tučné písmo	Označuje příkazy, funkce, klíčová slova, soubory, struktury, adresáře a další položky, jejichž názvy jsou v systému předdefinovány. Takto jsou označeny i grafické objekty (například tlačítka, názvy a ikony), mezi nimiž uživatelé vybírají.
Kurzíva	Takto se označují parametry, jejichž skutečné názvy nebo hodnoty zadává uživatel.
Neproporcionální písmo	Označuje příklady hodnot, textů zobrazovaných na obrazovce, částí zdrojových kódů programů, jak byste je napsali jako programátor, nebo zprávy systému a údaje, které můžete zadávat.

Rozlišování malých a velkých písmen v systému AIX

Při všech operacích v systému AIX se rozlišují velká a malá písmena. Chcete-li například zobrazit seznam souborů, můžete použít příkaz **ls**. Pokud zadáte příkaz LS, systém odpoví, že příkaz nebyl nalezen. Stejně tak řetězce SOUBORA, SouborA a soubora představují tři různé názvy souborů, a to i v případě, že se nacházejí ve stejném adresáři. Vždy proto zkontrolujte, zda byla malá a velká písmena použita správně. Zabráníte tak provedení nepředvídatelných akcí.

ISO 9000

Pro vývoj a výrobu tohoto produktu byly použity normy pro kvalitu ISO 9000.

IBM PowerSC Standard Edition 1.1.3

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

Novinky v modulu PowerSC Standard Edition 1.1.3

Seznamte se s novými nebo výrazně změněnými informacemi pro kolekci témat týkajících se modulu PowerSC Standard Edition verze 1.1.3.

V tomto souboru PDF se na levém okraji nových nebo změněných informací zobrazí revizní značka (|).

Prosinec 2013

- V tématu "Koncepce modulu PowerSC Standard Edition 1.1.3" byly aktualizovány systémové požadavky.
- V tématu "Předpoklady funkce Trusted Boot" na stránce 5 bylo určeno požadované nahrazení souborů funkce Trusted Boot po opětné instalaci operačního systému AIX.
- Do tématu "Monitorování funkce Trusted Firewall" na stránce 13 byly přidány informace o funkci monitorování modulu Trusted Firewall.
- Do tématu "Protokolování funkce Trusted Firewall" na stránce 13 byly přidány informace o funkci protokolování modulu Trusted Firewall.
- Bylo přidáno téma "Instalace funkce Trusted Logging" na stránce 18.
- Do tématu "Konfigurování serveru pro správu oprav" na stránce 24 byly přidány informace o aktualizacích prozatímních oprav pro funkci Trusted Network.
- Do tématu "Vytváření sestav pro server TNC" na stránce 29 byly přidány informace o vytváření sestav serveru Trusted Network Connect.
- Do tématu "Instalace ověřovacího modulu" na stránce 6 byly přidány informace o instalaci ověřovacího modulu funkce Trusted Network Connect.
- Do tématu "Příkazy modulu PowerSC Standard Edition" na stránce 30 byly přidány příkazy funkce Trusted Firewall.
- Příkaz **tscpmconsole** byl přejmenován na příkaz **pmconf** a do tématu "Příkaz pmconf" na stránce 34 byly přidány příslušné informace.
- Příkaz **tscconsole** byl přejmenován na příkaz **psconf** a do tématu "Příkaz psconf" na stránce 38 byly přidány příslušné informace.
- V tématu "Příkaz vlantfw" na stránce 44 byly aktualizovány informace o volbách pro příkaz **vlantfw**.

Listopad 2012

V tématu "Funkce Trusted Network Connect and Patch Management" na stránce 20 byly aktualizovány informace.

Květen 2012

V tématu "Trusted Firewall" na stránce 10 byla přidána dokumentace pro novou funkci.

Koncepce modulu PowerSC Standard Edition 1.1.3

Tento přehled modulu PowerSC Standard Edition popisuje funkce, komponenty a hardwarovou podporu související s funkcí PowerSC Standard Edition.

Modul PowerSC Standard Edition poskytuje možnost zabezpečení a řízení systémů pracujících v rámci cloudu nebo ve virtualizovaných datových střediscích a nabízí vhled z pozice podniku a možnosti správy. Modul PowerSC Standard

Edition představuje sadu funkcí, mezi něž patří funkce Security and Compliance Automation, Trusted Boot, Trusted Firewall, Trusted Logging a Trusted Network Connect and Patch Management. Technologie zabezpečení, která je součástí vrstvy virtualizace, poskytuje další zabezpečení pro samostatné systémy.

V následující tabulce jsou uvedeny podrobnosti o vydáních, funkcích zahrnutých ve vydáních, komponentách a procesorovém hardwaru, pro který jsou k dispozici jednotlivé komponenty.

Tabulka 1. Komponenty modulu PowerSC Standard Edition, popis, podpora operačního systému a hardwarová podpora

Komponenty	Popis	Podporovaný operační systém	Podporovaný hardware
Security and Compliance Automation	Automatizuje nastavení, monitorování a auditování konfigurace zabezpečení a shody pro následující standardy: • PCI DSS (Payment Card Industry Data Security Standard) • SOX/COBIT (Sarbanes-Oxley Act a shoda COBIT) • STIG Ministerstva obrany USA • HIPAA (Health Insurance Portability and Accountability Act)	• AIX 5.3 • AIX 6.1 • AIX 7.1	• POWER5 • POWER6 • POWER7
Trusted Boot	Provádí měření obrazu zavádění, operačního systém a aplikací a potvrzuje jejich důvěryhodnost s použitím technologie VTPM (Virtual Trusted Platform Module).	• AIX 6 s úrovní 6100-07 nebo novější • AIX 7 s úrovní 7100-01 nebo novější	POWER7 s firmwarem eFW7.4 nebo novější
Trusted Firewall	Šetří čas a prostředky díky umožnění přímého směrování mezi určenými virtuálními sítěmi LAN, které jsou řízeny tímtéž serverem Virtuální server I/O.	• AIX 6.1 • AIX 7.1 • VIOS verze 2.2.1.4 nebo novější	• POWER6 • POWER7 • Virtuální server I/O verze 6.1S nebo novější
Trusted Logging	Protokoly systému AIX jsou centrálně umisťovány na server VIOS (Virtual I/O Server) v reálném čase. Tato funkce umožňuje protokolování bez rizika zásahu ze strany neoprávněného uživatele a pohodlné zálohování a správu protokolů.	• AIX 5.3 • AIX 6.1 • AIX 7.1	• POWER5 • POWER6 • POWER7
Trusted Network Connect and Patch Management	Ověřuje, že systémy AIX ve virtuálním prostředí jsou na určené úrovni softwaru a oprav, a poskytuje nástroje pro správu, aby bylo možné zaručit, že se všechny systémy AIX nacházejí na určené úrovni softwaru. Pokud je do sítě přidán virtuální systém nižší úrovně nebo pokud je vydána oprava zabezpečení, která bude mít na systémy vliv, budou vygenerovány výstrahy.	• AIX 5.3 • AIX 6.1 • AIX 7.1 Klient Trusted Network Connect vyžaduje jednu z následujících komponent: • AIX 6.1 s úrovní 6100-06 nebo novější • Systém konzoly SUMA (Service Update Management Assistant) pro systém AIX verze 7.1 v rámci prostředí SUMA pro správu oprav	• POWER5 • POWER6 • POWER7

Instalace modulu PowerSC Standard Edition 1.1.3

Je třeba nainstalovat sadu souborů pro každou konkrétní funkci modulu PowerSC Standard Edition.

Pro modul PowerSC Standard Edition jsou k dispozici následující sady souborů:

- powerscExp.ice: Je instalována v systémech AIX vyžadujících funkci Security and Compliance Automation modulu PowerSC Standard Edition.
- powerscStd.vtpm: Je instalována v systémech AIX vyžadujících funkci Trusted Boot modulu PowerSC Standard Edition.
- powerscStd.vlog: Je instalována v systémech AIX vyžadujících funkci Trusted Logging modulu PowerSC Standard Edition.
- powerscStd.tnc_pm: Je instalována v systému AIX verze 6.1 s úrovní technologie 6100-06 nebo novějším či v systému konzoly nástroje SUMA (Service Update Management Assistant) pro systém AIX verze 7.1 v rámci prostředí SUMA pro správu oprav.
- powerscStd.svm: Je instalována v systémech AIX, v nichž může být přínosem funkce směrování modulu PowerSC Standard Edition.

Modul PowerSC Standard Edition lze nainstalovat prostřednictvím jednoho z následujících rozhraní:

- Příkaz **installp** z rozhraní příkazového řádku
- Rozhraní SMIT

Chcete-li modul PowerSC Standard Edition nainstalovat prostřednictvím rozhraní SMIT, proveďte následující kroky:

1. Spusťte následující příkaz:
   ```
   % smitty installp
   ```
2. Vyberte volbu **Instalace programového vybavení**.
3. Vyberte vstupní zařízení nebo adresář pro software, aby bylo možné určit umístění a instalační soubor obrazu instalace modulu IBM Compliance Expert. Pokud se například obraz instalace nachází v souboru s cestou /usr/sys/inst.images/powerscStd.vtpm, je třeba určit cestu k souboru v poli **VSTUP**.
4. Prostudujte si licenční smlouvu a přijměte ji. Licenční smlouvu lze přijmout tak, že pomocí šipky dolů vyberete volbu **PŘIJMOUT nové licenční smlouvy** a stisknutím klávesy Tab změníte hodnotu volby na hodnotu **Ano**.
5. Stisknutím klávesy **Enter** spusťte instalaci.
6. Po dokončení instalace ověřte, že má příkaz stav **OK**.

Zobrazení licence k softwaru

Licenci k softwaru lze zobrazit v rámci rozhraní příkazového řádku pomocí následujícího příkazu:

```
% installp –lE –d cesta/název_souboru
```

Parametr *cesta/název_souboru* určuje instalační obraz modulu PowerSC Standard Edition.

Prostřednictvím rozhraní příkazového řádku můžete například zadat následující příkaz pro určení licenčních informací týkajících se modulu PowerSC Standard Edition:

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

Související pojmy:

“Koncepce modulu PowerSC Standard Edition 1.1.3” na stránce 1
Tento přehled modulu PowerSC Standard Edition popisuje funkce, komponenty a hardwarovou podporu související s funkcí PowerSC Standard Edition.

“Instalace funkce Trusted Boot” na stránce 6
Pro instalaci funkce Trusted Boot jsou vyžadovány určité konfigurace hardwaru a softwaru.

“Instalace funkce Trusted Network Connect” na stránce 22
Instalace komponent funkce TNC (Trusted Network Connect) vyžaduje provedení určitých kroků.

Související úlohy:

“Instalace funkce Trusted Firewall” na stránce 12
Instalace funkce PowerSC Trusted Firewall je podobná instalaci dalších funkcí modulu PowerSC.

“Instalace funkce Trusted Logging” na stránce 18
Funkci PowerSC Trusted Logging lze nainstalovat prostřednictvím rozhraní příkazového řádku nebo nástroje SMIT.

Trusted Boot

Funkce Trusted Boot využívá modul VTPM (Virtual Trusted Platform Module), což je virtuální instance modulu TPM sdružení Trusted Computing Group. Modul VTPM slouží k bezpečnému ukládání měření zavedení systému pro budoucí ověřování.

Koncepce Trusted Boot

Je důležité porozumět integritě procesu zavádění a způsobu klasifikace zavádění jako důvěryhodného nebo nedůvěryhodného.

Pro každý fyzický systém lze prostřednictvím konzoly Hardware Management Console (HMC) konfigurovat nejvýše 60 logických oblastí (LPAR) s povoleným modulem VTPM. Je-li modul VTPM konfigurován, je jedinečný pro každou oblast LPAR. Je-li modul VTPM použit v kombinaci s technologií AIX Trusted Execution, zajišťuje zabezpečení a zajištění následujících oblastí:

- Obraz zavádění na disku
- Celý operační systém
- Aplikační vrstvy

Administrátor může zobrazit důvěryhodné a nedůvěryhodné systémy prostřednictvím centrální konzoly nainstalované spolu s ověřovacím modulem **openpts**, který je k dispozici v rozšiřující sadě pro systém AIX. Konzola **openpts** spravuje jeden či více serverů Power Systems a monitoruje nebo potvrzuje stav důvěryhodnosti systémů AIX v rámci datového střediska. Potvrzování je proces, při kterém ověřovací modul určí (potvrdí), zda kolektor provedl důvěryhodné zavedení systému.

Stav důvěryhodného zavedení systému

Oblast je považována za důvěryhodnou, pokud ověřovací modul úspěšně potvrdí integritu kolektoru. Ověřovacím modulem je vzdálená oblast, která určí, zda kolektor provedl důvěryhodné zavedení systému. Kolektorem je oblast se systémem AIX, ke které je připojen modul VTPM (Virtual Trusted Platform Module) a ve které je nainstalován balík TSS (Trusted Software Stack). Indikuje, že měření zaznamenaná v rámci modulu VTPM odpovídají referenční sadě uložené v ověřovacím modulu. Stav důvěryhodného zavedení systému indikuje, zda byl systém oblasti zaveden důvěryhodným způsobem. Tato informace se týká integrity procesu zavedení systému a neuvádí aktuální ani probíhající úroveň zabezpečení systému.

Stav nedůvěryhodného zavedení systému

Oblast přejde do stavu nedůvěryhodnosti, pokud ověřovací modul nemůže úspěšně potvrdit integritu procesu zavedení systému. Stav nedůvěryhodnosti znamená, že některý aspekt procesu zavedení systému není konzistentní s referenčními informacemi obsaženými v ověřovacím modulu. Mezi možné příčiny neúspěšného potvrzení patří zavedení systému z

jiného zaváděcího zařízení, zavedení jiného obrazu jádra či změna existujícího obrazu zavádění.

Související pojmy:

“Odstraňování problémů s funkcí Trusted Boot” na stránce 8
Existuje několik běžných situací a kroků nápravy potřebných při určování příčiny selhání potvrzování v případě použití funkce Trusted Boot.

Plánování použití funkce Trusted Boot

Seznamte se s informacemi o konfiguraci hardwaru a softwaru potřebné pro instalaci funkce Trusted Boot.

Předpoklady funkce Trusted Boot

Instalace funkce Trusted Boot zahrnuje konfigurování kolektoru a ověřovacího modulu.

Při přípravě na opětnou instalaci operačního systému AIX v systému, ve kterém je již nainstalována funkce Trusted Boot, je třeba zkopírovat soubor /var/tss/lib/tpm/system.data a použít jej k přepsání souboru v tomtéž umístění po dokončení opětné instalace. Pokud tento soubor nezkopírujete, je třeba odebrat virtualizovaný modul TPM (Trusted Platform Module) z konzoly správy a znovu jej nainstalovat v oblasti.

Kolektor

Konfigurační požadavky pro instalaci kolektoru zahrnují následující předpoklady:

- Hardware POWER7 spuštěný s firmwarem vydání 740.
- Nainstalovaný systém IBM AIX 6 s úrovní technologie 7 nebo nainstalovaný systém IBM AIX 7 s úrovní technologie 1.
- Nainstalovaná konzola správy hardwaru (HMC) verze 7.4 nebo novější.
- Nakonfigurovaná oblast s modulem VTPM a minimálním množstvím paměti 1 GB.
- Nainstalované zabezpečení Secure Shell (SSH), konkrétně OpenSSH nebo ekvivalentní.

Ověřovací modul

Ověřovací modul **openpts** je přístupný prostřednictvím rozhraní příkazového řádku i prostřednictvím grafického uživatelského rozhraní určeného pro použití na mnoha platformách. Verze ověřovacího modulu OpenPTS pro systém AIX je k dispozici v rozšiřující sadě pro systém AIX. Verze ověřovacího modulu OpenPTS pro systém Linux a další platformy jsou k dispozici prostřednictvím stažení z webu. Mezi konfigurační požadavky patří i následující:

- Nainstalované zabezpečení SSH, konkrétně OpenSSH nebo ekvivalentní.
- Vytvoření síťové připojení (prostřednictvím zabezpečení SSH) ke kolektoru.
- Nainstalované prostředí Java™ 1.6 nebo novější pro přístup ke konzole **openpts** prostřednictvím grafického rozhraní.

Příprava na nápravu situace

Informace o funkci Trusted Boot popsané v tomto dokumentu slouží jako vodítko při určování situací, které mohou vyžadovat nápravu. Na proces zavádění systému nemají žádný vliv.

Může se vyskytnout mnoho situací, v nichž dojde k selhání potvrzení, a předvídat situace, které mohou nastat, je obtížné. Odpovídající akci je třeba určit podle konkrétní situace. Je však užitečné připravit se na některé nepříznivé možnosti a mít k dispozici zásady nebo sled prací, abyste se s takovou situací vyrovnali snáze. Nápravou situace se rozumí opravná akce, kterou je třeba provést v případě, že po provedení potvrzování je jeden či více kolektorů považováno za nedůvěryhodné.

Pokud například došlo k selhání potvrzování v důsledku odlišnosti obrazu zavádění od reference ověřovacího modulu, zkuste odpovědět na následující otázky:

- Jak lze ověřit oprávněnost hrozby?
- Byla v poslední době provedena plánovaná akce údržby, přechod na vyšší verzi systému AIX nebo instalace nového hardwaru?

- Můžete se obrátit na administrátora, který má k těmto informacím přístup?
- Kdy byl naposled zaveden systém v důvěryhodném stavu?
- Pokud se hrozba zabezpečení jeví oprávněně, jakou akci je třeba provést? (Mezi návrhy patří shromáždění protokolu auditu, odpojení systému od sítě, vypnutí systému a upozornění uživatelů.)
- Došlo k ohrožení jakýchkoli dalších systémů, které je třeba ověřit?

Související pojmy:

"Odstraňování problémů s funkcí Trusted Boot" na stránce 8
Existuje několik běžných situací a kroků nápravy potřebných při určování příčiny selhání potvrzování v případě použití funkce Trusted Boot.

Aspekty migrace

Před migrací oblasti s povoleným modulem VTPM (Virtual Trusted Platform Module) vezměte v potaz tyto předpoklady.

Výhodou modulu VTPM oproti fyzickému modulu TPM je skutečnost, že umožňuje přesouvání oblasti mezi systémy, přičemž modul VTPM zůstává zachován. Firmware před přenosem zašifruje data modulu VTPM, aby mohla být logická oblast bezpečně migrována. Kvůli zaručení zabezpečené migrace je třeba před migrací zavést následující bezpečnostní opatření:

- Povolit zabezpečení IPSEC pro server Virtuální server I/O (Virtuální vstupně-výstupní server), který migraci provádí.
- Nastavit důvěryhodný klíč systému prostřednictvím konzoly správy hardwaru (HMC), aby bylo možné řídit spravované systémy s možností dešifrování dat modulu VTPM po provedení migrace. Cílový systém migrace musí mít k dispozici stejný klíč jako zdrojový systém, aby bylo možné úspěšně provést migraci dat.

Související informace:

Použití konzoly HMC

Migrace serveru VIOS

Instalace funkce Trusted Boot

Pro instalaci funkce Trusted Boot jsou vyžadovány určité konfigurace hardwaru a softwaru.

Související informace:

"Instalace modulu PowerSC Standard Edition 1.1.3" na stránce 3
Je třeba nainstalovat sadu souborů pro každou konkrétní funkci modulu PowerSC Standard Edition.

Instalace kolektoru

Kolektor je třeba nainstalovat s použitím sady souborů ze základního disku CD systému AIX.

Chcete-li kolektor nainstalovat, nainstalujte balíky powerscStd.vtpm a openpts.collector, které jsou k dispozici na základním disku CD, pomocí příkazu **smit** nebo **installp**.

Instalace ověřovacího modulu

Komponenta ověřovacího modulu OpenPTS je spouštěna v operačním systému AIX a na jiných platformách.

| Verzi ověřovacího modulu pro systém AIX lze nainstalovat ze sady souborů s použitím rozšiřující sady pro systém
| AIX. Chcete-li nainstalovat ověřovací modul v operačním systému AIX, nainstalujte balík openpts.verifier z
| rozšiřujícího balíku pro systém AIX pomocí příkazu **smit** nebo **installp**. Tímto způsobem je nainstalována verze
| ověřovacího modulu s rozhraním příkazového řádku i s grafickým rozhraním.

| Ověřovací modul OpenPTS pro jiné operační systémy lze stáhnout ze stránky Stažení ověřovacího modulu
| OpenPTS pro systém Linux určeného k použití v kombinaci s funkcí Trusted Boot systému AIX.

Související informace:

Stažení ověřovacího modulu OpenPTS pro systém Linux určeného k použití v kombinaci s funkcí Trusted Boot systému AIX

Konfigurování funkce Trusted Boot

Seznamte se s postupem při registraci a potvrzení systému pro funkci Trusted Boot.

Registrace systému

Seznamte se s postupem při registraci systému v ověřovacím modulu.

Registrace systému představuje proces poskytnutí počáteční sady měření ověřovacímu modulu, která tvoří základ pro další požadavky na potvrzení. Chcete-li systém zaregistrovat prostřednictvím příkazového řádku, použijte v ověřovacím modulu následující příkaz:

```
openpts -i <název_hostitele>
```

Informace o zaregistrované oblasti jsou umístěny v adresáři $HOME/.openpts. Každé nové oblasti je během procesu registrace přiřazen jedinečný identifikátor a informace týkající se zaregistrovaných oblastí jsou uloženy v adresáři odpovídajícím jedinečnému ID.

Chcete-li zaregistrovat systém prostřednictvím grafického rozhraní, proveďte následující kroky:

1. Spusťte grafické rozhraní pomocí příkazu **/opt/ibm/openpts_gui/openpts_GUI.sh**.
2. V navigační nabídce vyberte volbu **Registrovat**.
3. Zadejte název hostitele a pověření SSH systému.
4. Klepněte na volbu **Registrovat**.

Související pojmy:

"Potvrzení systému"
Seznamte se s postupem při potvrzování systému z příkazového řádku nebo prostřednictvím grafického rozhraní.

Potvrzení systému

Seznamte se s postupem při potvrzování systému z příkazového řádku nebo prostřednictvím grafického rozhraní.

Chcete-li zadat dotaz na integritu zavedení systému, použijte následující příkaz zadaný z ověřovacího modulu:

```
openpts <název_hostitele>
```

Chcete-li potvrdit systém prostřednictvím grafického rozhraní, proveďte následující kroky:

1. V navigační nabídce vyberte kategorii.
2. Vyberte jeden či více systémů pro potvrzení.
3. Klepněte na volbu **Potvrdit**.

Registrace a potvrzení systému bez hesla

Požadavek na potvrzení je odeslán prostřednictvím zabezpečení SSH (Secure Shell). Nainstalujte v kolektoru certifikát ověřovacího modulu, aby byla připojení SSH povolena i bez použití hesla.

Chcete-li v systému kolektoru nastavit certifikát ověřovacího modulu, proveďte následující kroky:

- V ověřovacím modulu spusťte následující příkaz:

  ```
  ssh-keygen    # bez přístupové fráze
  scp ~/.ssh/id_rsa.pub <kolektor>:/tmp
  ```

- V kolektoru spusťte následující příkaz:

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

Správa funkce Trusted Boot

Seznamte se s postupem správy výsledků potvrzování funkce Trusted Boot.

Interpretace výsledků potvrzování

Seznamte se s postupem při zobrazování výsledků potvrzování a porozumění těmto výsledkům.

Výsledkem potvrzování může být jeden z následujících stavů:

1. Selhání požadavku na potvrzení: Požadavek na potvrzení se nepodařilo zcela zpracovat. Prostudujte si část Odstraňování problémů, abyste porozuměli možným příčinám tohoto selhání.
2. Platná integrita systému: Potvrzování bylo úspěšně dokončeno a zavedení systému odpovídá referenčním informacím uloženým v ověřovacím modulu. Znamená to, že se jedná o úspěšné důvěryhodné zavedení systému.
3. Neplatná integrita systému: Zpracování požadavku bylo dokončeno, byl však zjištěn rozpor mezi informacemi shromážděnými během zavádění systému a referenčními informacemi uloženými v ověřovacím modulu. Znamená to, že se jedná o nedůvěryhodné zavedení systému.

V rámci potvrzování je prostřednictvím následující zprávy rovněž oznámeno, zda byla pro kolektor použita aktualizace:

Aktualizace systému k dispozici: Tato zpráva informuje o tom, že pro kolektor byla použita aktualizace a že je k dispozici sada aktualizovaných referenčních informací, jež budou uplatněny při příštím zavedení systému. Uživateli se v rámci ověřovacího modulu zobrazí výzva k přijetí nebo odmítnutí aktualizací. Uživatel například může zvolit přijetí těchto aktualizací, pokud si je vědom údržby probíhající v kolektoru.

Chcete-li přezkoumat selhání potvrzování prostřednictvím grafického rozhraní, proveďte následující kroky:

1. V navigační nabídce vyberte kategorii.
2. Vyberte systém, který chcete přezkoumat.
3. Poklepejte na položku odpovídající příslušnému systému. Zobrazí se okno s vlastnostmi. Toto okno obsahuje informace z protokolu o neúspěšném potvrzování.

Odstraňování systémů

Seznamte se s postupem odstranění systému z databáze ověřovacího modulu.

Chcete-li systém odebrat z databáze ověřovacího modulu, spusťte následující příkaz:

```
openpts -r <název_hostitele>
```

Odstraňování problémů s funkcí Trusted Boot

Existuje několik běžných situací a kroků nápravy potřebných při určování příčiny selhání potvrzování v případě použití funkce Trusted Boot.

Příkaz **openpts** deklaruje systém jako neplatný, pokud aktuální stav zavedení systému neodpovídá referenčním informacím uloženým v ověřovacím modulu. Příkaz **openpts** určí možnou příčinu neplatnosti integrity. Úplné zavedení systému AIX obsahuje několik proměnných a v případě selhání potvrzování je vyžadována analýza, na základě které lze určit příčinu selhání.

V následující tabulce jsou uvedeny obvyklé situace a kroky vedoucí k nápravě pro identifikaci příčiny selhání:

Tabulka 2. Odstraňování problémů v případě některých obvyklých situací, v nichž došlo k selhání

Důvod selhání	Možné příčiny selhání	Navrhovaná náprava situace

Potvrzování nebylo dokončeno.	• Nesprávný název hostitele.
	• Neexistence síťové trasy mezi zdrojem a cílem.
	• Nesprávná pověření zabezpečení.
		Zkontrolujte připojení se zabezpečením SSH (Secure Shell) pomocí následujícího příkazu:
		`ssh ptsc@název_hostitele`
		
		V případě úspěšného připojení SSH zkontrolujte, zda se nevyskytly následující příčiny selhání potvrzování:
		• V potvrzovaném systému není spuštěn démon **tcsd**.
		• Potvrzovaný systém nebyl inicializován příkazem **ptsc**. Tento proces by měl proběhnout automaticky během spouštění systému, ověřte však přítomnost adresáře /var/ptsc/ v kolektoru. Pokud adresář /var/ptsc/ neexistuje, spusťte v kolektoru následující příkaz:
		`ptsc -i`

Firmware komplexu CEC byl změněn.	• Byl proveden přechod na vyšší verzi firmwaru. • Oblast LPAR byla migrována do systému s jinou verzí firmwaru.	Zkontrolujte úroveň firmwaru v systému, který je hostitelem oblasti LPAR.
Prostředky přidělené pro oblast LPAR byly změněny.	Procesory nebo paměť přidělené pro oblast LPAR byly změněny.	Zkontrolujte profil oblasti v konzole HMC.
Pro adaptéry, které jsou v oblasti LPAR k dispozici, byl změněn firmware.	Do oblasti LPAR bylo přidáno hardwarové zařízení nebo z ní bylo odebráno.	Zkontrolujte profil oblasti v konzole HMC.
Byl změněn seznam zařízení připojených k oblasti LPAR.	Do oblasti LPAR bylo přidáno hardwarové zařízení nebo z ní bylo odebráno.	Zkontrolujte profil oblasti v konzole HMC.
Byl změněn obraz zavádění, který obsahuje i jádro operačního systému.	• Byla provedena aktualizace systému AIX a ověřovací modul o aktualizaci nebyl informován. • Byl spuštěn příkaz **bosboot**.	• Ověřte u administrátora nebo v kolektoru, zda před poslední operací opětného zavedení systému nebyla prováděna údržba. • Přezkoumejte protokoly v kolektoru a zjistěte, zda nedošlo k aktivitě v důsledku údržby.
Oblast LPAR je zavedena z jiného zařízení.	• Ihned po síťové instalaci byla provedena registrace. • Systém je zaveden ze zařízení údržby.	Zaváděcí zařízení a příznaky lze zkontrolovat pomocí příkazu **bootinfo**. Pokud byla registrace provedena ihned po instalaci správy NIM (Network Installation Management) a před operací opětného zavedení systému, budou se registrované informace týkat síťové instalace, a nikoli příštího zavedení z disku. Tuto registraci lze opravit odebráním registrace logické oblasti a její opětnou registrací.
Byla volána interaktivní nabídky zavádění SMS (System Management Services).		Proces zavádění musí být proveden bez přerušení a bez zásahu uživatele, aby mohl být systém považován za důvěryhodný. Přechod do nabídky zavádění SMS má za následek neplatné zavedení systému.
Databáze TE (Trusted Execution) byla změněna.	• Do databáze TE byly přidány binární soubory nebo z ní byly odebrány. • Binární soubory v databázi byly aktualizovány.	Spusťte příkaz **trustchk** a ověřte databázi.

Související pojmy:

“Příprava na nápravu situace” na stránce 5
Informace o funkci Trusted Boot popsané v tomto dokumentu slouží jako vodítko při určování situací, které mohou vyžadovat nápravu. Na proces zavádění systému nemají žádný vliv.

“Koncepce Trusted Boot” na stránce 4
Je důležité porozumět integritě procesu zavádění a způsobu klasifikace zavádění jako důvěryhodného nebo nedůvěryhodného.

Související informace:

Použití konzoly HMC

Trusted Firewall

Funkce Trusted Firewall poskytuje zabezpečení vrstvy virtualizace, jež zvyšuje výkon a efektivitu využívání prostředků při komunikaci mezi různými zónami zabezpečení virtuálních sítí LAN na stejném serveru Power Systems. Funkce Trusted Firewall snižuje zátěž externí sítě přesunutím možnosti filtrování balíků brány firewall splňujících určená pravidla do vrstvy virtualizace. Tato možnost filtrování je řízena snadno definovatelnými pravidly síťové filtrace, jež umožňují přecházení důvěryhodného síťového provozu mezi zónami zabezpečení virtuálních sítí LAN bez opuštění virtuálního prostředí. Funkce Trusted Firewall chrání a směruje interní síťový provoz mezi operačními systémy AIX, IBM i a Linux.

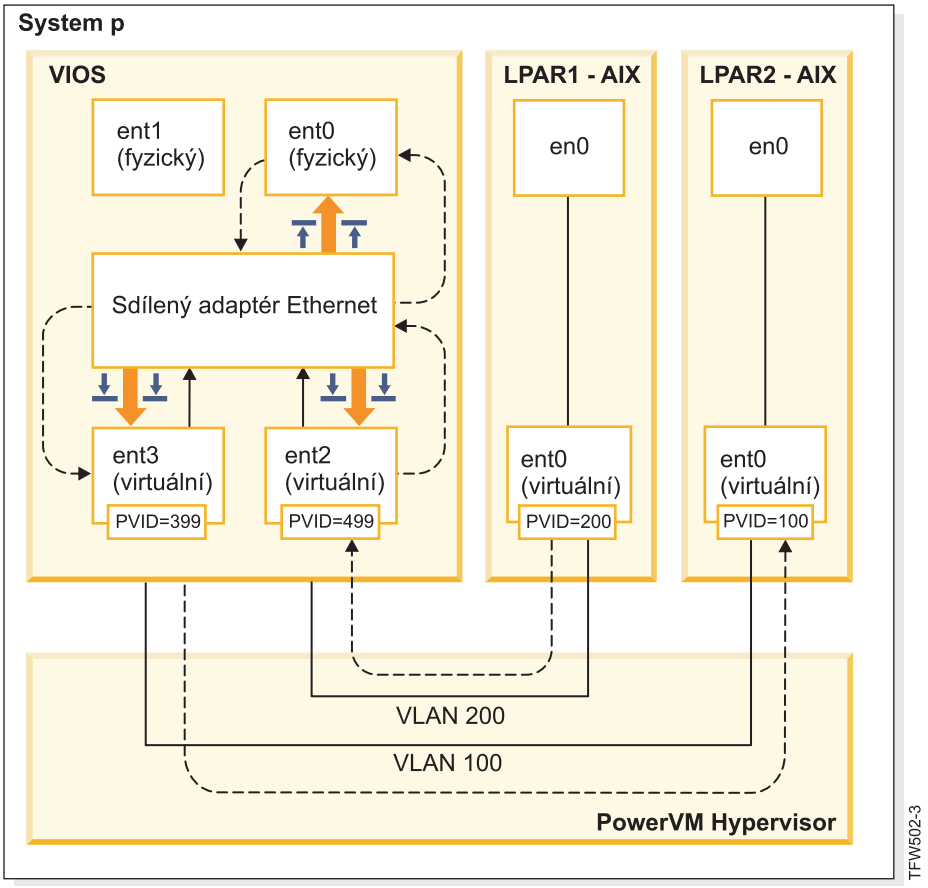
Koncepce funkce Trusted Firewall

Při používání funkce Trusted Firewall je vhodné porozumět její základní koncepci.

Hardware modulu Power Systems lze konfigurovat pro několik zón zabezpečení virtuálních sítí LAN. Zásady konfigurované uživatelem, které byly vytvořeny jako pravidlo filtrace funkce Trusted Firewall, umožňují důvěryhodnému provozu v síti přecházet mezi zónami zabezpečení virtuálních sítí LAN a zůstat pro vrstvu virtualizace interní. Tento princip je podobný zavedení fyzické brány firewall se síťovým připojením do virtualizovaného prostředí, což poskytuje metodu implementace možností brány firewall pro virtualizovaná datová střediska s vyšší efektivitou z hlediska výkonu.

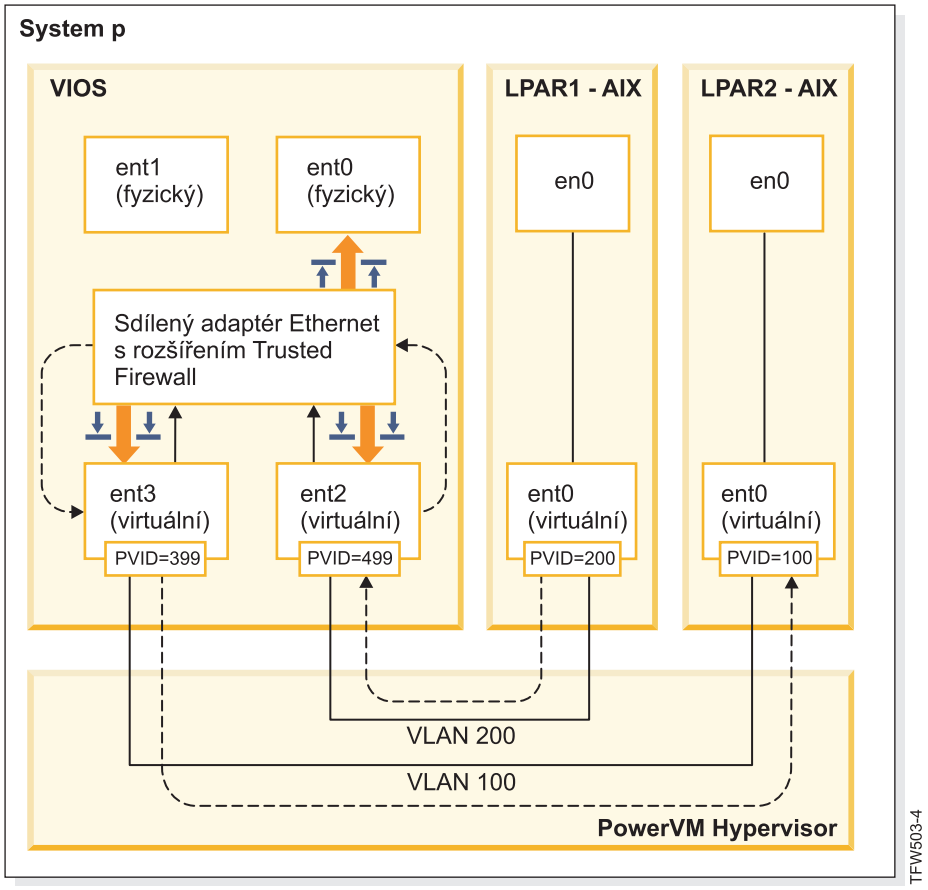
S použitím funkce Trusted Firewall můžete konfigurovat pravidla tak, aby byly povoleny určité typy provozu pro přímý přenos z jedné virtuální sítě LAN v rámci serveru Virtuální server I/O (Virtuální vstupně-výstupní server) do jiné virtuální sítě LAN v rámci téhož serveru Virtuální vstupně-výstupní server, přičemž stále zůstává zachována vysoká míra zabezpečení vzhledem k omezení jiných typů provozu. Jedná se o konfigurovatelnou bránu firewall v rámci vrstvy virtualizace serverů Power Systems.

V příkladu na obrázku Obrázek 1 na stránce 11 je cílem možnost zabezpečeného a efektivního přenosu informací z oblasti LPAR1 ve virtuální síti LAN 200 a z oblasti LPAR2 ve virtuální síti LAN 100. Není-li použita funkce Trusted Firewall, informace určené pro přenos do oblasti LPAR2 z oblasti LPAR1 jsou odeslány mimo interní síť do směrovače, který příslušné informace směruje zpět do oblasti LPAR2.



Obrázek 1. Příklad přenosu informací mezi virtuálními sítěmi LAN bez použití funkce Trusted Firewall

Prostřednictvím funkce Trusted Firewall můžete konfigurovat pravidla, která povolí předávání informací z oblasti LPAR1 do oblasti LPAR2, aniž by opustily interní síť. Trasa je znázorněna na obrázku Obrázek 2 na stránce 12.



Obrázek 2. Příklad přenosu informací mezi virtuálními sítěmi LAN s použitím funkce Trusted Firewall

Pravidla pro konfiguraci, která povolují zabezpečené přenášení určitých informací mezi virtuálními sítěmi LAN, zkracují trasu do místa určení. Funkce Trusted Firewall používá k povolení komunikace virtuální adaptér Ethernet a rozšíření jádra SVM (Security Virtual Machine).

Sdílený adaptér Ethernet
Sdílený adaptér Ethernet je místem, kde směrování začíná i končí. Po registraci modulu SVM obdrží sdílený adaptér Ethernet pakety a předá je modulu SVM. Pokud modul SVM určí, že je paket určen pro oblast LPAR na stejném serveru Power Systems, aktualizuje záhlaví vrstvy 2 paketu. Paket je vrácen sdílenému adaptéru Ethernet k předání do konečného místa určení buď v rámci systému, nebo v externí síti.

Security Virtual Machine
Modul SVM je místem, ve kterém jsou uplatněna pravidla filtrace. Pravidla filtrace jsou nutná kvůli zachování zabezpečení interní sítě. Po registraci modulu SVM ve sdíleném adaptéru Ethernet jsou pakety předávány modulu SVM před odesláním do externí sítě. Na základě aktivních pravidel filtrace modul SVM určí, zda paket zůstane v interní síti, nebo bude předán do externí sítě.

Instalace funkce Trusted Firewall

Instalace funkce PowerSC Trusted Firewall je podobná instalaci dalších funkcí modulu PowerSC.

Předpoklady:

- Verze modulu PowerSC nižší než 1.1.1.0 nemají k dispozici sadu souborů potřebnou pro instalaci funkce Trusted Firewall. Ověřte, že máte k dispozici instalační disk CD modulu PowerSC verze 1.1.1.0 nebo novější.
- Chcete-li využívat funkci Trusted Firewall, je třeba, aby již dříve byly prostřednictvím konzoly správy hardwaru (HMC) nebo serveru Virtuální server I/O (Virtuální vstupně-výstupní server) konfigurovány virtuální sítě LAN.

Funkce Trusted Firewall je k dispozici jako další sada souborů na instalačním disku CD modulu PowerSC Standard Edition. Název souboru je powerscStd.svm.rte. Funkci Trusted Firewall můžete přidat do existující instance modulu PowerSC verze 1.1.0.0 nebo novější, anebo ji nainstalovat jako součást nové instalace modulu PowerSC verze 1.1.1.0 nebo novější.

Přidání funkce Trusted Firewall do existující instance modulu PowerSC:

1. Ověřte, že je spuštěn server Virtuální vstupně-výstupní server verze 2.2.1.4 nebo novější.
2. Vložte instalační disk CD modulu PowerSC verze 1.1.1.0 nebo stáhněte obraz instalačního disku CD.
3. Použijte příkaz **oem_setup_env** pro přístup uživatele root.
4. Pomocí příkazu **installp** nebo nástroje SMIT nainstalujte sadu souborů PowerscStd.svm.rte.

Související informace:

“Instalace modulu PowerSC Standard Edition 1.1.3” na stránce 3
Je třeba nainstalovat sadu souborů pro každou konkrétní funkci modulu PowerSC Standard Edition.

Konfigurování funkce Trusted Firewall

Po instalaci funkce Trusted Firewall je potřebné vytvořit další nastavení konfigurace.

Monitorování funkce Trusted Firewall

V rámci monitorování funkce Trusted Firewall probíhá analýza provozu systému z různých logických oblastí (LPAR) s cílem poskytovat užitečné informace pro určování, zda spuštění funkce Trusted Firewall vede ke zvýšení výkonu systému.

Pokud funkce monitorování Trusted Firewall zaznamená výrazné množství provozu z různých virtuálních sítí LAN ve stejném komplexu CEC (Central Electronics Complex), mělo by povolení funkce Trusted Firewall přinést pro systém výhody.

Chcete-li povolit monitorování funkce Trusted Firewall, zadejte následující příkaz:

```
vlantfw -m
```

Chcete-li zobrazit výsledky monitorování funkce Trusted Firewall, zadejte následující příkaz:

```
vlantfw -D
```

Chcete-li zakázat monitorování funkce Trusted Firewall, zadejte následující příkaz:

```
vlantfw -M
```

Protokolování funkce Trusted Firewall

Protokolování funkce Trusted Firewall sestavuje seznam cest síťového provozu v komplexu CEC (Central Electronics Complex). V seznamu jsou uvedeny filtry, které funkce Trusted Firewall používá ke směrování provozu.

Když je v rámci monitorování funkce Trusted Firewall určeno, že interní provoz vede ke zvýšení efektivity, je v rámci protokolování funkce Trusted Firewall udržován seznam cest v souboru svm.log. Maximální velikost souboru svm.log je 16 MB. Pokud velikost překročí mezní hodnotu 16 MB, dojde k odebrání nejstarších položek ze souboru protokolu.

Chcete-li zahájit protokolování funkce Trusted Firewall, zadejte následující příkaz:

```
vlantfw -l
```

Chcete-li zastavit protokolování funkce Trusted Firewall, zadejte následující příkaz:

```
vlantfw -L
```

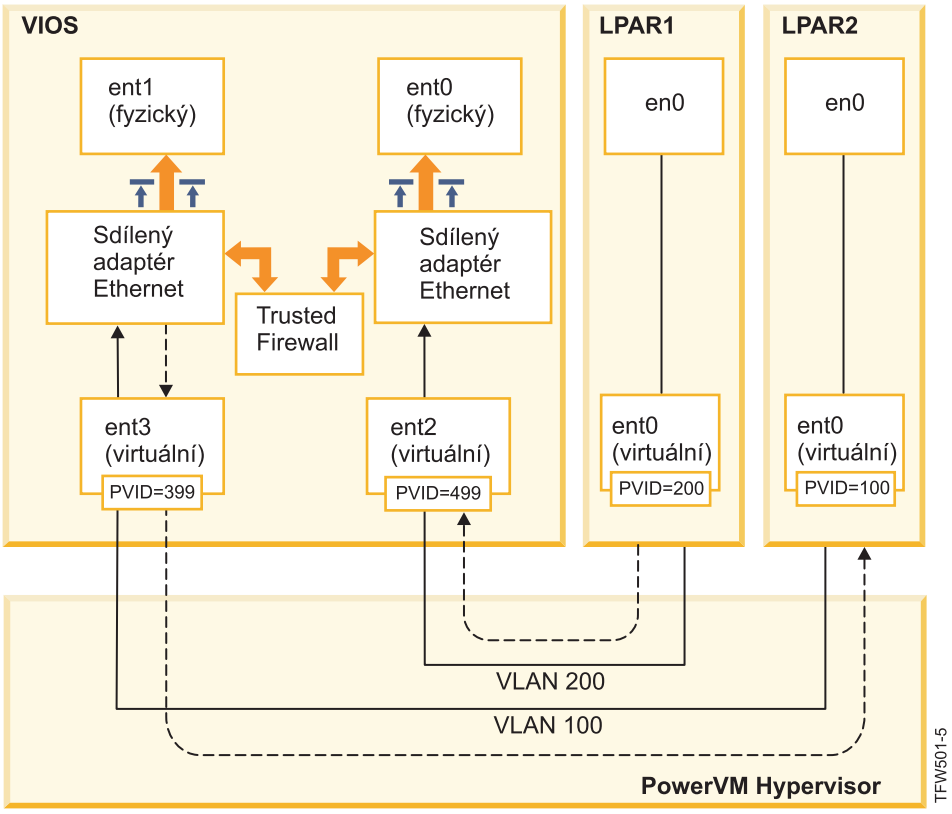
Soubor protokolu lze zobrazit v následujícím umístění: /home/padmin/svm/svm.log.

Několik sdílených adaptérů Ethernet

Funkci Trusted Firewall lze konfigurovat v systémech, které využívají několik sdílených adaptérů Ethernet.

Některé konfigurace používají několik sdílených adaptérů Ethernet v rámci téhož serveru Virtuální server I/O (Virtuální vstupně-výstupní server). Použití několika sdílených adaptérů Ethernet může přinášet výhody v podobě ochrany překonáním selhání a určování úrovně prostředků. Funkce Trusted Firewall podporuje směrování mezi několika sdílenými adaptéry Ethernet, pokud se nacházejí v rámci téhož serveru Virtuální vstupně-výstupní server.

Na obrázku Obrázek 3 je znázorněno prostředí s použitím několika sdílených adaptérů Ethernet.



Obrázek 3. Konfigurace s použitím několika sdílených adaptérů Ethernet v rámci jednoho serveru Virtuální vstupně-výstupní server

Dále jsou uvedeny příklady konfigurací s několika sdílenými adaptéry Ethernet podporovaných funkcí Trusted Firewall:

- Sdílené adaptéry Ethernet jsou konfigurovány s použitím kmenových adaptérů ve stejném virtuálním přepínači modulu Hypervisor Power. Tato konfigurace je podporována, protože každý sdílený adaptér Ethernet podporuje provoz v síti s různými ID virtuální sítě LAN.
- Sdílené adaptéry Ethernet jsou konfigurovány s použitím kmenových adaptérů v různých virtuálních přepínačích modulu Hypervisor Power a každý kmenový adaptér je přiřazen k jinému ID virtuální sítě LAN. V této konfiguraci každý sdílený adaptér Ethernet i nadále přijímá provoz v síti s použitím různých ID virtuální sítě LAN.
- Sdílené adaptéry Ethernet jsou konfigurovány s použitím kmenových adaptérů v různých virtuálních přepínačích modulu Hypervisor Power a ve virtuálních přepínačích jsou opakovaně používána tatáž ID virtuální sítě LAN. V tomto případě jsou pro provoz obou sdílených adaptérů Ethernet používána tatáž ID virtuální sítě LAN.

  Příkladem této konfigurace je oblast LPAR2 v síti VLAN200 s virtuálním přepínačem 10 a oblast LPAR3 v síti VLAN200 s virtuálním přepínačem 20. Jelikož obě oblasti LPAR a příslušné sdílené adaptéry Ethernet sdílejí totéž ID virtuální sítě LAN (VLAN200), mají oba sdílené adaptéry Ethernet přístup k paketům s tímto ID virtuální sítě LAN.

Přemostění nelze povolit pro více než jeden server Virtuální vstupně-výstupní server. Následující konfigurace s několika sdílenými adaptéry Ethernet proto nejsou funkcí Trusted Firewall podporovány:

- Několik serverů Virtuální vstupně-výstupní server a několik ovladačů sdílených adaptérů Ethernet.
- Sdílení zátěže u redundantních sdílených adaptérů Ethernet: Kmenové adaptéry konfigurované pro směrování mezi virtuálními sítěmi LAN nelze rozdělit mezi servery Virtuální vstupně-výstupní server.

Odebírání sdílených adaptérů Ethernet

Kroky při odebírání zařízení sdílených adaptérů Ethernet ze systému musí být prováděny v přesném pořadí.

Chcete-li odebrat sdílený adaptér Ethernet (SEA) ze systému, proveďte následující kroky:

1. Odeberte modul SVM (Security Virtual Machine) přidružen k příslušnému adaptéru SEA zadáním následujícího příkazu:

   ```
   rmdev -dev svm
   ```

2. Odeberte adaptér SEA zadáním následujícího příkazu:

   ```
   rmdev -dev ID_sdíleného_adaptéru_Ethernet
   ```

Poznámka: V případě odebrání adaptéru SEA před odebráním modulu SVM může dojít k selhání systému.

Vytváření pravidel

Můžete vytvářet pravidla pro povolení směrování mezi virtuálními sítěmi LAN s použitím funkce Trusted Firewall.

Chcete-li povolit funkce směrování v rámci modulu Trusted Firewall, je třeba vytvořit pravidla, která určují povolenou komunikaci. Z důvodu lepšího zabezpečení neexistuje jedno pravidlo, které by povolovalo komunikaci mezi všemi virtuálními sítěmi LAN v systému. Každé povolené připojení vyžaduje vlastní pravidlo, ačkoli každé aktivované pravidlo povoluje komunikaci mezi určenými koncovými body v obou směrech.

Jelikož vytváření pravidel probíhá v rámci rozhraní serveru Virtuální server I/O (Virtuální vstupně-výstupní server), jsou další informace o příkazech k dispozici v kolekci témat týkajících se serveru Virtuální vstupně-výstupní server v Informačním centru hardwaru Power Systems.

Chcete-li vytvořit pravidlo, proveďte následující kroky:

1. Otevřete rozhraní příkazového řádku serveru Virtuální vstupně-výstupní server.
2. Inicializujte ovladač modulu SVM zadáním následujícího příkazu:

   ```
   mksvm
   ```

3. Spusťte funkci Trusted Firewall zadáním následujícího příkazu:

   ```
   vlantfw -s
   ```

4. Zobrazte všechny známé adresy IP a MAC oblasti LPAR, zadejte následující příkaz:

   ```
   vlantfw -d
   ```

   Budete potřebovat adresy IP a MAC logických oblastí (LPAR), pro které vytváříte pravidla.

5. Vytvořte pravidlo filtrace pro povolení komunikace mezi oběma oblastmi LPAR ((LPAR1 a LPAR2) zadáním jednoho z následujících příkazů:
   - ```
     genvfilt -v4 -a P -z [ID_virtuální_sítě_LAN_oblasti_LPAR1] -Z [ID_virtuální_sítě_LAN_oblasti_LPAR2]
              -s [adresa_IP_oblasti_LPAR1] -d [adresa_IP_oblasti_LPAR2]
     ```
   - ```
     genvfilt -v4 -a P -z [ID_virtuální_sítě_LAN_oblasti_LPAR1] -Z [ID_virtuální_sítě_LAN_oblasti_LPAR2]
              -s [adresa_IP_oblasti_LPAR1] -d [adresa_IP_oblasti_LPAR2]
              -o any -p 0 -O gt -P 23
     ```

   Poznámka: Jedno pravidlo filtrace při výchozím nastavení povoluje komunikaci v obou směrech v závislosti na portu a položkách protokolu. Můžete například povolit pakety Telnet z oblasti LPAR1 do oblasti LPAR2 spuštěním následujícího příkazu:

   ```
   genvfilt -v4 -a-P -z [ID_virtuální_sítě_LAN_oblasti_LPAR1] -Z [ID_virtuální_sítě_LAN_oblasti_LPAR2]
            -s [adresa_IP_oblasti_LPAR1] -d [adresa_IP_oblasti_LPAR2]
            -o any -p 0 -O eq -P 23
   ```

6. Aktivujte všechna pravidla filtrace v jádru zadáním následujícího příkazu:

   ```
   mkvfilt -u
   ```

Poznámka: Tento postup aktivuje toto pravidlo i veškerá další pravidla filtrace, která v systému existují.

Další příklady

Následující příklady ilustrují několik dalších pravidel filtrace, která lze vytvořit s použitím funkce Trusted Firewall.

- Chcete-li povolit komunikaci se zabezpečením Secure Shell z oblasti LPAR ve virtuální síti LAN 100 do oblasti LPAR ve virtuální síti LAN 200, zadejte následující příkaz:
  ```
  genvfilt -v4 -a P -z 100 -Z 200 -o any -p 0 -O eq -P 22 -c tcp
  ```
- Chcete-li povolit provoz mezi všemi porty v rozsahu 0 až 499, zadejte následující příkaz:
  ```
  genvfilt -v4 -a P -z 100 -z 200 -o lt -p 500 -O lt -P 500 -c tcp
  ```
- Chcete-li mezi oblastmi LPAR povolit provoz TCP, zadejte následující příkaz:
  ```
  genvfilt -v4 -a P -z 100 -Z 200 -c tcp
  ```

  Neurčíte-li žádné porty nebo operace portu, bude provoz moci používat všechny porty.
- Chcete-li mezi oblastmi LPAR povolit zprávy protokolu ICMP (Internet Control Message Protocol), zadejte následující příkaz:
  ```
  genvfilt -v4 -a P -z 100 -Z 200 -c icmp
  ```

Související pojmy:

“Deaktivace pravidel”
V rámci funkce Trusted Firewall můžete deaktivovat pravidla umožňující směrování mezi virtuálními sítěmi LAN.

Související odkazy:

“Příkaz genvfilt” na stránce 32

“Příkaz mkvfilt” na stránce 34

“Příkaz vlantfw” na stránce 44

Související informace:

Virtual I/O Server (VIOS) = virtuální vstupně-výstupní server

Deaktivace pravidel

V rámci funkce Trusted Firewall můžete deaktivovat pravidla umožňující směrování mezi virtuálními sítěmi LAN.

Jelikož je deaktivace pravidel prováděna v rámci rozhraní serveru Virtuální server I/O (Virtuální vstupně-výstupní server), jsou v kolekci témat týkajících se serveru Virtuální vstupně-výstupní server v Informačním centru hardwaru Power Systems k dispozici další informace o příkazech a procesech.

Chcete-li deaktivovat pravidlo, proveďte následující kroky:

1. Otevřete rozhraní příkazového řádku serveru Virtuální vstupně-výstupní server.
2. Chcete-li zobrazit všechna aktivní pravidla filtrace, zadejte následující příkaz:
   ```
   lsvfilt -a
   ```

   Chcete-li zobrazit všechna pravidla filtrace uložená ve správci datových objektů (ODM), můžete příznak **-a** vynechat.
3. Všimněte si identifikačního čísla pravidla filtrace, jehož deaktivaci provádíte. V tomto příkladu má příslušné pravidlo filtrace identifikační číslo 23.
4. Deaktivujte pravidlo filtrace 23, je-li v jádru aktivní, zadáním následujícího příkazu:
   ```
   rmvfilt -n 23
   ```

   Chcete-li deaktivovat všechna pravidla filtrace v jádru, zadejte následující příkaz:
   ```
   rmvfilt -n all
   ```

Související pojmy:

“Vytváření pravidel” na stránce 15
Můžete vytvářet pravidla pro povolení směrování mezi virtuálními sítěmi LAN s použitím funkce Trusted Firewall.

Související odkazy:

“Příkaz lsvfilt” na stránce 33

“Příkaz rmvfilt” na stránce 43

Trusted Logging

Funkce PowerVM Trusted Logging umožňuje oblastem AIX LPAR zapisovat do souborů protokolu uložených na připojeném serveru Virtuální server I/O (Virtuální vstupně-výstupní server). Data jsou přenášena na server Virtuální vstupně-výstupní server přímo prostřednictvím modulu Hypervisor a není vyžadováno síťové připojení mezi oblastí LPAR klienta a serverem Virtuální vstupně-výstupní server.

Virtuální protokoly

Administrátor serveru Virtuální server I/O (Virtuální vstupně-výstupní server) vytváří a spravuje soubory protokolu. Tyto soubory jsou operačnímu systému AIX předávány jako zařízení virtuálního protokolu v adresáři /dev podobně jako virtuální disky či virtuální optická média.

Ukládání souborů protokolu v podobě virtuálních protokolů zvyšuje úroveň důvěryhodnosti záznamů, protože nemohou být změněny uživatelem s oprávněními uživatele root v oblasti LPAR klienta, v níž byly vygenerovány. K jedné oblasti LPAR klienta může být připojeno několik zařízení virtuálního protokolu a každý protokol představuje jiný soubor v adresáři /dev.

Funkce Trusted Logging umožňuje konsolidaci dat protokolu z více oblastí LPAR klienta do jednoho systému souborů, který je přístupný ze serveru Virtuální vstupně-výstupní server. Server Virtuální vstupně-výstupní server tudíž poskytuje jedno umístění v systému pro analýzu a archivaci protokolů. Administrátor oblasti LPAR klienta může konfigurovat aplikace a operační systém AIX tak, aby data byla zapisována do zařízení virtuálního protokolu, což je podobné zápisu dat do lokálních souborů. Subsystém auditu systému AIX lze konfigurovat tak, aby záznamy auditu byly přesměrovány do virtuálních protokolů. Další služby systému AIX, například systémový protokol, pracují s existující konfigurací a směrují data do virtuálních protokolů.

Má-li být konfigurován virtuální protokol, administrátor serveru Virtuální vstupně-výstupní server pro něj musí určit název, který sestává z následujících samostatných komponent:

- Název klienta
- Název protokolu

Administrátor serveru Virtuální vstupně-výstupní server může pro názvy obou komponent nastavit libovolné hodnoty, název klienta však obvykle bývá stejný pro všechny virtuální protokoly připojené k dané oblasti LPAR (například název hostitele příslušné oblasti LPAR). Název protokolu slouží k identifikaci účelu protokolu (například audit nebo systémový protokol).

V oblasti LPAR systému AIX je každé zařízení virtuálního protokolu reprezentováno dvěma funkčně ekvivalentními soubory v systému souborů /dev. První soubor má název podle příslušného zařízení, například /dev/vlog0, a název druhého souboru vznikne zřetězením předpony vl s názvem protokolu a číslem zařízení. Pokud například zařízení virtuálního protokolu vlog0 používá název protokolu audit, bude v systému souborů /dev reprezentováno soubory vlog0 a vlaudit0.

Související informace:

Vytváření virtuálních protokolů

Zjišťování zařízení virtuálního protokolu

Poté, co administrátor serveru VIOS vytvořil zařízení virtuálního protokolu a připojil je k oblasti LPAR klienta, jde třeba aktualizovat konfiguraci zařízení oblasti LPAR klienta, aby zařízení byla viditelná.

Administrátor oblasti LPAR klienta může aktualizovat nastavení pomocí jedné z následujících metod:

- Opětné zavedení oblasti LPAR klienta.
- Spuštění příkazu **cfgmgr**.

Spuštění příkazu **lsdev** s cílem zobrazit zařízení virtuálního protokolu. Při výchozím nastavení mají tato zařízení předponu vlog. V následujícím příkladu je uveden výstup příkazu **lsdev** v oblasti LPAR systému AIX, jež obsahuje dvě zařízení virtuálního protokolu:

```
lsdev
vlog0  Zařízení virtuálního protokolu
vlog1  Zařízení virtuálního protokolu
```

Vlastnosti konkrétního zařízení virtuálního protokolu lze přezkoumat pomocí příkazu lsattr –El <*název_zařízení*>, jehož výstup je podobný následujícímu:

```
lsattr –El vlog0
PCM                          Modul řízení cesty                          Ne
název_klienta      dev-lpar-05 Název klienta                               Ne
název_zařízení     vlsyslog0   Název zařízení                              Ne
název_protokolu    syslog      Název protokolu                             Ne
max_vel_protokolu  4194304     Maximální velikost datového souboru protokolu   Ne
max_vel_stav_soub  2097152     Maximální velikost stavového souboru protokolu  Ne
pvid               žádné       Identifikátor fyzického disku               Ne
```

Tento výstup obsahuje název klienta, název zařízení a množství dat protokolu, která mohou být v rámci serveru VIOS uložena.

Ve virtuálním protokolu jsou uloženy následující dva typy údajů protokolu:

- Údaje protokolu: Prvotní data protokolu vygenerované aplikacemi oblasti LPAR systému AIX.
- Údaje o stavu: Informace o době konfigurování, otevření, zavření a dalších operacích pro zařízení, jež slouží k analýze aktivity protokolu.

Administrátor serveru VIOS určuje množství **údajů protokolu** a **údajů o stavu**, které lze uložit pro každý virtuální protokol. Množství je určeno atributy max_log_size a max_state_size. Pokud množství uložených dat překročí určenou mezní hodnotu, budou nejstarší údaje protokolu přepsány. Administrátor serveru VIOS musí zaručit časté shromažďování a archivování údajů protokolu, aby zůstaly protokoly zachovány.

Instalace funkce Trusted Logging

Funkci PowerSC Trusted Logging lze nainstalovat prostřednictvím rozhraní příkazového řádku nebo nástroje SMIT.

Předpokladem pro instalaci funkce Trusted Logging je server Virtuální vstupně-výstupní server 2.2.1.0 nebo novější a systém IBM AIX 6 s úrovní technologie 7 nebo IBM AIX 7 s úrovní technologie 1.

Název souboru pro instalaci funkce Trusted Logging je powerscStd.vlog. Soubor je k dispozici na instalačním disku CD modulu PowerSC Standard Edition.

Instalace funkce Trusted Logging:

1. Ověřte, že je spuštěn server Virtuální vstupně-výstupní server verze 2.2.1.0 nebo novější.
2. Vložte instalační disk CD modulu PowerSC nebo stáhněte obraz instalačního disku CD.
3. Pomocí příkazu **installp** nebo nástroje SMIT nainstalujte sadu souborů powerscStd.vlog.

| **Související informace**:
| “Instalace modulu PowerSC Standard Edition 1.1.3” na stránce 3
| Je třeba nainstalovat sadu souborů pro každou konkrétní funkci modulu PowerSC Standard Edition.

Konfigurování funkce Trusted Logging

Seznamte se s postupem při konfigurování funkce Trusted Logging v subsystému auditu systému AIX a v systémovém protokolu.

Konfigurování subsystému auditu systému AIX

Subsystém auditu systému AIX lze konfigurovat tak, aby kromě zapisování protokolů do lokálního systému souborů zapisoval binární data i do virtuálního protokolovacího zařízení.

Poznámka: Před konfigurováním subsystému auditu systému AIX je třeba provést postup uvedený v části “Zjišťování zařízení virtuálního protokolu” na stránce 17.

Chcete-li konfigurovat subsystém auditu systému AIX, proveďte následující kroky:

1. Konfigurujte subsystém auditu systému AIX tak, aby protokoloval data v binárním režimu (auditbin).
2. Aktivujte funkci Trusted Logging pro auditování systému AIX úpravou konfiguračního souboru /etc/security/audit/config.
3. Přidejte parametr virtual_log = /dev/vlog0 do oddílu bin:.

   Poznámka: Pokyn je platný, pokud administrátor oblasti LPAR chce, aby byla data programu auditbin zapisována do umístění /dev/vlog0.
4. Restartujte subsystém auditu systému AIX provedením příkazů v následujícím pořadí:

   ```
   audit shutdown
   audit start
   ```

Záznamy auditu budou kromě zapsání protokolů do lokálního systému souborů zapsány i na server Virtuální server I/O (Virtuální vstupně-výstupní server) prostřednictvím určeného zařízení virtuálního protokolování. Protokoly jsou uloženy podle určení existujících parametrů bin1 a bin2 v oddílu bin: konfiguračního souboru /etc/security/audit/config.

Související informace:

Subsystém auditování

Konfigurování systémového protokolu

Systémový protokol lze konfigurovat tak, aby byly zprávy zapisovány do virtuálních protokolů. Lze tak učinit přidáním pravidel do souboru /etc/syslog.conf.

Poznámka: Před konfigurováním souboru /etc/syslog.conf je třeba provést postup uvedený v části “Zjišťování zařízení virtuálního protokolu” na stránce 17.

Soubor /etc/syslog.conf lze upravit tak, aby odpovídal zprávám protokolu založeným na následujících kritériích:

- zařízení,
- úroveň priority.

Chcete-li pro zprávy systémového protokolu používat virtuální protokoly, musí být soubor /etc/syslog.conf konfigurován s použitím pravidel pro zápis požadovaných zpráv do příslušného virtuálního protokolu v adresáři /dev.

Chcete-li například odesílat zprávy na úrovni ladění, jež byly vygenerovány kterýmkoli zařízením, do virtuálního protokolu vlog0, přidejte do souboru /etc/syslog.conf následující řádek:

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

Poznámka: Pro žádný příkaz, který zapisuje data do virtuálních protokolů, nepoužívejte zařízení pro cyklické ukládání do protokolů, která jsou k dispozici v rámci démona syslogd. Soubory v systému souborů /dev nejsou běžnými soubory a nelze je přejmenovávat a přesouvat. Cyklické ukládání do virtuálních protokolů musí v rámci serveru VIOS nastavit jeho administrátor.

Po vytvoření konfigurace je třeba démona syslogd restartovat pomocí následujícího příkazu:

```
refresh -s syslogd
```

Související informace:

Démon syslogd

Zápis dat do virtuálních protokolovacích zařízení

Do virtuálního protokolovacího zařízení lze zapsat libovolná data. Po otevření příslušného souboru v adresáři /dev je proveden zápis dat do souboru. Virtuální protokol může být otevřen vždy pouze jedním procesem.

Příklad:

Chcete-li zapisovat zprávy do virtuálních protokolovacích zařízení pomocí příkazu **echo**, zadejte následující příkaz:

```
echo "Zpráva protokolu" > /dev/vlog0
```

Chcete-li ukládat soubory do virtuálních protokolovacích zařízení pomocí příkazu **cat**, zadejte následující příkaz:

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

Maximální velikost jednoho zápisu je omezena na 32 kB a programy, které se v rámci jedné operace zápisu pokusí zapsat více dat, obdrží chybu vstupu/výstupu (EIO). Obslužné programy rozhraní příkazového řádku, jako je například příkaz **cat**, automaticky rozdělují přenesená data do operací zápisu o velikosti 32 kB.

Funkce Trusted Network Connect and Patch Management

Funkce TNC (Trusted Network Connect) je součástí skupiny TCG (Trusted Computing Group), jež poskytuje specifikace pro ověření integrity koncových bodů. Funkce TNC definovala architekturu otevřených řešení, která administrátorům usnadňuje prosazování zásad pro účinné řízení přístup k síťové infrastruktuře.

Koncepce funkce Trusted Network Connect

Seznamte se s informacemi o komponentách, konfigurování zabezpečené komunikace a systému správy oprav funkce TNC (Trusted Network Connect).

Komponenty funkce Trusted Network Connect

Seznamte se s informacemi o komponentách funkce TNC (Trusted Network Connect).

Model TNC sestává z následujících komponent:

Server Trusted Network Connect:

Server TNC (Trusted Network Connect) identifikuje klienty přidané do sítě a zahájí jejich ověřování.

Klient TNC poskytuje požadované informace o úrovni sady souborů pro ověření na serveru. Server určuje, zda se klient nachází na úrovni konfigurované administrátorem. Pokud klient neodpovídá požadavkům, server TNC upozorní administrátora na nutnost nápravy situace.

Server TNC zahájí ověřování klientů, kteří se pokoušejí o přístup k síti. Server TNC načte sadu ověřovacích modulů měření integrity (IMV), které mohou od klientů vyžadovat měření integrity a ověřovat je. Pro systém AIX existuje výchozí modul IMV, který ověřuje úroveň sady souborů a opravy zabezpečení systémů. Server TNC představuje strukturu načítající a spravující několik modulů IMV. Při ověřování klientů spoléhá na moduly IMV, které si z klientů vyžádají informace, a provádí ověřování klientů.

Správa oprav:

Server TNC (Trusted Network Connect) je integrován s modulem SUMA s cílem poskytovat řešení správy oprav.

Modul SUMA systému AIX stahuje nejnovější opravy zabezpečení a aktualizace, které jsou k dispozici na webu IBM ECC and Fix Central. Funkce TNC a démon správy oprav předají serveru TNC nejnovější aktualizované informace, jež slouží jako základní sada souborů pro ověřování klientů.

Démon **tncpmd** musí být konfigurován pro správu stahování modulu SUMA (Průvodce správou servisních aktualizací) a pro předávání informací o sadách souborů na server TNC. Hostitelem tohoto démona musí být systém připojený k Internetu, aby bylo možné stahovat aktualizace automaticky. Chcete-li používat server pro správu oprav TNC bez připojení k Internetu, můžete na serveru pro správu oprav TNC zaregistrovat úložiště oprav definované uživatelem.

Poznámka: Hostitelem serveru TNC a démona **tncpmd** může být tentýž systém.

Klient Trusted Network Connect:

Klient TNC (Trusted Network Connect) poskytuje informace požadované serverem TNC kvůli ověření.

Server určuje, zda se klient nachází na úrovni konfigurované administrátorem. Pokud klient neodpovídá požadavkům, server TNC upozorní administrátora na nutnost provedení aktualizací.

Klient TNC načte při spuštění kolektory měření integrity (IMC) a pomocí těchto kolektorů IMC shromažďuje požadované informace.

Modul IP Referrer funkce Trusted Network Connect:

Server funkce TNC (Trusted Network Connect) může automaticky zahájit ověřování v klientech, kteří jsou připojeni k síti. Modul IP Referrer spuštěný v oblasti se serverem Virtuální server I/O (Virtuální vstupně-výstupní server) zjišťuje nové klienty obsluhované serverem Virtuální vstupně-výstupní server a odesílá jejich adresy IP na server TNC. Server TNC ověřuje klienta podle definovaných zásad.

Zabezpečená komunikace funkce Trusted Network Connect

Démoni funkce TNC (Trusted Network Connect) komunikují prostřednictvím šifrovaných kanálů s povoleným zabezpečením TLS (Transport Layer Security) nebo SSL (Secure Sockets Layer).

Účelem zabezpečené komunikace je zajistit ověřování a zabezpečení dat přenášených v síti. Každý systém musí mít vlastní klíč a certifikát. Jejich generování je provedeno po spuštění inicializačního příkazu pro příslušné komponenty. Tento proces je pro administrátora zcela transparentní a vyžaduje nižší míru jeho zapojení.

| Chcete-li ověřit nového klienta, je třeba importovat do databáze na serveru certifikát příslušného klienta. Certifikát je
| nejprve označen jako nedůvěryhodný. Administrátor poté pomocí příkazu **psconf** zobrazí certifikáty a označí je jako
| důvěryhodné zadáním následujícího příkazu:

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

| Chcete-li použít jiný klíč a certifikát, příkaz **psconf** umožňuje importovat certifikát prostřednictvím příslušné volby.

| Chcete-li importovat certifikát ze serveru, zadejte následující příkaz:

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

| Chcete-li importovat certifikát z klienta, zadejte následující příkaz:

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

Protokol Trusted Network Connect

Protokol TNC (Trusted Network Connect) je používán v kombinaci se strukturou TNC pro údržbu integrity sítě.

Funkce TNC poskytuje specifikace pro ověřování integrity koncových bodů. Koncové body požadující přístup jsou posouzeny na základě měření integrity kritických komponent, které mohou mít vliv na příslušné provozní prostředí. Struktura TNC umožňuje administrátorům monitorovat integritu systémů v síti. Funkce TNC je integrována s infrastrukturou pro distribuci oprav systému AIX s cílem vytvořit úplné řešení pro správu oprav.

Specifikace funkce TNC musí splňovat požadavky architektury systémů AIX a řada POWER. Komponenty funkce TNC jsou navrženy tak, aby poskytovaly úplné řešení pro správu oprav v operačním systému AIX. Tato konfigurace umožňuje administrátorům efektivně spravovat konfigurace softwaru v implementacích systému AIX. Poskytuje nástroje pro ověřování úrovní oprav systémů a generování sestav pro klienty, kteří neodpovídají požadavkům. Správa oprav navíc usnadňuje proces stahování oprav a jejich instalace.

Moduly IMC a IMV

Server a klient TNC (Trusted Network Connect) interně používají pro ověřování serverů moduly IMC (Integrity Measurement Collector) a IMV (Integrity Measurement Verifier).

Tato struktura umožňuje načtení několika modulů IMC a IMV na server a do klientů. Modul, který provádí ověřování úrovně operačního systému a sady souborů, je při výchozím nastavení dodáván spolu s operačním systémem AIX. Moduly dodávané spolu s operačním systémem AIX jsou přístupné prostřednictvím následujících cest:

- /usr/lib/security/tnc/libfileset_imc.a: Shromáždí informace o úrovni operačního systému a o sadě souborů nainstalované z klientského systému a odešle je k ověření do modulu IMV (server TNC).
- /usr/lib/security/tnc/libfileset_imv.a: Vyžádá si informace o úrovni operačního systému a sadě souborů z klienta a porovná je se základními informacemi. Provede také aktualizaci stavu klienta v databázi serveru TNC. Stav lze zobrazit zadáním následujícího příkazu:

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

Související odkazy:

“Příkaz psconf” na stránce 38

Instalace funkce Trusted Network Connect

Instalace komponent funkce TNC (Trusted Network Connect) vyžaduje provedení určitých kroků.

Chcete-li konfigurovat nastavení pro používání komponent funkce TNC, proveďte následující kroky:

1. Určete adresy IP systémů pro nastavení serveru TNC, serveru TNCPM (Trusted Network Connect and Patch Management) a modulu IP Referrer funkce TNC pro server Virtuální server I/O (Virtuální vstupně-výstupní server).

   Poznámka: Server TNC nelze konfigurovat jako klienta TNC.
2. Nastavte server správy NIM (Network Installation Management). Systém konfigurovaný jako server je hlavním počítačem správy NIM a v systému klienta musí být nainstalovány sady souborů sets:bos.sysmgt.nim.master.
3. Konfigurujte server TNCPM. Tuto konfiguraci lze vytvořit v systému správy NIM. Server TNCPM využívá nástroj SUMA ke stahování oprav z webů IBM Fix Central a ECC. Chcete-li stahovat aktualizace, musí být systém připojen k Internetu. Chcete-li konfigurovat server TNCPM, zadejte následující příkaz:

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

   Příklad:

   ```
   pmconf mktncpm pmport=20000 tncserver=1.1.1.1:10000
   ```
4. Konfigurujte zásady na serveru TNC. Informace o vytváření zásad pro ověřování klientů naleznete v tématu “Vytváření zásad pro klienta Trusted Network Connect” na stránce 26.
5. Konfigurujte modul IP Referrer funkce TNC v rámci serveru Virtuální vstupně-výstupní server. Tato konfigurace v rámci serveru Virtuální vstupně-výstupní server spouští ověřování klientů, kteří se připojují k síti. Chcete-li konfigurovat modul IP Referrer, zadejte následující příkaz:

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

   Příklad:

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

Poznámka: Hodnota portu serveru a portu TNC (portu klienta) musí být stejná.

6. Konfigurujte klienty pomocí následujícího příkazu:

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

Příklad:

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

Související odkazy:

"Příkaz psconf" na stránce 38

Související informace:

"Instalace modulu PowerSC Standard Edition 1.1.3" na stránce 3
Je třeba nainstalovat sadu souborů pro každou konkrétní funkci modulu PowerSC Standard Edition.

Instalace s využitím správy NIM

IBM Fix Central

Středisko nápovědy online pro službu Passport Advantage

Konfigurování funkce Trusted Network Connect and Patch Management

Funkci TNC (Trusted Network Connect) je třeba konfigurovat jako démona správce oprav. Server TNC je integrován s modulem SUMA s cílem poskytovat komplexní řešení správy oprav.

Konfigurování serveru Trusted Network Connect

Seznamte se s kroky prováděnými při konfigurování serveru TNC.

Chcete-li konfigurovat server TNC, musí soubor /etc/tnccs.conf obsahovat hodnotu podobnou následující:

```
component = SERVER
```

Chcete-li systém konfigurovat jako server, zadejte následující příkaz:

```
psconf mkserver tncport=<port> pmserver=<adresa_IP|název_hostitele[,adresa_IP_2|název_hostitele_2..]:port>
[recheck_interval=<čas_v_minutách>]
```

Příklad:

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

Poznámka: Porty tncport a pmserver musí být nastaveny na rozdílné hodnoty, a pokud není zadán parametr recheck_interval, bude použita výchozí hodnota 1440 minut.

Pro port tncport je použita výchozí hodnota 42830 minut a pro port pmserver je použita výchozí hodnota 38240 minut.

Související odkazy:

"Příkaz psconf" na stránce 38

Konfigurování klienta Trusted Network Connect

Seznamte se s kroky při konfigurování klienta TNC (Trusted Network Connect) a potřebnými nastaveními konfigurace.

Chcete-li konfigurovat klienta TNC, musí soubor /etc/tnccs.conf obsahovat hodnotu podobnou následující:

```
component = CLIENT
```

Chcete-li systém konfigurovat jako klienta, zadejte následující příkaz:

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

Příklad:

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

Poznámka: Hodnota portu serveru a portu klienta (tncport) musí být stejná.

Související odkazy:

"Příkaz psconf" na stránce 38

Konfigurování serveru pro správu oprav

Seznamte se s postupem při konfigurování systému jako serveru pro správu oprav.

Server pro správu oprav TNC (Trusted Network Connect) musí být konfigurován na serveru správy NIM (Network Installation Management), aby bylo možné aktualizovat klienty TNC.

Chcete-li inicializovat úložiště oprav pro správu oprav TNC, zadejte následující příkaz:

```
pmconf init -i <interval_stahování> -l <seznam_úrovní_technologie> [-A] [-P <cesta_stahování>]
[-x <interval_oprav_ifix>] [-K <klíč_opravy_ifix>]
```

Příklad použití příkazu **pmconf**:

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

Příkaz **init** stáhne nejnovější opravnou sadu pro každou úroveň technologie a zpřístupní ji pro server TNC. Aktualizované opravné sady umožňují serveru TNC provádět základní ověřování klientů TNC a serveru pro správu oprav TNC umožňují instalovat aktualizace klienta TNC. Chcete-li při provádění aktualizací klientů přijmout všechny licenční smlouvy, určete příznak **-A**. Při výchozím nastavení se úložiště oprav stažených serverem pro správu oprav TNC nacházejí v souboru /var/tnc/tncpm/fix_repository. Jiný adresář lze určit pomocí příznaku **-P**.

Chcete-li povolit automatické stahování údajů IBM Security Advisory a prozatímních oprav, můžete určit interval prozatímních oprav. Tato funkce umožňuje automatické oznamování nově vydaných prozatímních oprav zabezpečení a přidružených identifikátorů běžných rizik a míst ohrožení (CVE). Všechny údaje Security Advisory a prozatímní opravy jsou před registrací v rámci funkce TNC ověřovány. Veřejný klíč pro případ ohrožení zabezpečení systému IBM AIX, který je vyžadován pro automatické stahování prozatímních oprav, je k dispozici na webu zabezpečení systému IBM AIX. Automatické stahování opravných sad a prozatímních oprav lze zakázat nastavením intervalu stahování i intervalu prozatímních oprav na hodnotu 0.

Registraci opravných sad a prozatímních oprav lze aktualizovat také ručně. Chcete-li položku IBM Security zaregistrovat ručně spolu s příslušnými prozatímními opravami, zadejte následující příkaz:

```
pmconf add -y <soubor_Advisory> -v <soubor_s_podpisem>  -e <soubor_TAR_opravy_ifix>
```

Chcete-li ručně registrovat samostatnou prozatímní opravu, zadejte následující příkaz:

```
pmconf add -p <opravná_sada> -e <soubor_ifix>
```

Chcete-li registrovat novou úroveň technologie a stáhnout příslušnou nejnovější opravnou sadu, zadejte následující příkaz:

```
pmconf add -l <seznam_úrovní_technologie>
```

Chcete-li stáhnout opravnou sadu jiné než aktuální verze nebo úroveň technologie, která má být použita pro ověřování a aktualizace klientů, zadejte následující příkaz:

```
pmconf add -l <seznam_úrovní_technologie> -d
pmconf add -s <seznam_opravných_sad>
```

Chcete-li registrovat úložiště oprav pro opravné sady nebo úrovně technologie, které v systému existuje, zadejte následující příkaz:

```
pmconf add -s <opravná_sada> -p <úložiště_oprav_definované_uživatelem>
pmconf add -l <úroveň_technologie> -p <úložiště_oprav_definované_uživatelem>
```

Chcete-li systém konfigurovat tak, aby sloužil jako server pro správu oprav, zadejte následující příkaz:

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

Příklad použití tohoto příkazu:

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

Server pro správu oprav TNC vždy podporuje správu oprav zabezpečení APAR (Authorized Problem Analysis Report). Chcete-li konfigurovat správu oprav TNC tak, aby bylo možné spravovat jiné typy oprav APAR, zadejte následující příkaz:

```
pmconf add -t <seznam_typů_oprav_APAR>
```

V předchozím příkladu parametr <seznam_typů_oprav_APAR> obsahuje seznam následujících typů oprav APAR (s čárkami jako oddělovači):

- HIPER
- PE
- Rozšíření

Server pro správu oprav TNC podporuje příkaz **syslog** pro stahování aktualizací opravných sad, úrovní technologie a klientů. Prostředek má hodnotu user a priorita má hodnotu info. Příkladem je zápis user.info.

Server pro správu oprav TNC rovněž udržuje protokol se všemi aktualizacemi klientů v adresáři /var/tnc/tncpm/log/update/<adresa_IP>/<časový_údaj>.

Související odkazy:

"Příkaz psconf" na stránce 38

Související informace:

Zabezpečení systému IBM AIX

Konfigurování e-mailových oznámení serveru Trusted Network Connect

Seznamte se s postupem při konfigurování e-mailových oznámení pro server TNC (Trusted Network Connect).

Server TNC zobrazí úroveň oprav klienta. Pokud zjistí neshodu klienta, odešle administrátorovi e-mail s výsledkem a popisem potřebné nápravy situace.

Chcete-li konfigurovat e-mailovou adresu administrátora, zadejte následující příkaz:

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

Příklad:

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

V předchozím příkladu by e-mail pro skupinu adres IP *vayugrp1* a *vayugrp2* byl odeslán na e-mailovou adresu abc@ibm.com.

Chcete-li odeslat e-mail na globální e-mailovou adresu pro skupinu adres IP, které není přiřazena e-mailová adresa, zadejte následující příkaz:

```
psconf add –e <e-mailová_adresa>
```

Příklad:

```
psconf add –e abc@ibm.com
```

V předchozím příkladu by byl e-mail odeslán na e-mailovou adresu abc@ibm.com, není-li skupině adres IP přiřazena e-mailová adresa. Tato adresa slouží jako globální e-mailová adresa.

Související odkazy:

"Příkaz psconf" na stránce 38

Konfigurování modulu IP Referrer na serveru VIOS

Seznamte se s postupem konfigurování modulu IP Referrer na serveru Virtuální server I/O (Virtuální vstupně-výstupní server) s cílem automaticky zahajovat ověřování.

Poznámka: Na serveru VIOS (Virtuální vstupně-výstupní server) je třeba konfigurovat rozšíření jádra SVM předtím, než budete konfigurovat modul IP Referrer.

Chcete-li konfigurovat modul IP Referrer funkce TNC, musí konfigurační soubor /etc/tnccs.conf obsahovat nastavení podobné následujícímu: component = IPREF.

| Systém lze konfigurovat jako klienta zadáním následujícího příkazu:

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

| Příklad:

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

| Hodnota portu tncserver a portu klienta (tncport) musí být stejná.

Související odkazy:

"Příkaz psconf" na stránce 38

Správa funkce Trusted Network Connect and Patch Management

Seznamte se postupy správy funkce TNC (Trusted Network Connect) s cílem implementovat úlohy, jako je přidávání klientů, zásad, protokolů, výsledků ověřování a certifikátů souvisejících s funkcí TNC.

Zobrazení protokolů serveru Trusted Network Connect

Seznamte se s postupem při zobrazování protokolů serveru TNC (Trusted Network Connect).

| Server TNC zaznamenává výsledky ověřování všech klientů. Chcete-li protokol zobrazit, spusťte příkaz **psconf**:

```
psconf list –H –i <ip |ALL>
```

| **Související odkazy**:

"Příkaz psconf" na stránce 38

Vytváření zásad pro klienta Trusted Network Connect

Seznamte se s postupem při vytváření zásad týkajících se klienta TNC (Trusted Network Connect).

| Konzola příkazu psconf poskytuje rozhraní potřebné pro správu zásad funkce TNC. K některé zásadě lze přidružit
| každého klienta či skupinu klientů.

Vytvořit lze následující zásady:

- Skupina adres IP (Internet Protocol) obsahuje několik adres IP klientů.
- Každá adresa IP klienta může náležet pouze do jedné skupiny.
- Skupina adres IP je přidružena ke skupině zásad.
- Skupina zásad obsahuje různé druhy zásad. Příklad: zásady pro sady souborů, jež určují požadovanou úroveň operačního systému klienta (tedy vydání, úroveň technologie a opravnou sadu). Skupina zásad může obsahovat více zásad pro sady souborů a klient odkazující na tyto zásady musí být na úrovni určené jednou ze zásad pro sady souborů.

Následující příkazy ilustrují postup při vytváření skupiny adres IP, skupiny zásad a zásad pro sady souborů.

| Chcete-li vytvořit skupinu adres IP, zadejte následující příkaz:

| `psconf add –G <název_skupiny_adres_IP> ip=[±]<adresa_IP_1,adresa_IP_2,adresa_IP_3 ...>`

| Příklad:
| `psconf add –G myipgrp ip=1.1.1.1,2.2.2.2`

| **Poznámka:** V případě skupiny je třeba uvést alespoň jednu adresu IP. Více adres IP je třeba oddělit čárkami.

| Chcete-li vytvořit zásady pro sady souborů, zadejte následující příkaz:
| `psconf add –F <název_zásad_sady_souborů> <vyd00-úroveň_technologie_opravná_sada>`

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

| **Poznámka:** Informace o sestavení musí být uvedeny ve formátu <vyd00-úroveň_technologie_opravná_sada>.

| Chcete-li vytvořit zásady a přiřadit skupinu adres IP, zadejte následující příkaz:
| `psconf add –P <název_zásad> ipgroup=[±] <skupina_adres_IP_1, skupina_adres_IP_2 ...]`

| Příklad:
| `psconf add –P mypol ipgroup=myipgrp,myipgrp1`

Chcete-li k zásadám přiřadit zásady pro sady souborů, zadejte následující příkaz:
`psconf add –P <název_zásad> fspolicy=[±]<zásady_pro_sady_souborů_1, zásady_pro_sady_souborů_fspol2 ...>`

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

Poznámka: Je-li uvedeno několik zásad pro sady souborů, systém v klientu vynutí zásady s nejvyšší mírou shody. Pokud je například klient na úrovni 6100-02-01 a určíte zásady pro sady souborů jako úroveň 7100-03-04 a 6100-02-03, bude v klientu vynucena úroveň 6100-02-03.

Související odkazy:

“Příkaz psconf” na stránce 38

Zahájení ověřování pro klienta Trusted Network Connect

Seznamte se s postupem při ověřování klienta TNC (Trusted Network Connect).

Při ověřování klienta můžete použít jednu z následujících metod:

- Démon modulu IP Referrer v rámci serveru Virtuální server I/O (Virtuální vstupně-výstupní server) předá adresu IP klienta na server TNC: Oblast LPAR klienta obdrží adresu IP a pokusí se o přístup k síti. Démon modulu IP Referrer v rámci serveru Virtuální vstupně-výstupní server zjistí novou adresu IP a předá ji na server TNC: Server TNC po přijetí nové adresy IP zahájí ověřování.
- Server TNC pravidelně ověřuje klienta: Administrátor může přidat adresy IP klientů k ověření do databáze zásad funkce TNC. Server TNC ověří klienty uvedené v databázi. Opětně ověřování probíhá automaticky v pravidelných intervalech podle hodnoty atributu recheck_interval určené v konfiguračním souboru /etc/tnccs.conf.
- Administrátor zahájí ověřování klienta ručně: Administrátor může ručně zahájit ověřování, zda byl klient přidán do sítě, spuštěním následujícího příkazu:
  `tncconsole verify -i <adresa_IP>`

Poznámka: V případě prostředků, jež nejsou připojeny k serveru Virtuální vstupně-výstupní server, lze klienty ověřit a aktualizovat po jejich ručním přidání na server TNC.

Související odkazy:

“Příkaz psconf” na stránce 38

Zobrazování výsledků ověřování funkce Trusted Network Connect

Seznamte se s postupem při zobrazování výsledků ověřování klienta TNC (Trusted Network Connect).

Chcete-li zobrazit výsledky ověřování klientů v síti, zadejte následující příkaz:

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

Tento příkaz zobrazí všechny klienty se stavem **IGNOROVÁNO**, **SHODA** nebo **SELHÁNÍ**.

- **IGNOROVÁNO:** Adresa IP klienta je v seznamu adres IP ignorována (to znamená, že klient může být zproštěn ověřování).
- **SHODA:** Klient úspěšně absolvoval ověřování (to znamená, že klient je ve shodě se zásadami).
- **SELHÁNÍ:** Ověření klienta se nezdařilo (to znamená, že klient není ve shodě se zásadami a je třeba provést administrativní akci).

Chcete-li určit příčinu selhání, spusťte příkaz **psconf** s adresou IP klienta, pro kterého došlo k selhání:

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

Související odkazy:

“Příkaz psconf” na stránce 38

Aktualizace klienta Trusted Network Connect

Server TNC (Trusted Network Connect) ověří klienta a aktualizuje databázi s informacemi o stavu klienta a výsledku ověřování. Administrátor může zobrazit výsledky a provést akci aktualizace klienta.

Chcete-li aktualizovat klienta na předchozí úrovni, zadejte následující příkaz:

```
psconf update -i <ip> -r <informace_o_sestavení> [-a oprava_apar1,oprava_apar2...]
```

Příklad:

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

Příkaz **psconf** aktualizuje klienta s použitím instalací sestavení a oprav APAR, nejsou-li nainstalovány.

Související odkazy:

“Příkaz psconf” na stránce 38

Správa zásad pro správu oprav

Příkaz **pmconf** slouží ke konfigurování zásad pro správu oprav.

Zásady pro správu oprav poskytují informace, jako je adresa IP serveru TNC a časový interval pro zahájení aktualizace modulu SUMA.

Chcete-li spravovat zásady pro správu oprav, zadejte následující příkaz:

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

Příklad:

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

Poznámka: Porty parametrů pmport a tncserver se musí lišit.

Související odkazy:

"Příkaz pmconf" na stránce 34

Importování certifikátů funkce Trusted Network Connect

Seznamte se s postupem importování certifikátu a zabezpečeného přenosu dat v síti.

Démoni funkce TNC (Trusted Network Connect) komunikují prostřednictvím šifrovaných kanálů s povoleným zabezpečením TLS (Transport Layer Security) nebo SSL (Secure Sockets Layer). Tento démon zajišťuje, aby údaje přenášené v síti byly ověřené a zabezpečené. Každý systém má vlastní klíč a certifikát. Jejich generování je provedeno po spuštění inicializačního příkazu pro příslušné komponenty. Tento proces je pro administrátora transparentní a vyžaduje nižší míru jeho zapojení. Při prvním ověřování klienta je jeho certifikát importován do databáze serveru. Certifikát je nejprve označen jako nedůvěryhodný. Administrátor poté pomocí příkazu **psconf** zobrazí certifikáty a označí je jako důvěryhodné zadáním následujícího příkazu:

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

Chce-li administrátor použít jiný klíč a certifikát, příkaz **psconf** umožňuje importovat klíč a certifikát prostřednictvím příslušné funkce.

Chcete-li importovat certifikát ze serveru, zadejte následující příkaz:

```
psconf import  -S -k<název_souboru_s_klíči> -f<název_souboru>
```

Chcete-li importovat certifikát z klienta, zadejte následující příkaz:

```
psconf import  -C -k<název_souboru_s_klíči> -f<název_souboru>
```

Související odkazy:

"Příkaz psconf" na stránce 38

Vytváření sestav pro server TNC

Server TNC (Trusted Network Connect) podporuje u sestav běžných rizik a míst ohrožení (CVE), sestav údajů IBM Security Advisory, sestav zásad serveru TNC, sestav oprav zabezpečení klientů TNC a sestav registrovaných opravných sad a prozatímních oprav formát s hodnotami oddělenými čárkou (CSV) i formát textového výstupu.

V sestavě CVE jsou zobrazena všechna běžná rizika a místa ohrožení registrovaných opravných sad. Chcete-li zobrazit výsledky této sestavy, zadejte následující příkaz:

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

Sestava údajů IBM Security Advisory obsahuje známá místa bezpečnostních rizik v nainstalovaném softwaru IBM. Chcete-li zobrazit výsledky této sestavy, zadejte následující příkaz:

```
psconf report -A <název_položky_Advisory>
```

Sestava zásad serveru TNC obsahuje zásady zabezpečení vynucené na serveru TNC. Chcete-li zobrazit výsledky této sestavy, zadejte následující příkaz:

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

Sestava oprav klienta TNC obsahuje nainstalované a chybějící prozatímní opravy pro klienta TNC. Chcete-li zobrazit výsledky této sestavy, zadejte následující příkaz:

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

Můžete rovněž spustit sestavu, která generuje seznam registrovaných opravných sad a souvisejících oprav APAR a prozatímních oprav. Chcete-li zobrazit výsledky této sestavy, zadejte následující příkaz:

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

| **Související odkazy**:
| "Příkaz psconf" na stránce 38

Odstraňování problémů s funkcí Trusted Network Connect and Patch Management

Seznamte se s možnými příčinami selhání a kroky při odstraňování problémů s funkcí TNC a systémem správy oprav.

Chcete-li odstraňovat problémy s funkcí TNC a systémem správy oprav, ověřte nastavení konfigurace uvedená v následující tabulce.

Tabulka 3. Odstraňování problémů s nastaveními konfigurace pro funkci TNC a systémy správy oprav

Problém	Řešení
Server TNC se nespustil nebo neodpovídá.	Proveďte následující postup: 1. Určete, zda je spuštěn démon serveru TNC, zadáním následujícího příkazu: `ps –eaf | grep tnccsd` 2. Není-li spuštěn, odstraňte soubor /var/tnc/.tncsock. 3. Restartujte server. Pokud se tímto postupem problém neodstraní, ověřte, že konfigurační soubor /etc/tnccs.conf na serveru TNC obsahuje položku component = SERVER.
Server správy oprav funkce TNC se nespustil nebo neodpovídá.	• Určete, zda je spuštěn démon serveru správy oprav funkce TNC, zadáním následujícího příkazu: `ps –eaf | grep tncpmd` • Ověřte, že konfigurační soubor /etc/tnccs.conf na serveru správy oprav funkce TNC obsahuje položku component = TNCPM.
Klient TNC se nespustil nebo neodpovídá.	• Určete, zda je spuštěn démon klienta TNC, zadáním následujícího příkazu: `ps –eaf | grep tnccsd` • Ověřte, že konfigurační soubor /etc/tnccs.conf v klientu TNC obsahuje položku component = CLIENT.
V rámci serveru Virtuální server I/O (Virtuální vstupně-výstupní server) není spuštěn modul IP Referrer funkce TNC.	• Určete, zda je spuštěn démon modulu IP Referrer funkce TNC, zadáním následujícího příkazu: `ps –eaf | grep tnccsd` • Ověřte, že konfigurační soubor /etc/tnccs.conf v rámci serveru Virtuální vstupně-výstupní server obsahuje položku component = IPREF.
Systém nelze konfigurovat jako server TNC i klienta TNC.	V jednom systému nemůže být souběžně spuštěn server TNC i klient TNC.
Démoni jsou spuštěni, ověřování však neprobíhá.	Povolte zprávy protokolu pro démony. V souboru /etc/tnccs.conf nastavte pro protokol položku level=info. Můžete analyzovat zprávy protokolu.

Příkazy modulu PowerSC Standard Edition

Modul PowerSC Standard Edition poskytuje příkazy umožňující komunikaci s komponentou Trusted Firewall a Trusted Network Connect prostřednictvím příkazového řádku.

Příkaz chvfilt

Účel

Změní hodnoty pro existující pravidlo filtrace přecházení mezi virtuálními sítěmi LAN.

Syntaxe

chvfilt [**-v <4|6>**] **-n ID_filtru** [**-a <D|P>**] [**-z <zdrojová_virtuální_síť_LAN>**] [**-Z <cílová_virtuální_síť_LAN>**] [**-s <zdrojová_adresa>**] [**-d <cílová_adresa>**] [**-o <operace_zdrojového_portu>**] [**-p <zdrojový_port>**] [**-O <operace_cílového_portu>**] [**-P <cílový_port>**] [**-c <protokol>**]

Popis

Příkaz **chvfilt** slouží ke změně definice pravidla filtrace přecházení mezi virtuálními sítěmi LAN v tabulce s pravidly filtrace.

Příznaky

-a Určuje akci. Platné hodnoty jsou následující:
- D (odepření): Blokuje provoz.
- P (povolení): Povolí provoz.

-c Určuje různé protokoly, kterých se příslušné pravidlo filtrace týká. Platné hodnoty jsou následující:
- udp
- icmp
- icmpv6
- tcp
- any

-d Určuje cílovou adresu ve formátu IPv4 nebo IPv6.

-m Určuje masku zdrojové adresy.

-M Určuje masku cílové adresy.

-n Určuje ID pravidla filtrace, které bude upraveno.

-o Určuje operaci zdrojového portu nebo typu ICMP (Internet Control Message Protocol). Platné hodnoty jsou následující:
- lt
- gt
- eq
- any

-O Určuje operaci cílového portu nebo kódu ICMP. Platné hodnoty jsou následující:
- lt
- gt
- eq
- any

-p Určuje zdrojový port nebo typ ICMP.

-P Určuje cílový port nebo kód ICMP.

-s Určuje zdrojovou adresu ve formátu v4 nebo v6.

-v Určuje verzi IP tabulky s pravidly filtrace. Platné hodnoty jsou 4 a 6.

-z Určuje ID virtuální sítě LAN zdrojové logické oblasti.

-Z Určuje ID virtuální sítě LAN cílové logické oblasti.

Stav ukončení

Tento příkaz vrací následující hodnoty ukončení:

0 Úspěšné dokončení.

>0 Došlo k chybě.

Příklady

1. Chcete-li změnit platné pravidlo filtrace v jádru, zadejte příkaz následujícím způsobem:
   ```
   chvfilt -n 1 -v4 -a P -z 100 -Z 300 -o eq -p 23 -O lt -P 345 -c tcp
   ```
2. Pokud pravidlo filtrace (n=2) v jádru neexistuje, bude příkaz následující:
   ```
   chvfilt -n 2 -v4 -a P -z 100 -Z 300 -o eq -p 23 -O lt -P 345 -c tcp
   ```

   Systém zobrazí následující výstup:
   ```
   Volání ioctl(QUERY_FILTER) selhalo. Chyba: Pravidlo filtrace neexistuje (2). Pravidlo filtrace nelze změnit.
   ```

Příkaz genvfilt

Účel

Přidá pravidlo filtrace pro virtuální síť LAN, která přechází mezi logickými oblastmi na tomtéž serveru IBM Power Systems.

Syntaxe

genvfilt -v <4|6> -a <D|P> -z <zdrojová_virtuální_síť_LAN> -Z <cílová_virtuální_síť_LAN> [**-s <zdrojová_adresa>**] [**-d <cílová_adresa>**] [**-o <operace_zdrojového_portu>**] [**-p <zdrojový_port>**] [**-O <operace__cílového_portu>**] [**-P <cílový_port>**] [**-c <protokol>**]

Popis

Příkaz **genvfilt** přidá pravidlo filtrace pro virtuální síť LAN, která přechází mezi logickými oblastmi (LPAR) na tomtéž serveru IBM Power Systems.

Příznaky

-a Určuje akci. Platné hodnoty jsou následující:
- D (odepření): Blokuje provoz.
- P (povolení): Povolí provoz.

-c Určuje různé protokoly, kterých se příslušné pravidlo filtrace týká. Platné hodnoty jsou následující:
- udp
- icmp
- icmpv6
- tcp
- any

-d Určuje cílovou adresu ve formátu v4 nebo v6.

-m Určuje masku zdrojové adresy.

-M Určuje masku cílové adresy.

-o Určuje operaci zdrojového portu nebo typu ICMP (Internet Control Message Protocol). Platné hodnoty jsou následující:
- lt

- gt
- eq
- any

-O Určuje operaci cílového portu nebo kódu ICMP. Platné hodnoty jsou následující:
- lt
- gt
- eq
- any

-p Určuje zdrojový port nebo typ ICMP.

-P Určuje cílový port nebo kód ICMP.

-s Určuje zdrojovou adresu ve formátu IPv4 nebo IPv6.

-v Určuje verzi IP tabulky s pravidly filtrace. Platné hodnoty jsou 4 a 6.

-z Určuje ID virtuální sítě LAN zdrojové oblasti LPAR. ID virtuální sítě musí ležet v rozsahu 1 až 4096.

-Z Určuje ID virtuální sítě LAN cílové oblasti LPAR. ID virtuální sítě musí ležet v rozsahu 1 až 4096.

Stav ukončení

Tento příkaz vrací následující hodnoty ukončení:

0 Úspěšné dokončení.

>0 Došlo k chybě.

Příklady

1. Chcete-li přidat pravidlo filtrace, které povolí data TCP ze zdrojové virtuální sítě LAN s ID 100 do cílové virtuální sítě LAN s ID 200 na konkrétních portech, zadejte příkaz následujícím způsobem:
   ```
   genvfilt -v4 -a P -z 100 -Z 200  -o lt -p 345 -O lt -P 345 -c tcp
   ```

Související odkazy:

"Příkaz mkvfilt" na stránce 34

"Příkaz vlantfw" na stránce 44

Příkaz lsvfilt
Účel

Zobrazí seznam pravidel filtrace přecházení mezi virtuálními sítěmi LAN z tabulky filtrů.

Syntaxe

lsvfilt [**-a**]

Popis

Příkaz **lsvfilt** slouží k vypsání seznamu pravidel filtrace přecházení mezi virtuálními sítěmi LAN a jejich stavu.

Příznaky

-a Vypíše pouze aktivní pravidla filtrace.

Stav ukončení

Tento příkaz vrací následující hodnoty ukončení:

0 Úspěšné dokončení.

>0 Došlo k chybě.

Příklady

1. Chcete-li zobrazit všechna aktivní pravidla filtrace v jádru, zadejte příkaz následujícím způsobem:

```
lsvfilt -a
```

Související pojmy:

“Deaktivace pravidel” na stránce 16
V rámci funkce Trusted Firewall můžete deaktivovat pravidla umožňující směrování mezi virtuálními sítěmi LAN.

Příkaz mkvfilt
Účel

Aktivuje pravidla filtrace přecházení mezi virtuálními sítěmi LAN definovaná pomocí příkazu **genvfilt**.

Syntaxe

mkvfilt -u

Popis

Příkaz **mkvfilt** aktivuje pravidla filtrace přecházení mezi virtuálními sítěmi LAN definovaná pomocí příkazu **genvfilt**.

Příznaky

-u Aktivuje pravidla filtrace v tabulce s pravidly filtrace.

Stav ukončení

Tento příkaz vrací následující hodnoty ukončení:

0 Úspěšné dokončení.

>0 Došlo k chybě.

Příklady

1. Chcete-li aktivovat pravidla filtrace v jádru, zadejte příkaz následujícím způsobem:

```
mkvfilt -u
```

Související odkazy:

“Příkaz genvfilt” na stránce 32

Příkaz pmconf
Účel

Vytváří sestavy a provádí správu serveru TNCPM (Trusted Network Connect Patch Management) registrováním nejnovějších oprav úrovně technologie a serverů TNC a generováním sestav pro stav funkce TNCPM.

Poznámka: Server TNCPM lze spustit pouze v systému AIX verze 7.1 s úrovni technologie 7100-02, aby bylo možné stahovat metadata opravných sad.

Syntaxe

pmconf mktncpm [**pmport=**<*port*>] **tncserver=***ip* | název_hostitele **:** *port*

pmconf rmtncpm

pmconf start

pmconf stop

| **pmconf init -i** <*interval_stahování*> **-l** <*seznam_úrovní_technologie*> **-A** [**-P** <*cesta_stahování*>] [**-x** <*ifix*
| *interval*>] [**-K** <*ifix klíč*>]

pmconf add -l *seznam_úrovní_technologie*

pmconf add -p <*seznam_opravných_sad*> [**-U** <*cesta_k_opravným_sadám_definovaná_uživatelem*>]

| **pmconf add -p** <*opravná_sada*> **-e** <*soubor_ifix*>

| **pmconf add -y** <*soubor_Advisory*> **-v** <*soubor_s_podpisem*> **-e** <*soubor_TAR_opravy_ifix*>

pmconf delete -l *seznam_úrovní_technologie*

pmconf delete -p <*seznam_opravných_sad*>

| **pmconf delete -p** <*opravná_sada*>**-e** *soubor_ifix*

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

pmconf list -l *opravná_sada*

pmconf list -C

pmconf list -a *opravná_sada*

pmconf hist -u

pmconf hist -d

pmconf import -f *název_souboru_s_certifikáty* **-k** *název_souboru_s_klíči*

pmconf export -f *název_souboru*

pmconf modify -i <*interval_stahování*>

pmconf modify -P <*cesta_stahování*>

pmconf modify -g <*přijmout_všechny_licence?*>

pmconf modify -t <*seznam_typů_oprav_APAR*>

| **pmconf modify -x** <*interval_oprav_ifix*>

| **pmconf modify -K** <*klíč_opravy_ifix*>

pmconf delete -l <*seznam_úrovní_technologie*>

pmconf restart

pmconf status

pmconf log loglevel = info | error | none

pmconf chtncpm attribute = *hodnota*

Popis

Funkce příkazu **pmconf** jsou následující:

Správa úložiště oprav
Registruje úrovně technologie nebo ruší jejich registraci; ruší registraci serverů TNC. Funkce TNCPM vytvoří pro každou úroveň technologie úložiště oprav obsahující nejnovější opravy, informace příkazu **lslpp** (například informace o nainstalovaných sadách souborů či aktualizacích sad souborů) a informace o opravách zabezpečení pro příslušnou úroveň technologie.

Vytváření sestav
Generuje sestavy s informacemi o stavu funkce TNCPM.

Pomocí příkazu **pmconf** lze provádět následující operace:

Položka	Popis
add	Zaregistruje novou úroveň technologie s použitím funkce TNCPM.
chtncpm	Změní atributy v souboru tnccs.conf. Aby se změny projevily na serveru TNCPM, je potřebný explicitní příkaz **start**.
delete	Zruší registraci úrovně technologie s použitím funkce TNCPM.
history	Zobrazí historii aktualizací a stahování.
list	Zobrazí informace o funkci TNCPM.
log	Nastaví úroveň protokolování pro komponenty funkce TNC.
mktncpm	Vytvoří server TNCPM.
modify	Upraví atributy souboru tncpm.conf.
rmtncpm	Odebere server TNCPM.
start	Spustí server TNCPM.
stop	Zastaví server TNCPM.

Příznaky

Položka	Popis
-A	Při provádění aktualizací klientů přijme všechny licenční smlouvy.
-a <soubor_Advisory>	Určuje soubor Advisory odpovídající parametru **ifix**. Není-li soubor Advisory uveden, není parametr **ifix** považován za adresu prozatímní opravy pro běžná rizika a místa ohrožení.
-e <soubor_ifix>	Určuje prozatímní opravy přidané do funkce TNCPM.
-i *interval_stahování*	Určuje interval, ve kterém funkce TNCPM zjišťuje existenci nové opravné sady pro registrované úrovně technologie. Interval představuje celočíselná hodnota určující počet minut nebo hodnota v následujícím formátu: **d** (počet dnů): **h** (hodiny): **m** (minuty).
-K <klíč_opravy_ifix>	Určuje veřejný klíč nástroje PSIRT (IBM AIX Product Security Incident Response Tool), který je používán k ověřování a stažených položek Advisory a prozatímních oprav. Tento veřejný klíč lze stáhnout ze serveru s veřejnými klíči PGP s použitím ID **0x28BFAA12**.
-p *seznam_opravných_sad*	Určuje seznam opravných sad, jež mají být staženy. Seznam obsahuje hodnoty (oddělené čárkami) ve formátu VYD00-úroveň_technologie-opravná_sada (zápis 6100-01-04 například představuje opravnou sadu 04 pro úroveň technologie 01 a verzi 6.1). V případě použití příznaku -U určete pouze opravnou sadu.
-t *seznam_typů_oprav_APAR*	Určuje typy oprav APAR podporovaných funkcí TNCPM pro aktualizaci klienta a výpis serveru TNC. Opravy zabezpečení APAR jsou podporovány vždy. Parametr seznam_typů_oprav_APAR představuje seznam hodnot (oddělených čárkami) následujících typů: HIPER, FileNet Process Engine, Rozšíření.
-P *cesta_k_úložišti_oprav*	Určuje adresář stahování pro úložiště oprav, které budou stahovány funkcí TNCPM. Výchozí adresář je **/var/tnc/tncpm/fix_repository**.
-U *úložiště_oprav_definované_uživatelem*	Určuje cestu k úložišti oprav definovanému uživatelem. Určete vydání, úroveň technologie a opravnou sadu přidruženou k úložišti oprav používanému k ověřování a aktualizacím klientů.
-s	Generuje sestavu registrovaných opravných sad.

Položka	Popis
-l *opravná_sada*	Generuje sestavu informací příkazu **lslpp** pro příslušnou opravnou sadu. Parametr *opravná_sada* je uveden ve formátu VYD00-úroveň_technologie-opravná_sada (zápis 6100-01-04 například představuje opravnou sadu 04 pro úroveň technologie 01 a verzi 6.1).
-u	Generuje sestavu historie aktualizací klienta.
-d	Generuje sestavu historie stahování opravných sad.
-C	Generuje sestavu pro certifikát serveru.
-a *opravná_sada*	Generuje sestavu informací o opravě zabezpečení APAR (Authorized Program Analysis Report) pro příslušnou opravnou sadu. Parametr *opravná_sada* je uveden ve formátu VYD00-úroveň_technologie-opravná_sada (zápis 6100-01-04 například představuje opravnou sadu 04 pro úroveň technologie 01 a verzi 6.1).
-f *název_souboru*	Určuje název souboru certifikátu.
-k *název_souboru_s_klíči*	Určuje soubor, ze kterého musí být načten klíč certifikátu v případě operace importování.

-c	Zobrazuje atributy uživatelů v podobě záznamů oddělených dvojtečkami. Příklad:
	`# název: atribut_1: atribut_2: ...`
	`zásada: hodnota_1: hodnota_2: ...`

-v <*soubor_s_podpisem*>	Určuje soubor s podpisem pro údaje IBM AIX Vulnerability Advisory.
-y <*soubor_Advisory*>	Určuje soubor IBM AIX Vulnerability Advisory.
-q	Potlačí informace v záhlaví.
-x <*interval_oprav_ifix*>	Určuje interval v minutách pro zjišťování a stahování nových prozatímních oprav. Je-li nastavena hodnota 0, bude automatické stahování prozatímních oprav a oznamování zakázáno. Výchozí interval je 24 hodin.

Stav ukončení

Tento příkaz vrací následující hodnoty ukončení:

Položka	Popis
0	Příkaz byl úspěšně proveden a veškeré požadované změny byly provedeny.
>0	Došlo k chybě. Zobrazená chybová zpráva obsahuje podrobnější informace o typu selhání.

Příklady

1. Chcete-li inicializovat funkci TNCPM, zadejte následující příkaz:
   ```
   pmconf init -f 10080 -l 5300-11,6100-00
   ```
2. Chcete-li vytvořit démona TNCPM, zadejte následující příkaz:
   ```
   mktncpm pmport=55777 tncserver=11.11.11.11:77555
   ```
3. Chcete-li spustit server, zadejte následující příkaz:
   ```
   pmconf start
   ```
4. Chcete-li server zastavit, zadejte následující příkaz:
   ```
   pmconf stop
   ```
5. Chcete-li registrovat novou úroveň technologie s použitím funkce TNCPM, zadejte následující příkaz:
   ```
   pmconf add -l 6100-01
   ```
6. Chcete-li zrušit registraci úrovně technologie z funkce TNCPM, zadejte následující příkaz:
   ```
   pmconf delete -l 6100-01
   ```
7. Chcete-li zrušit registraci serveru TNC s adresou IP 11.11.11.11 z funkce TNCPM, zadejte následující příkaz:
   ```
   pmconf delete -t 11.11.11.11
   ```
8. Chcete-li registrovat novější verzi dřívější opravné sady ve funkci TNCPM, zadejte následující příkaz:
   ```
   pmconf add -s 6100-01-04
   ```
9. Chcete-li zrušit registraci dřívější opravné sady z funkce TNCPM, zadejte následující příkaz:
   ```
   pmconf delete -s 6100-01-04
   ```
10. Chcete-li vygenerovat sestavu úložišť oprav pro každou registrovanou úroveň technologie, zadejte následující příkaz:
    ```
    pmconf list -s
    ```
11. Chcete-li vygenerovat sestavu informací příkazu **lslpp** pro registrovanou úroveň technologie, zadejte následující příkaz:

```
pmconf list -l 6100-01-02
```

12. Chcete-li vygenerovat sestavu z historie aktualizací, zadejte následující příkaz:
```
pmconf hist -u
```
13. Chcete-li vygenerovat sestavu z historie stahování, zadejte následující příkaz:
```
pmconf hist -d
```
14. Chcete-li vygenerovat sestavu certifikátu serveru, zadejte následující příkaz:
```
pmconf list -C
```
15. Chcete-li vygenerovat sestavu informací o opravách zabezpečení APAR pro opravnou sadu, zadejte následující příkaz:
```
pmconf list -a 6100-01-02
```
16. Chcete-li importovat certifikát serveru, zadejte následující příkaz:
```
pmconf import -f /tmp/server.txt -k /tmp/server-cert-key.txt
```
17. Chcete-li exportovat certifikát serveru, zadejte následující příkaz:
```
pmconf export -f /tmp/server.txt
```

Příkaz psconf

Účel

Vytváří sestavy a spravuje server TNC (Trusted Network Connect), klienta TNC, modul IP Referrer (IPRef) funkce TNC a modul SUMA (Service Update Management Assistant). Spravuje zásady pro sady souborů a zásady pro správu oprav týkající se integrity koncových bodů (serverů a klientů) při připojení k síti a po připojení k síti. Cílem je chránit síť před hrozbami a útoky.

Syntaxe

Operace serveru TNC:

psconf mkserver [**tncport=**<*port*>] **pmserver=**<*hostitel***:***port*> [tsserver=<hostitel>] [**recheck_interval=**<*čas_v_minutách*> | **d** (dny) : **h** (hodiny) : **m** (minuty)] [**dbpath** = <*adresář_definovaný_uživatelem*>]

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

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

psconf chserver attribute = *hodnota*

psconf add -F <*název_zásad_sady_souborů*> -r <*informace_o_sestavení*> [**apargrp=** [**±**]<*skupina_APAR_1, skupina_APAR_2.. >*] [*ifixgrp*=[+|-]<*skupina_ifix_1*,*skupina_ifix_2...*>]

psconf add { **-G** <*název_skupiny_adres_IP*> **ip=**[**±**]<*hostitel_1, hostitel_2...*> | {**-A**<*skupina_APAR*> [**aparlist**=[**±**]*APAR_1, APAR_2...* | {**-V** <*skupina_ifix*> [*ifixlist*=[+|-]*ifix_1*,*ifix_2...*]}

psconf add -P <*název_zásad*> { **fspolicy=**[**±**]<*f1,f2...*> | **ipgroup=**[**±**]<*skupina_1,skupina_2...*> }

psconf add -e *ID_e-mailu* [-E FAIL | COMPLIANT | ALL] [**ipgroup=** [**±**]<*skupina_1,skupina_2...*>]

psconf add -I ip= [**±**]<*hostitel_1, hostitel_2...*>

psconf delete { **-F** <*název_zásad_sady_souborů*> | **-G** <*název_skupiny_adres_IP*> | **-P** <*policyname*> | **-A** <*skupina_APAR*> | **-V** <*skupina_ifix*>}

psconf delete -H -i <*hostitel* | **ALL**> **-D** <*rrrr-mm-dd*>

| **psconf certadd -i** <*hostitel*> **-t** <**TRUSTED | UNTRUSTED**>

| **psconf certdel -i** <*hostitel*>

| **psconf verify -i** <*hostitel*> **| -G** <*skupina_adres_IP*>

| **psconf update [-p] {-i**< *hostitel* >**| -G** <*skupina_adres_IP*> [**-r** <*informace_o_sestavení*> **| -a** <*APAR_1, APAR_2...*> **|**
| [**-u**] **-v** <*ifix_1*, *ifix_2*,...>}

| **psconf log loglevel=<info | error | none**>

| **psconf import -C -i** <*hostitel*> **-f** <*název_souboru*> **| –d** <*název_databáze_importu*>

| **psconf** { **import -k** <*název_souboru_s_klíči*> **| export**} **-S -f** <*název_souboru*>

| **psconf list** { **-S | -G** < *název_skupiny_adres_IP* **| ALL** > **| -F** < *název_zásad_sady_souborů* **| ALL** > **| -P** < *název_zásad*
| **| ALL** > **| -r** < *informace_o_sestavení* **| ALL** > **| -I -i** < *ip* **| ALL** > **| -A** < *skupina_APAR* **| ALL** > **| -V** <*skupina_ifix*>}
| [**-c**] [**-q**]

| **psconf list** { **-H | -s <COMPLIANT | IGNORE | FAILED | ALL**> } **-i** <*hostitel* **| ALL**> [**-c**] [**-q**]

| **psconf export -d** <*cesta_k_adresáři_exportu*>

| **psconf report -v <ID_CVE|ALL> -o <TEXT|CSV>**

| **psconf report -A <název_položky_Advisory>**

| **psconf report -P <název_zásad|ALL> -o <TEXT|CSV>**

| **psconf report -i <adresa_IP|ALL> -o <TEXT|CSV>**

| **psconf report -B <informace_o_sestavení|ALL> -o <TEXT|CSV>**

| Operace klienta TNC:

| **psconf mkclient** [**tncport=**<*port*>] **tncserver=**<*hostitel:port*>

| **psconf mkclient tncport=**<*port*> -T

| **psconf** { **rmclient | status** }

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

| **psconf chclient** attribute = *hodnota*

| **psconf list** { **-C | -S** }

| **psconf export** { **-C | -S** } **-f** <*název_souboru*>

| **psconf import** { **-S | -C -k** <*název_souboru_s_klíči*> } **-f** <*název_souboru*>

| Operace modulu IPRef funkce TNC:

| **psconf mkipref** [**tncport=**<*port*>] **tncserver=**<hostitel:port>

| **psconf** { **rmipref | status**}

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

psconf chipref attribute = *hodnota*

psconf { **import -k** <*název_souboru_s_klíči*> **| export** } **-R -f** <*název_souboru*>

psconf list -R

Popis

Technologie TNC představuje architekturu založenou na otevřených standardech. Je určena pro ověřování koncových bodů, měření integrity platforem a integraci systémů zabezpečení. Architektura TNC přezkoumává koncové body (klienty a servery v síti) a zjišťuje jejich shodu se zásadami zabezpečení, než je v chráněné síti povolí. Modul IPRef architektury TNC informuje server TNC o každé nové adrese IP zjištěné v rámci serveru VIOS.

Modul SUMA umožňuje administrátorům systému věnovat méně pozornosti úloze ručního načítání aktualizací údržby z webu. Nabízí flexibilní možnosti, díky kterým může administrátor systému vytvořit automatizované rozhraní pro stahování oprav z webu pro distribuci oprav do příslušných systémů.

Příkaz **psconf** spravuje síťový server a klienty z hlediska přidávání nebo odstraňování zásad zabezpečení, ověřování klientů jako důvěryhodných či nedůvěryhodných, generování sestav a aktualizace serveru a klienta.

Pomocí příkazu **psconf** lze provádět následující operace:

Položka	Popis
add	Přidá informace o zásadě, klientu nebo e-mailu na server TNC.
apargrp	Určuje názvy skupin opravy APAR jako součást zásad pro sady souborů, které jsou použity pro ověřování klientů TNC.
aparlist	Určuje seznam oprav APAR, které jsou součástí skupiny oprav APAR.
certadd	Označí certifikát jako důvěryhodný nebo nedůvěryhodný.
certdel	Odstraní informace o klientu.
chclient	Změní atributy v souboru tnccs.conf. Aby se změny projevily v klientu TNC, je potřebný explicitní příkaz **start**. Syntaxe zápisu attribute=hodnota je stejná jako u příkazu **mkclient**.
chipref	Změní atributy v souboru tnccs.conf. Aby se změny projevily v modulu IPRef, je potřebný explicitní příkaz **start**. Syntaxe zápisu attribute=hodnota je stejná jako u příkazu **mkipref**.
chserver	Změní atributy v souboru tnccs.conf. Aby se změny projevily na serveru TNC, je potřebný explicitní příkaz **start**. Syntaxe zápisu attribute=hodnota je stejná jako u příkazu **mkserver**. **Poznámka:** Atribut **dbpath** nelze změnit pomocí příkazu **chserver**. Změnit jej lze pouze spuštěním příkazu **mkserver**.
dbpath	Určuje umístění databáze funkce TNC. Výchozí hodnota je /var/tnc.
delete	Odstraní zásady nebo informace o klientu.
export	Exportuje certifikát klienta nebo serveru či databázi na serveru TNC.
fspolicy	Určuje zásady pro sady souborů příslušného vydání, úroveň technologie a opravnou sadu použitou pro ověřování klientů TNC.
import	Importuje certifikát v klientu nebo na serveru či databázi na serveru TNC.
ipgroup	Určuje skupinu adres IP (Internet Protocol), která obsahuje několik adres IP nebo názvů hostitele klientů.
list	Zobrazuje informace o serveru TNC, klientu TNC nebo modulu SUMA.
log	Nastaví úroveň protokolování pro komponenty funkce TNC.
mkclient	Konfiguruje klienta TNC.
mkipref	Konfiguruje modul IPRef funkce TNC.
mkserver	Konfiguruje server TNC.
pmport	Určuje číslo portu, na kterém příkaz **pmserver** přijímá data. Výchozí hodnota je 38240.
pmserver	Určuje název hostitele nebo adresu IP příkazu **suma**, který stahuje nejnovější opravné sady a opravy zabezpečení, jež jsou k dispozici na webu IBM® ECC a na webu IBM Fix Central.
recheck_interval	Určuje interval serveru TNC v minutách nebo ve formátu d (dny : h (hodiny) : m (minuty) pro ověřování klientů TNC. **Poznámka:** Hodnota **recheck_interval=0** znamená, že plánovač nebude zahajovat ověřování klientů v pravidelných intervalech a že registrovaní klienti budou automaticky ověřování během spouštění. V takových případech lze klienta ověřit ručně.
report	Vygeneruje sestavu s příponou souboru TXT nebo CSV.

Položka	Popis
restart	Restartuje klienta TNC, server TNC nebo modul IPRef funkce TNC.
rmclient	Zruší konfiguraci klienta TNC.
rmipref	Zruší konfiguraci modulu IPRef funkce TNC.
rmserver	Zruší konfiguraci serveru TNC.
start	Spustí klienta TNC, server TNC nebo modul IPRef funkce TNC.
status	Zobrazí stav konfigurace funkce TNC.
stop	Zastaví klienta TNC, server TNC nebo modul IPRef funkce TNC.
tncport	Určuje číslo portu, na kterém server TNC přijímá data. Výchozí hodnota je 42830.
tncserver	Určuje server TNC, který ověřuje nebo aktualizuje klienty TNC.
tssserver	Určuje adresu IP nebo název hostitele serveru Trusted Surveyor.
update	Nainstaluje opravy v klientu.
verify	Zahájí ruční ověřování klienta.

Příznaky

Položka	Popis
-A <název_položky_Advisory>	Určuje název položky Advisory pro sestavu.
-B <informace_o_sestavení>	Určuje informace o sestavení pro přípravu sestavy oprav.

-c	Zobrazuje atributy uživatelů v podobě záznamů s dvojtečkami jako oddělovači následujícím způsobem:
	`# název: atribut_1: atribut_2: ...`
	`zásada: hodnota_1: hodnota_2: ...`

-C	Určuje, že je operace určena pro komponentu klienta.
-d *umístění_databázového_souboru/cesta_k_adresáři_databáze*	Určuje umístění souboru pro importování databáze či umístění adresáře pro exportování databáze.
-D *rrrr-mm-dd*	Určuje datum pro konkrétní položku klienta v historii protokolu, přičemž parametr *rrrr* představuje rok, parametr *mm* měsíc a parametr *dd* den.
-e *ID_e-mailu* **ipgroup=[±]***skupina_1, skupina_2...*	Určuje ID e-mailu následované seznamem názvů skupin adres IP s čárkami jako oddělovači.
-E | FAIL | COMPLIANT | ALL |	Určuje událost, pro kterou je třeba odeslat e-maily na konfigurované ID e-mailu. FAIL - e-maily jsou odeslány, pokud je stav ověřování klienta SELHÁNÍ. COMPLIANT - e-maily jsou odeslány, pokud je stav ověřování klienta SHODA. ALL - e-maily jsou odeslány pro všechny stavy ověřování klienta.
-f *název_souboru*	Určuje soubor, ze kterého musí být načten certifikát v případě operace importování, nebo umístění, do kterého musí být zapsán certifikát v případě operace exportování.
-F *zásady_sady_souborů informace_o_sestavení*	Určuje název zásad systému souborů následovaný informacemi o sestavení. Informace o sestavení lze uvést v následujícím formátu: 6100-04-01, kde řetězec 6100 představuje verzi 6.1, řetězec 04 označuje úroveň údržby a řetězec 01 označuje opravnou sadu.
-G *název_skupiny_adres_IP* **ip=[±]***adresa_IP_1, adresa_IP_2...*	Určuje název skupiny adres IP následovaný seznamem adres IP s čárkami jako oddělovači.
-H	Uvádí protokol historie.
-i *hostitel*	Určuje adresu IP nebo název hostitele.
-I ip=[±]*adresa_IP_1,adresa_IP_2...* | [±] hostitel_1,hostitel_2...	Určuje adresu IP nebo název hostitele, který musí být během ověření ignorován.
-k *název_souboru*	Určuje soubor, ze kterého musí být načten klíč certifikátu v případě operace importování.
-p	Zobrazuje náhled aktualizace klienta TNC.
-P <název_zásad>	Určuje název zásad pro přípravu sestavy zásad klienta.
-q	Potlačí informace v záhlaví.
-r *informace_o_sestavení*	Vygeneruje sestavu na základě informací o sestavení. Informace o sestavení lze uvést v následujícím formátu: 6100-04-01, kde řetězec 6100 představuje verzi 6.1, řetězec 04 označuje úroveň údržby a řetězec 01 označuje opravnou sadu.

Položka	Popis
-R	Určuje, že je operace určena pro komponentu IPRef.
-s COMPLIANT | IGNORE | FAILED | ALL	Zobrazí klienta podle stavu následujícím způsobem: **COMPLIANT** Zobrazí aktivní klienty. **IGNORE** Zobrazí klienty vyloučené z jakéhokoli ověřování. **FAILED** Zobrazí klienty, u kterých se ověřování s použitím konfigurovaných zásad nezdařilo. **ALL** Zobrazí všechny klienty bez ohledu na jejich stav.
-S <hostitel>	Určuje název hostitele pro přípravu sestavy oprav zabezpečení klienta.
-t TRUSTED | UNTRUSTED	Označí určeného klienta jako důvěryhodného nebo nedůvěryhodného. **Poznámka:** Ověřit server či klienta a označit, zde je důvěryhodný nebo nedůvěryhodný, mohou pouze administrátoři systému.
-T	Určuje, že klient může přijmout požadavek ze kteréhokoli serveru TS s platným certifikátem.
-u	Odinstaluje prozatímní opravu, jež je nainstalována v klientu TNC.
-v	Určuje seznam prozatímních oprav s čárkami jako oddělovači.
-V	Určuje název skupiny prozatímních oprav.

Stav ukončení

Tento příkaz vrací následující hodnoty ukončení:

Položka	Popis
0	Příkaz byl úspěšně proveden a veškeré požadované změny byly provedeny.
>0	Došlo k chybě. Zobrazená chybová zpráva obsahuje podrobnější informace o typu selhání.

Příklady

1. Chcete-li spustit server TNC, zadejte následující příkaz:
   ```
   psconf start server
   ```
2. Chcete-li přidat zásady systému souborů s názvem 71D_latest pro sestavení 7100-04-02, zadejte následující příkaz:
   ```
   psconf add -F 71D_latest 7100-04-02
   ```
3. Chcete-li odstranit zásady systému souborů s názvem 71D_old, zadejte následující příkaz:
   ```
   psconf delete -F 71D_old
   ```
4. Chcete-li ověřit, zda je klient s adresou IP 11.11.11.11 **důvěryhodný**, zadejte následující příkaz:
   ```
   psconf certadd -i 11.11.11.11 -t TRUSTED
   ```
5. Chcete-li klienta s adresou IP 11.11.11.11 odstranit ze serveru, zadejte následující příkaz:
   ```
   psconf certdel -i 11.11.11.11
   ```
6. Chcete-li ověřit informace o klientu s adresou IP 11.11.11.11, zadejte následující příkaz:
   ```
   psconf verify -i 11.11.11.11
   ```
7. Chcete-li zobrazit informace o klientu s adresou IP 11.11.11.11, zadejte následující příkaz:
   ```
   psconf list -i 11.11.11.11
   ```
8. Chcete-li vygenerovat sestavu pro klienty se stavem **SHODA**, zadejte následující příkaz:
   ```
   psconf list -s CPMPLIANT -i ALL
   ```
9. Chcete-li vygenerovat sestavu pro sestavení 7100-04-02, zadejte následující příkaz:
   ```
   psconf list -r 7100-04-02
   ```
10. Chcete-li zobrazit historii připojení klienta s adresou IP 11.11.11.11, zadejte následující příkaz:
    ```
    psconf list -H -i 11.11.11.11
    ```
11. Chcete-li z historie protokolu odstranit položku klienta s adresou IP 11.11.11.11 z 1. února nebo starší, zadejte následující příkaz:

```
psconf delete -H -i 11.11.11.11 -D 2009-02-01
```

12. Chcete-li importovat certifikát klienta s adresou IP 11.11.11.11 ze serveru, zadejte následující příkaz:
    ```
    psconf import -C -i 11.11.11.11 -f /tmp/client.txt
    ```
13. Chcete-li exportovat certifikát serveru z klienta, zadejte následující příkaz:
    ```
    psconf export -S -f /tmp/server.txt
    ```
14. Chcete-li klienta s adresou IP 11.11.11.11 aktualizovat ze serveru na odpovídající úroveň, zadejte následující příkaz:
    ```
    psconf update -i 11.11.11.11
    ```
15. Chcete-li zobrazit informace o stavu klientů, zadejte následující příkaz:
    ```
    psconf status
    ```
16. Chcete-li zobrazit certifikát klienta, zadejte následující příkaz:
    ```
    psconf list -C
    ```
17. Chcete-li spustit klienta, zadejte následující příkaz:
    ```
    psconf start client
    ```

Zabezpečení

Upozornění pro uživatele prostředí RBAC a Trusted AIX:

Tento příkaz může provádět privilegované operace. Privilegované operace mohou provádět pouze privilegovaní uživatelé. Další informace o autorizaci a oprávněních naleznete v databázi privilegovaných příkazů v části Zabezpečení. Seznam oprávnění přidružených k tomuto příkazu naleznete v popisu příkazu **lssecattr** nebo v popisu dílčího příkazu **getcmdattr**.

Příkaz rmvfilt

Účel

Odebere seznam pravidel filtrace přecházení mezi virtuálními sítěmi LAN z tabulky filtrů.

Syntaxe

rmvfilt -n [**fid|all>**]

Popis

Příkaz **rmvfilt** slouží k odebrání pravidel filtrace přecházení mezi virtuálními sítěmi LAN z tabulky filtrů.

Příznaky

-n Určuje ID pravidla filtrace, které bude odebráno. Volba **all** slouží k odebrání všech pravidel filtrace.

Stav ukončení

Tento příkaz vrací následující hodnoty ukončení:

0 Úspěšné dokončení.

>0 Došlo k chybě.

Příklady

1. Chcete-li odebrat všechna pravidla filtrace nebo deaktivovat všechna pravidla filtrace v jádru, zadejte příkaz následujícím způsobem:
   ```
   rmvfilt -n all
   ```

Související pojmy:

“Deaktivace pravidel” na stránce 16
V rámci funkce Trusted Firewall můžete deaktivovat pravidla umožňující směrování mezi virtuálními sítěmi LAN.

Příkaz vlantfw

Účel

Zobrazuje nebo maže informace týkající se mapování adres IP a položek MAC (Media Access Control) a řídí funkci protokolování.

Syntaxe

vlantfw -h | -s | -t | -d | -f | -G | -q | -D | -E | -F | -i | -l | -L | -m | -M | -N *celé_číslo*

Popis

Příkaz **vlantfw** zobrazuje nebo maže položky mapování adres IP a položek MAC. Umožňuje také spustit nebo zastavit protokolovací zařízení funkce Trusted Firewall.

Příznaky

-d Zobrazí veškeré informace týkající se mapování adres IP.

-D Zobrazí shromážděné údaje o připojení.

-E Zobrazí údaje připojení mezi logickými oblastmi (LPAR) v různých komplexech CPC (Central Processor Complex).

-f Odebere veškeré informace týkající se mapování adres IP.

-F Vymaže mezipaměť údajů o připojení.

-G Zobrazí pravidla filtrace, která lze konfigurovat, aby byl provoz směrován interně s použitím funkce Trusted Firewall.

-I Zobrazí údaje připojení mezi oblastmi LPAR, které jsou přidruženy k různým identifikátorům virtuální sítě LAN, ale sdílejí stejné komplexy CPC (Central Processor Complex).

-l Spustí protokolovací zařízení funkce Trusted Firewall.

-L Zastaví protokolovací zařízení funkce Trusted Firewall a přesměruje obsah trasovacího souboru do souboru /home/padmin/svm/svm.log.

-m Povolí monitorování funkce Trusted Firewall.

-M Zakáže monitorování funkce Trusted Firewall.

-q Zadá dotaz na stav modulu SVM (Secure Virtual Machine).

-s Spustí funkci Trusted Firewall.

-t Zastaví funkci Trusted Firewall.

Parametry

-N *celé_číslo*
Zobrazí pravidlo filtrace odpovídající zadané celočíselné hodnotě.

Stav ukončení

Tento příkaz vrací následující hodnoty ukončení:

0 Úspěšné dokončení.

>0 Došlo k chybě.

Příklady

1. Chcete-li zobrazit veškerá mapování adres IP, zadejte příkaz následujícím způsobem:
   ```
   vlantfw -d
   ```
2. Chcete-li odebrat veškerá mapování adres IP, zadejte příkaz následujícím způsobem:
   ```
   vlantfw -f
   ```
3. Chcete-li spustit funkci protokolování modulu Trusted Firewall, zadejte příkaz následujícím způsobem:
   ```
   vlantfw -l
   ```
4. Chcete-li zkontrolovat stav modulu SVM (Secure Virtual Machine), zadejte příkaz následujícím způsobem:
   ```
   vlantfw -q
   ```
5. Chcete-li spustit funkci Trusted Firewall, zadejte příkaz následujícím způsobem:
   ```
   vlantfw -s
   ```
6. Chcete-li funkci Trusted Firewall zastavit, zadejte příkaz následujícím způsobem:
   ```
   vlantfw -t
   ```
7. Chcete-li zobrazit odpovídající pravidla, která lze použít ke generování filtrů směrujících provoz v rámci komplexu CPC (Central Processor Complex), zadejte příkaz následujícím způsobem:
   ```
   vlantfw -G
   ```

Související odkazy:

"Příkaz genvfilt" na stránce 32

Poznámky

Tyto informace jsou určeny pro produkty a služby nabízené v USA.

Společnost IBM nemusí nabízet produkty, služby nebo vlastnosti zmiňované v tomto dokumentu v jiných zemích. Informace o produktech a službách, které jsou aktuálně ve vaší zemi dostupné, můžete získat od zástupce společnosti IBM pro vaši oblast. Jakákoliv zmínka o produktu, programu nebo službě společnosti IBM neznamená, že lze použít pouze zmíněný produkt, program nebo službu společnosti IBM. Místo nich lze použít jakýkoliv funkčně ekvivalentní produkt, program nebo službu, které neobsahují žádné duševní vlastnictví společnosti IBM. Za operace prováděné produkty, programovým vybavením nebo službami, které nepochází od společnosti IBM, nese zodpovědnost uživatel.

Společnost IBM může mít patenty nebo patentové přihlášky pro aplikace popisované v tomto dokumentu. Získání tohoto dokumentu nezakládá právo licence k těmto patentům. Dotazy na licence můžete poslat dopisem na adresu:

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

S dotazy na licence vztahující se ke dvoubajtovým znakovým sadám (DBCS) se obracejte na oddělení IBM Intellectual Property Department ve vaší zemi nebo napište na adresu:

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

Následující odstavec se netýká Velké Británie nebo kterékoliv jiné země, kde taková opatření odporují místním zákonům:: FIRMA INTERNATIONAL BUSINESS MACHINES CORPORATION TUTO PUBLIKACI POSKYTUJE TAKOVOU, "JAKÁ JE", BEZ JAKÝCHKOLIV ZÁRUK, VYJÁDŘENÝCH NEBO ZAHRNUTÝCH, VČETNĚ, ALE NE VÝHRADNĚ, ODVOZENÝCH ZÁRUK PORUŠENÍ ZÁKONŮ, PRODEJNOSTI NEBO VHODNOSTI PRO URČITÝ ÚČEL. Některé státy nepovolují neposkytování vyjádřených nebo zahrnutých záruk v jistých transakcích, v tomto případě se na vás uvedený výrok nevztahuje.

Tyto informace mohou obsahovat technické nepřesnosti nebo typografické chyby. Údaje zde uvedené podléhají změnám, tyto změny budou uvedeny v nových vydáních této publikace. Společnost IBM má právo kdykoliv bez upozornění zdokonalovat nebo měnit produkty a programy popsané v této publikaci.

Jakékoliv odkazy v této publikaci na webové stránky nepatřící společnosti IBM jsou poskytovány pouze pro pohodlí zákazníků a v žádném případě nemají podporovat tyto stránky. Materiály na těchto webových stránkách nejsou součástí materiálů pro tento produkt společnosti IBM a odpovědnost za používání těchto stránek nese uživatel.

Jestliže zašlete společnosti IBM informace, udělujete tím společnosti IBM nevýluční právo používat či šířit tyto informace jakýmkoliv způsobem, který považuje za odpovídající, aniž by tím společnosti IBM vznikly jakékoliv závazky vůči vám.

Ten, kdo si přeje získat informace o licencích na tento program za účelem umožnit: (i) výměnu informací mezi nezávisle vytvořenými programy a ostatními programy (včetně tohoto) a (ii) společné použití vyměněných informací, se má obrátit na:

IBM Corporation

Dept. LRAS/Bldg. 903
11501 Burnet Road
Austin, TX 78758-3400
U.S.A.

Tyto informace mohou být dostupné za určitých podmínek, v některých případech je to zaplacení poplatku.

Licencovaný program popsaný v tomto dokumentu a veškerý licencovaný materiál dostupný pro tento program je poskytován společností IBM podle podmínek smluv IBM Customer Agreement, IBM International Program License Agreement nebo jiné ekvivalentní smlouvy.

Jakákoliv zde uvedená data o výkonnosti byla získána v řízeném prostředí. Výsledky získané v jiném operačním prostředí se mohou podstatně lišit. Některá měření byla provedena na vývojových systémech a není žádná záruka, že měření na dodávaných systémech dají stejný výsledek. Navíc byly některé údaje odhadnuty pomocí extrapolace. Skutečné výsledky se mohou lišit. Uživatelé tohoto dokumentu by měli ověřit příslušná data ve svém konkrétním prostředí.

Informace týkající se produktů jiných společností byly získány od dodavatelů těchto produktů, z jejich tištěných materiálů nebo z jiných veřejně dostupných zdrojů. Společnost IBM netestovala tyto produkty a nemůže potvrdit spolehlivost jejich provozu, kompatibilitu nebo jiné tvrzení týkající se těchto produktů. Otázky týkající se možností produktů jiných společností by měly být adresovány dodavatelům těchto produktů.

Všechny výroky týkající se budoucího směru činnosti nebo záměrů společnosti IBM mohou být změněny či odvolány bez upozornění. Jedná se pouze o cíle a úmysly.

Všechny uvedené ceny společnosti IBM jsou doporučenými cenami pro koncový prodej, jsou aktuální a mohou být změněny bez upozornění. Ceny u prodejců se mohou lišit.

Tyto informace jsou určeny pouze pro plánování. Informace uvedené zde mohou být změněny, než budou popsané produkty k dispozici.

Tyto informace obsahují příklady dat a zpráv používaných v každodenní práci. Pro ilustraci jsou poskytovány co nejúplnější, včetně jmen osob, společností, značek a produktů. Všechny názvy jsou smyšleny a jakákoliv podobnost se skutečnými názvy či adresami obchodních subjektů je zcela náhodná.

LICENCE PRO COPYRIGHT:

Tato dokumentace obsahuje vzorové aplikační programy ve zdrojovém jazyku, které ilustrují programovací techniky na různých platformách. Tyto zdrojové programy můžete bez poplatku společnosti IBM kopírovat, modifikovat a šířit za účelem vývoje, používání, prodeje či distribuce aplikačních programů, které odpovídají aplikačnímu rozhraní (API) pro operační platformy, pro které byly vzorové programy napsány. Tyto vzorové programy nebyly řádně testovány za všech podmínek. Společnost IBM tedy nemůže zaručit bezchybnost, udržovatelnost nebo funkčnost těchto programů. Vzorové programy jsou poskytovány "TAK, JAK JSOU", bez jakékoli záruky. Společnost IBM není odpovědná za žádné škody způsobené vaším používáním vzorových programů.

Každá kopie nebo libovolná část těchto ukázkových programů nebo jejich odvozenin musí být opatřena následující copyrightovou doložkou:

© (jméno společnosti) (rok). Části tohoto kódu jsou odvozeny od vzorových programů společnosti IBM Corp. © Copyright IBM Corp. _vložte rok nebo roky_.

V případě zobrazení těchto informací na obrazovce se nemusí zobrazit fotografie a barevné ilustrace.

Aspekty zásad ochrany osobních údajů

Softwarové produkty společnosti IBM včetně řešení SaaS (souhrnně „softwarové produkty“) mohou pomocí souborů cookie nebo jiných technologií shromažďovat informace o využití produktů, které slouží ke zlepšování prostředí pro koncové uživatele, přizpůsobení interakcí s koncovým uživatelem nebo k jiným účelům. V mnoha případech softwarové produkty neshromažďují žádné údaje, které by umožňovaly osobní identifikaci. Některé z našich softwarových produktů vám dovolují přispívat ke shromažďování údajů umožňujících osobní identifikaci. Pokud tento softwarový produkt pomocí souborů cookie shromažďuje údaje umožňující osobní identifikaci, platí pro něj níže uvedené specifické informace o využití souborů cookie.

Tento softwarový produkt neshromažďuje údaje umožňující osobní identifikaci pomocí souborů cookie ani jiných technologií.

Pokud vám jako zákazníkovi umožňují implementované konfigurace tohoto softwarového produktu shromažďovat pomocí souborů cookie a jiných technologií údaje umožňující osobní identifikaci koncových uživatelů, doporučujeme vám poradit se s právníkem o případných zákonech, kterým může shromažďování takových údajů podléhat, včetně předpisů vyžadujících povinná oznámení a žádosti o vyjádření souhlasu.

Další informace o použití různých technologií, včetně souborů cookie, k výše popsaným účelům naleznete v zásadách ochrany osobních údajů společnosti IBM na adrese http://www.ibm.com/privacy, v online prohlášení společnosti IBM o ochraně soukromí na adrese http://www.ibm.com/privacy/details v části „Cookies, Web Beacons and Other Technologies“ (Soubory cookie, webové signály a další technologie) a v prohlášení o ochraně soukromí pro softwarové produkty a řešení SaaS společnosti IBM na adrese http://www.ibm.com/software/info/product-privacy.

Ochranné známky

IBM, logo IBM a ibm.com jsou ochranné známky nebo registrované ochranné známky společnosti International Business Machines Corp registrované v mnoha jurisdikcích na celém světě. Ostatní produkty a názvy služeb mohou být ochrannými známkami společnosti IBM a případně dalších jiných společností. Aktuální seznam ochranných známek společnosti IBM je k dispozici na webové stránce Copyright and trademark information (Informace o autorském právu a ochranných známek) na adrese www.ibm.com/legal/copytrade.shtml.

Linux je registrovaná ochranná známka Linuse Torvaldse v USA a jiných zemích.

Java a ostatní ochranné známky a loga založená na technologii Java jsou registrované ochranné známky společnosti Oracle a jejích poboček.

Rejstřík

V

Z

Vytištěno v Dánsku společností IBM Danmark A/S.