IBM PowerSC

Standard Edition

1.1.3 változat

PowerSC Standard Edition

IBM PowerSC

Standard Edition

1.1.3 változat

PowerSC Standard Edition

Megjegyzés

A kiadvány és termék használata előtt olvassa el a “Nyilatkozatok” oldalszám: 47 rész információit.

Ez a kiadás az IBM PowerSC 1.1.3 változatára és az összes azt követő kiadásra és módosításra vonatkozik, amíg azt a következő kiadások máshogy nem jelzik.

Tartalom

A kiadványról

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

Kiemelés

A dokumentum az alábbi kiemelési megállapodásokat használja:

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

Kis- és nagybetűk megkülönböztetése az AIX rendszeren

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

ISO 9000

A termék fejlesztése és gyártása regisztrált ISO 9000 minőségbiztosítási tanúsítvánnyal rendelkező rendszereken történt.

IBM PowerSC Standard Edition 1.1.3

Az IBM® PowerSC Standard Edition a Megbízható rendszerbetöltés, a Megbízható tűzfal, a Megbízható naplózás, a Megbízható hálózati kapcsolat és javításkezelés, valamint a Biztonság és megfelelés automatizálási szolgáltatásokat tartalmazza.

PowerSC Standard Edition 1.1.3 újdonságai

Ismerje meg a PowerSC Standard Edition 1.1.3 változat témakör gyűjtemény új vagy jelentősen megváltozott információit.

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

2013 december

- Frissített rendszerkövetelmények: “PowerSC Standard Edition 1.1.3 alapelvek”.
- Kötelező Megbízható rendszerbetöltés fájlcsere azonosítása az AIX operációs rendszer újratelepítésekor: “Megbízható rendszerbetöltés - előfeltételek” oldalszám: 5.
- A Megbízható tűzfal megfigyelési funkcióval kapcsolatos információk hozzáadása: “Megbízható tűzfal megfigyelés” oldalszám: 13.
- A Megbízható tűzfal naplózási funkcióval kapcsolatos információk hozzáadása: “Megbízható tűzfal naplózás” oldalszám: 13.
- A dokumentáció a “Megbízható naplózás telepítése” oldalszám: 18 témakörrel egészült ki.
- A Megbízható hálózati kapcsolat köztes javításaival kapcsolatos információk hozzáadása: “Javításkezelő szerver konfigurálása” oldalszám: 24.
- A Megbízható hálózati kapcsolat szerver jelentéskészítéssel kapcsolatos információk hozzáadása: “TNC szerver jelentéskészítés” oldalszám: 29.
- A Megbízható hálózati kapcsolat ellenőrző telepítésével kapcsolatos információk hozzáadása: “Az ellenőrző telepítése” oldalszám: 6.
- A Megbízható tűzfal parancsok hozzáadása: “PowerSC Standard Edition parancsok” oldalszám: 30.
- A **tscpmconsole** parancs átnevezése **pmconf** parancsra, és az ezzel kapcsolatos információk hozzáadása: “pmconf parancs” oldalszám: 34.
- A **tscconsole** parancs átnevezése **psconf** parancsra, és az ezzel kapcsolatos információk hozzáadása: “psconf parancs” oldalszám: 38.
- A **vlantfw** parancs paramétereivel kapcsolatos információk frissítése: “vlantfw parancs” oldalszám: 44.

2012. november

Frissített információk a “Megbízható hálózati kapcsolat és javításkezelés” oldalszám: 20 témakörben.

2012. május

Az új szolgáltatás dokumentációjának hozzáadása: “Megbízható tűzfal” oldalszám: 10.

PowerSC Standard Edition 1.1.3 alapelvek

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

A PowerSC Standard Edition egy felhőn belül vagy virtualizált adatközpontokban működő rendszerek biztonságát és vezérlését biztosítja, valamint egy vállalati nézetet és felügyeleti képességeket nyújt. A PowerSC Standard Edition egy

Biztonság és megfelelés automatizálás, Megbízható rendszerbetöltés, Megbízható tűzfal, Megbízható naplózás valamint Megbízható hálózati kapcsolat és javításkezelés összetevőket tartalmazó szolgáltatáscsomag. A virtualizációs rétegben elhelyezett biztonsági technológia további biztonságot nyújt önálló rendszereknek.

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

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

Összetevők	Leírás	Támogatott operációs rendszer	Támogatott hardver
Biztonság és megfelelés automatizálás	A következő szabványok esetén automatizálja a biztonsági és megfelelési konfiguráció beállításait, megfigyelését és felülvizsgálatát: • Fizetőkártya ipari adatbiztonsági szabvány (PCI DSS) • Sarbanes-Oxley törvény és COBIT szabvány (SOX/COBIT) • USA Védelmi minisztérium (DoD) STIG • Az egészségbiztosítás hordozhatóságát és elszámoltathatóságát előíró törvény (HIPAA)	• AIX 5.3 • AIX 6.1 • AIX 7.1	• POWER5 • POWER6 • POWER7
Megbízható rendszerbetöltés	A rendszerbetöltési képfájlt, az operációs rendszert és az alkalmazásokat méri, és ezek megbízhatóságát a Virtuális megbízható platform modul (TPM) technológia használatával hitelesíti.	• AIX 6 (6100-07) vagy újabb • AIX 7 (7100-01) vagy újabb	POWER7 firmware eFW7.4 vagy újabb
Megbízható tűzfal	Időt és erőforrásokat takarít meg azzal, hogy lehetővé teszi a közvetlen továbbítást megadott virtuális helyi hálózatok (VLAN) között, amelyeket ugyanaz a Virtuális I/O szerver vezérel.	• AIX 6.1 • AIX 7.1 • VIOS 2.2.1.4 vagy újabb változat	• POWER6 • POWER7 • Virtuális I/O szerver 6.1S vagy újabb változat
Megbízható naplózás	Az AIX naplói központilag, valós időben a Virtuális I/O szerveren (VIOS) találhatók. Ez a szolgálatás hamisíthatatlan naplózást és a naplók kényelmes biztonsági mentését és kezelését biztosítja.	• AIX 5.3 • AIX 6.1 • AIX 7.1	• POWER5 • POWER6 • POWER7
Megbízható hálózati kapcsolat és javításkezelés	Ellenőrzi, hogy a virtuális környezetben lévő minden AIX rendszer a megadott szoftver- és javítási szinten van-e, és felügyeleti eszközöket nyújt annak biztosításához, hogy minden AIX rendszer a megadott szoftver szinten legyen. Riasztásokat biztosít, ha egy alacsonyabb szintű virtuális rendszer hozzáadásra kerül a hálózathoz, vagy ha a rendszereket érintő biztonsági javítás jelenik meg.	• AIX 5.3 • AIX 6.1 • AIX 7.1 A Megbízható hálózati kapcsolat klienshez a következő összetevők egyike szükséges: • AIX 6.1 (6100-06) vagy újabb • AIX 7.1 változatú Szolgáltatásfrissítés-kezelő segéd (SUMA) konzol rendszer a SUMA környezeten belül, a javításkezeléshez	• POWER5 • POWER6 • POWER7

PowerSC Standard Edition 1.1.3 telepítése

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

A PowerSC Standard Edition alkalmazáshoz a következő fájlkészletek érhetők el:

- powerscExp.ice: Olyan AIX rendszereken van telepítve, amelyek a PowerSC Standard Edition Biztonság és megfelelés automatizálási szolgáltatást igénylik.
- powerscStd.vtpm: Olyan AIX rendszereken van telepítve, amelyek a PowerSC Standard Edition Megbízható rendszerbetöltés szolgáltatását igénylik.
- powerscStd.vlog: Olyan AIX rendszereken van telepítve, amelyek a PowerSC Standard Edition Megbízható naplózás szolgáltatását igénylik.
- powerscStd.tnc_pm: 6100-06 technikai szintű AIX 6.1 változat vagy újabb, illetve AIX 7.1 változat Szolgáltatásfrissítés-kezelő segéd (SUMA) konzol rendszeren van telepítve, a SUMA környezeten belül, javításkezeléshez.
- powerscStd.svm: Olyan AIX rendszereken van telepítve, amelyek számára hasznos lehet a PowerSC Standard Edition útválasztási szolgáltatása.

A PowerSC Standard Edition a következő felületek használatával telepíthető:

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

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

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

Szoftverlicenc megtekintése

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

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

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

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

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

Kapcsolódó fogalmak:

“PowerSC Standard Edition 1.1.3 alapelvek” oldalszám: 1
A PowerSC Standard Edition jelen áttekintése a szolgáltatásokat, összetevőket és a PowerSC Standard Edition szolgáltatásra vonatkozó hardvertámogatást mutatja be.

“Megbízható rendszerbetöltés telepítése” oldalszám: 6
A Megbízható rendszerbetöltés telepítéséhez szükségesek bizonyos hardver- és szoftverkonfigurációk.

“Megbízható hálózati kapcsolat telepítése” oldalszám: 22
A Megbízható hálózati kapcsolat (TNC) telepítéséhe el kell végeznie bizonyos lépéseket.

Kapcsolódó feladatok:

“Megbízható tűzfal telepítése” oldalszám: 12
A PowerSC Megbízható tűzfal telepítése hasonló a többi PowerSC szolgáltatás telepítéséhez.

“Megbízható naplózás telepítése” oldalszám: 18
A PowerSC Megbízható naplózás szolgáltatását a parancssori felület vagy az SMIT eszköz használatával telepítheti.

Megbízható rendszerbetöltés

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

Megbízható rendszerbetöltés - alapelvek

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

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

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

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

Megbízható rendszerbetöltés állapota

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

Nem megbízható rendszerbetöltési állapot

Egy partíció akkor lesz megbízhatatlan állapotú, ha az ellenőrző nem tudta sikeresen hitelesíteni a rendszerbetöltési folyamat integritását. A megbízhatatlan állapot azt jelzi, hogy a rendszerbetöltési folyamat néhány aspektusa nem konzisztens az ellenőrző által fenntartott referencia információkkal. Egy sikertelen hitelesítés lehetséges okai közé

tartozik a rendszerbetöltés egy eltérő rendszerbetöltési eszközről, egy eltérő kernel képfájlból, illetve a meglévő rendszerbetöltési képfájl módosítása.

Kapcsolódó fogalmak:

“Megbízható rendszerbetöltés hibaelhárítása” oldalszám: 8
A Megbízható rendszerbetöltés használatakor van néhány általános forgatókönyv és kiigazító lépés, amelyek segítenek a hitelesítési hiba okának azonosításában.

Megbízható rendszerbetöltés tervezése

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

Megbízható rendszerbetöltés - előfeltételek

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

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

Adatgyűjtő

Egy adatgyűjtő telepítésének konfigurációs követelményei a következő előfeltételeket jelentik:

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

Ellenőrző

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

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

Felkészülés a kiigazításra

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

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

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

- Hogyan ellenőrizheti, hogy a fenyegetettség hitelt érdemlő?
- Történt bármilyen tervezett karbantartás, AIX frissítés, vagy volt telepítve nemrégiben új hardver?
- Kapcsolatba tud lépni az adminisztrátorral, akinek van hozzáférése ezekhez az információkhoz?

- Mikor volt a rendszer legutóbb betöltve megbízható állapotban?
- Ha a biztonsági fenyegetettség szabályszerűnek tűnik, akkor mit kell tennie? (A javaslatok közé tartozik a megfigyelési naplók összegyűjtése, a rendszer leválasztása a hálózatról, a rendszer kikapcsolása, illetve a felhasználók figyelmeztetése).
- Más rendszerek is veszélyeztetve voltak, amelyeket ellenőrizni kell?

Kapcsolódó fogalmak:

“Megbízható rendszerbetöltés hibaelhárítása” oldalszám: 8
A Megbízható rendszerbetöltés használatakor van néhány általános forgatókönyv és kiigazító lépés, amelyek segítenek a hitelesítési hiba okának azonosításában.

Áttérési szempontok

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

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

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

Kapcsolódó tájékoztatás:

HMC használata

VIOS átállítás

Megbízható rendszerbetöltés telepítése

A Megbízható rendszerbetöltés telepítéséhez szükségesek bizonyos hardver- és szoftverkonfigurációk.

Kapcsolódó tájékoztatás:

“PowerSC Standard Edition 1.1.3 telepítése” oldalszám: 3
A PowerSC Standard Edition minden egyes adott funkciójához telepítenie kell egy fájlkészletet.

Az adatgyűjtő telepítése

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

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

Az ellenőrző telepítése

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

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

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

Kapcsolódó tájékoztatás:

Linux OpenPTS ellenőrző letöltése az AIX Megbízható rendszerbetöltéssel való használathoz

Megbízható rendszerbetöltés konfigurálása

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

Rendszer bejegyzése

Megismerheti az eljárást, amellyel bejegyezhet egy rendszert az ellenőrzőhöz.

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

```
openpts -i <hosztnév>
```

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

Egy rendszer bejegyzéséhez a grafikus felületről, tegye a következőket:

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

Kapcsolódó fogalmak:

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

Rendszer hitelesítése

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

Egy rendszerbetöltés integritásának lekérdezéséhez használja a következő parancsot az ellenőrzőből:

```
openpts <hosztnév>
```

Egy rendszer hitelesítéséhez a grafikus felületről, tegye a következőket:

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

Rendszer bejegyzése és hitelesítése jelszó nélkül

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

Az ellenőrző tanúsítványának beállításához az adatgyűjtő rendszerén tegye a következőket:

- Az ellenőrzőn futtassa a következő parancsokat:

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

- Az adatgyűjtőn futtassa a következő parancsot:

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

Megbízható rendszerbetöltés kezelése

A Megbízható rendszerbetöltés hitelesítési eredményeinek kezeléséhez szükséges eljárás bemutatása.

Hitelesítési eredmények értelmezése

A hitelesítési eredmények megtekintéséhez és megértéséhez szükséges eljárás bemutatása.

A hitelesítés eredménye a következő állapotok egyike lehet:

1. A hitelesítési kérés meghiúsult: A hitelesítési kérés nem fejeződött be sikeresen. A hiba lehetséges okainak megértéséhez tekintse meg a Hibaelhárítás szakaszt.
2. A rendszerintegritás érvényes: A hitelesítés sikeresen befejeződött, és a rendszerbetöltés megfelel az ellenőrző által fenntartott referencia információknak. Ez egy sikeres Megbízható rendszerbetöltést jelez.
3. A rendszerintegritás érvénytelen: A hitelesítési kérés befejeződött, azonban ellentmondás található a rendszerindítás során gyűjtött információk és az ellenőrző által fenntartott referencia információk között. Ez egy nem megbízható rendszerbetöltés jelez.

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

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

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

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

Rendszerek törlése

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

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

```
openpts -r <hosztnév>
```

Megbízható rendszerbetöltés hibaelhárítása

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

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

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

2. táblázat: Néhány hiba forgatókönyv hibaelhárítása

Hiba jellege	Hiba lehetséges okai	Javasolt kiigazítás

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

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

Kapcsolódó fogalmak:

“Felkészülés a kiigazításra” oldalszám: 5
Az itt leírt Megbízható rendszerbetöltési információk iránymutatásként szolgálnak azon helyzetek azonosításához, amelyek kiigazítást igényelhetnek. Ez nincs hatással a rendszerbetöltési folyamatra.

“Megbízható rendszerbetöltés - alapelvek” oldalszám: 4
Fontos megérteni a rendszerbetöltési folyamat integritását, valamint azt, hogy a rendszerbetöltés minek alapján minősül megbízható vagy megbízhatatlan rendszerbetöltésnek.

Kapcsolódó tájékoztatás:

HMC használata

Megbízható tűzfal

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

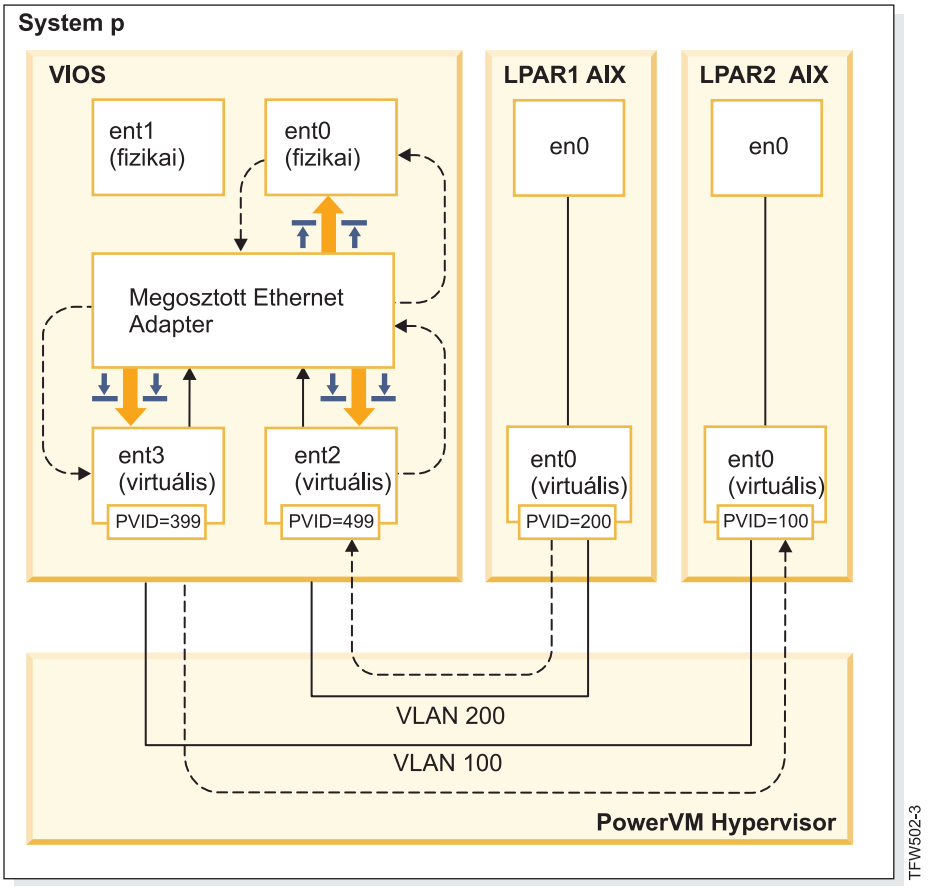
Megbízható tűzfal - alapelvek

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

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

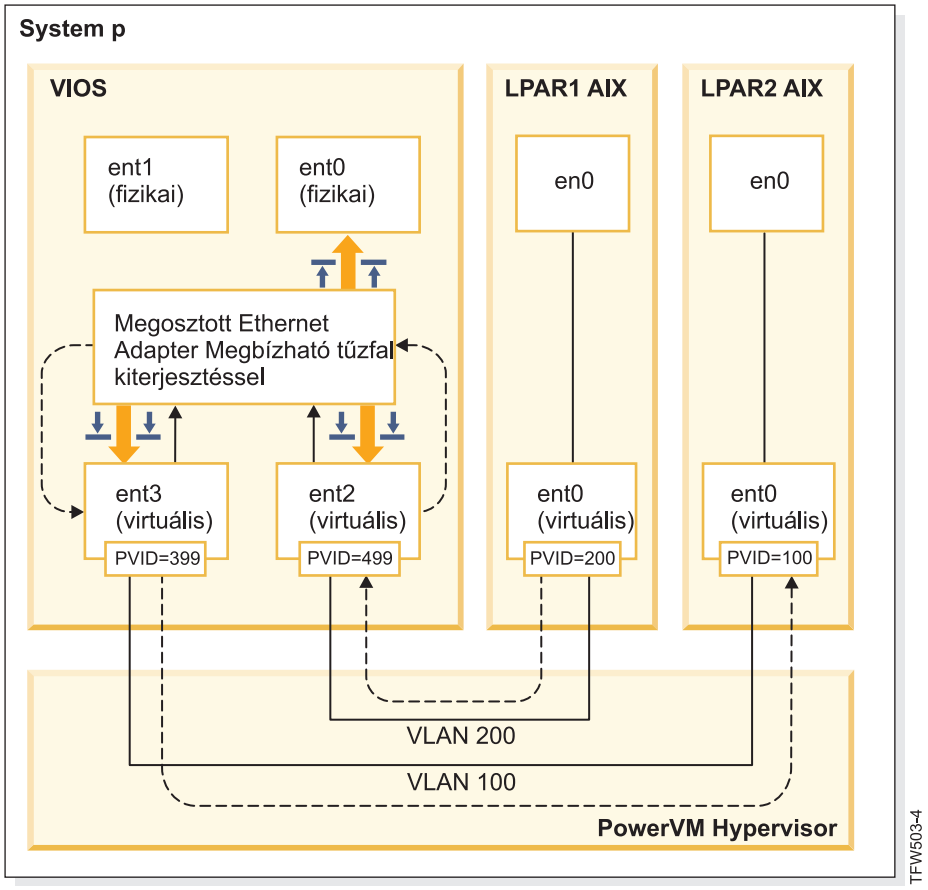
A Megbízható tűzfal lehetővé teszi szabályok konfigurálását, hogy bizonyos típusú forgalom közvetlenül átvitele engedélyezve legyen a Virtuális I/O szerveren (VIOS) lévő egyik VLAN hálózatról egy azonos VIOS szerveren lévő másik VLAN hálózatba, miközben más típusú forgalom korlátozásával továbbra is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

Az alábbi ábrán (1. ábra: oldalszám: 11) bemutatott példa használatával, a cél az, hogy az információk átvitele biztonságosan és hatékonyan történjen a VLAN 200 hálózaton lévő LPAR1 egy és a VLAN 100 hálózaton lévő LPAR2 között. A Megbízható tűzfal nélkül az LPAR1 partícióról az LPAR2 partícióra irányuló információk a belső hálózatról az útválasztónak vannak kiküldve, amely továbbítja az információkat vissza az LPAR2 partícióra.



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

A Megbízható tűzfal használatával konfigurálhat szabályokat, hogy az információk az LPAR1 partícióról az LPAR2 partícióra a belső hálózat elhagyása nélkül mehessenek át. Ez az útvonal látható a következő helyen is: 2. ábra: oldalszám: 12.



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

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

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

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

Megbízható tűzfal telepítése

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

Előfeltételek:

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

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

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

A Megbízható tűzfal funkció hozzáadásához egy meglévő PowerSC példányhoz:

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

Kapcsolódó tájékoztatás:

“PowerSC Standard Edition 1.1.3 telepítése” oldalszám: 3
A PowerSC Standard Edition minden egyes adott funkciójához telepítenie kell egy fájlkészletet.

Megbízható tűzfal konfigurálása

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

Megbízható tűzfal megfigyelés

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

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

A Megbízható tűzfal megfigyelés engedélyezéséhez adja ki a következő parancsot:

```
vlantfw -m
```

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

```
vlantfw -D
```

A Megbízható tűzfal megfigyelés letiltásához adja ki a következő parancsot:

```
vlantfw -M
```

Megbízható tűzfal naplózás

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

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

A Megbízható tűzfal naplózás elindításához adja ki a következő parancsot:

```
vlantfw -l
```

A Megbízható tűzfal naplózás leállításához adja ki a következő parancsot:

```
vlantfw -L
```

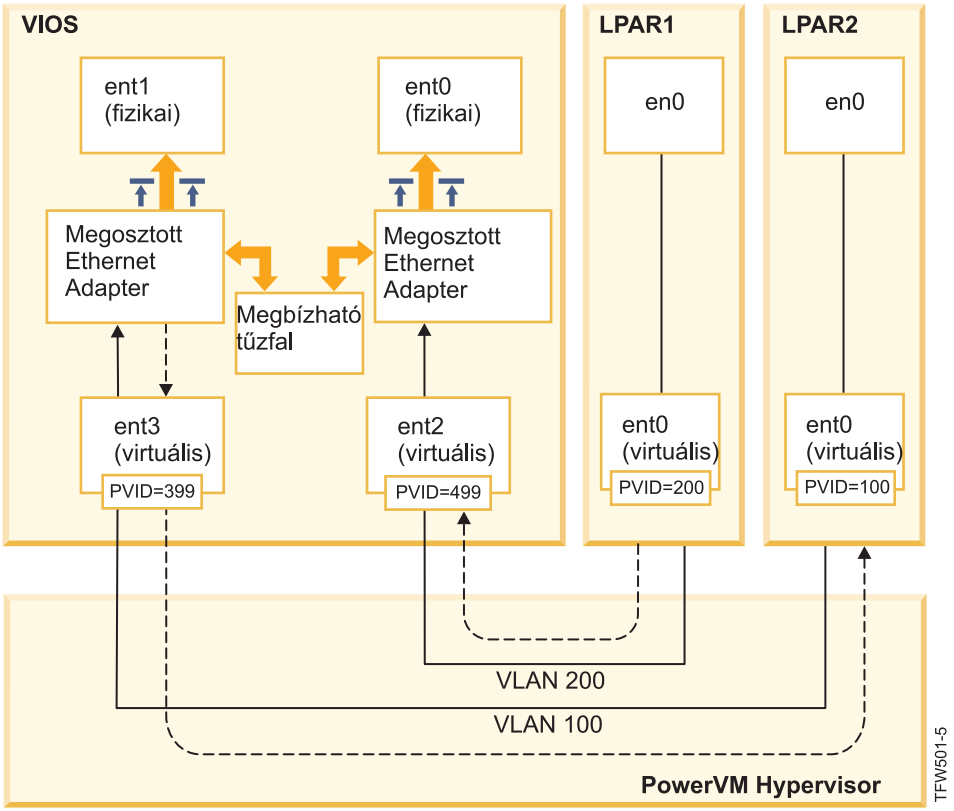
A naplófájlt a következő helyen tekintheti meg: /home/padmin/svm/svm.log.

Több Megosztott Ethernet adapter

A Megbízható tűzfal konfigurálható több Megosztott Ethernet adaptert használó rendszereken.

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

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



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

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

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

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

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

- Több VIOS és több SEA illesztőprogram.

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

Megosztott Ethernet adapterek eltávolítása

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

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

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

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

Szabályok létrehozása

Létrehozhat szabályokat a Megbízható tűzfal VLAN hálózatok közötti útválasztásához.

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

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

Egy szabály létrehozásához tegye a következőket:

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

   Azoknak a logikai partícióknak (LPAR) az IP és MAC címére lesz szüksége, amelyekhez szabályokat szeretne létrehozni.
5. Hozza létre a szűrőszabályt a két LPAR (LPAR1 és LPAR2) közötti kommunikáció engedélyezéséhez a következő parancsok egyikének kiadásával:
   - `genvfilt -v4 -a P -z [lpar1vlanid] -Z [lpar2vlanid] -s [lpar1ipaddress] -d [lpar2ipaddress]`
   - `genvfilt -v4 -a P -z [lpar1vlanid] -Z [lpar2vlanid] -s [lpar1ipaddress] -d [lpar2ipaddress]-o any -p 0 -O gt -P 23`

   Megjegyzés: Az egyik szűrőszabály alapértelmezés szerint mindkét irányban engedélyezi a kommunikációt, a port és protokoll bejegyzésektől függően. Például a Telnet kommunikációt az LPAR1 partícióról az LPAR2 partíció irányában a következő parancs futtatásával engedélyezheti:
   ```
   genvfilt -v4 -a-P -z [lpar1vlanid] -Z [lpar2vlanid] -s [lpar1ipaddress] -d [lpar2ipaddress] -o any -p 0 -O eq -P 23
   ```
6. A kernelben lévő összes szűrőszabály aktiválásához a következő parancsot adja ki:
   ```
   mkvfilt -u
   ```

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

További példák

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

- A Secure Shell kommunikáció engedélyezéséhez a VLAN 100 hálózaton található LPAR partícióról a VLAN 200 hálózaton található LPAR partícióra, adja ki a következő parancsot:
  ```
  genvfilt -v4 -a P -z 100 -Z 200 -o any -p 0 -O eq -P 22 -c tcp
  ```
- A 0 - 499 tartományba eső összes port közötti forgalom engedélyezéséhez adja ki a következő parancsot:
  ```
  genvfilt -v4 -a P -z 100 -z 200 -o lt -p 500 -O lt -P 500 -c tcp
  ```
- A logikai partíciók közötti összes TCP forgalom engedélyezéséhez adja ki a következő parancsot:
  ```
  genvfilt -v4 -a P -z 100 -Z 200 -c tcp
  ```

  Ha nem ad meg portokat vagy portműveleteke, akkor a forgalom minden portot használhat.
- Az Internet vezérlőüzenet protokoll (ICMP) üzenetek engedélyezéséhez a logikai partíciók között, adja ki a következő parancsot:
  ```
  genvfilt -v4 -a P -z 100 -Z 200 -c icmp
  ```

Kapcsolódó fogalmak:

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

Kapcsolódó hivatkozás:

“genvfilt parancs” oldalszám: 32

“mkvfilt parancs” oldalszám: 34

“vlantfw parancs” oldalszám: 44

Kapcsolódó tájékoztatás:

Virtuális I/O szerver

Szabályok deaktiválása

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

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

Egy szabály deaktiválásához tegye a következőket:

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

   Az **-a** kapcsoló elhagyásával az Objektumadat-kezelőben tárolt összes szabályt jelenítheti meg.
3. Jegyezze fel a deaktiválni kívánt szűrőszabály azonosítószámát. Ebben a példában a szűrőszabály azonosítószáma 23.
4. A kernelben aktív 23-as azonosítószámú szűrőszabály deaktiválásához adja ki a következő parancsot:
   ```
   rmvfilt -n 23
   ```

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

Kapcsolódó fogalmak:

“Szabályok létrehozása” oldalszám: 15
Létrehozhat szabályokat a Megbízható tűzfal VLAN hálózatok közötti útválasztásához.

Kapcsolódó hivatkozás:

“lsvfilt parancs” oldalszám: 33

“rmvfilt parancs” oldalszám: 43

Megbízható naplózás

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

Virtuális naplók

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

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

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

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

- Kliens neve
- Napló neve

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

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

Kapcsolódó tájékoztatás:

Virtuális naplók létrehozása

Virtuális naplóeszközök észlelése

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

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

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

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

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

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

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

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

A virtuális napló kétféle típusú naplóadatot tárol. Ezek:

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

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

Megbízható naplózás telepítése

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

A Megbízható naplózás előfeltételei a VIOS 2.2.1.0 vagy újabb változat, és az 7-es technikai szintű IBM AIX 6 változat vagy 1-es technikai szintű IBM AIX 7 változat.

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

A Megbízható naplózás funkció telepítéséhez:

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

Kapcsolódó tájékoztatás:

“PowerSC Standard Edition 1.1.3 telepítése” oldalszám: 3

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

Megbízható naplózás konfigurálása

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

AIX megfigyelési alrendszer konfigurálása

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

Megjegyzés: Mielőtt konfigurálná az AIX megfigyelési alrendszert, el kell végeznie a következő helyen leírt eljárást: “Virtuális naplóeszközök észlelése” oldalszám: 17.

Az AIX megfigyelési alrendszer konfigurálásához tegye a következőket:

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

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

   ```
   audit shutdown
   audit start
   ```

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

Kapcsolódó tájékoztatás:

Megfigyelési alrendszer

syslog konfigurálása

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

Megjegyzés: Mielőtt konfigurálná az /etc/syslog.conf fájlt, el kell végeznie a következő helyen leírt eljárást: “Virtuális naplóeszközök észlelése” oldalszám: 17.

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

- Funkció
- Prioritási szint

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

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

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

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

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

```
refresh -s syslogd
```

Kapcsolódó tájékoztatás:

syslogd démon

Adatok írása virtuális naplóeszközökbe

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

Például:

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

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

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

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

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

Megbízható hálózati kapcsolat és javításkezelés

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

Megbízható hálózati kapcsolat alapelvek

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

Megbízható hálózati kapcsolat összetevői

A Megbízható hálózati kapcsolat (TNC) keretrendszer összetevőinek bemutatása.

A TNC modell a következő összetevőkből áll:

Megbízható hálózati kapcsolat szerver:

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

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

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

Javításkezelés:

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

Az AIX SUMA letölti az IBM ECC és Fix Central webhelyeken elérhető legfrissebb javítócsomagokat és biztonsági javításokat. A TNC és a javításkezelés démon feltölti a legutóbbi frissített információkat a TNC szerverre, amely egy alapsor fájlkészletként szolgál a kliensek ellenőrzéséhez.

A **tncpmd** démont konfigurálni kell a Szolgáltatásfrissítés-kezelő segéd (SUMA) letöltések kezeléséhez és a fájlkészlet információk feltöltéshez a TNC szerverre. A démont egy Internethez csatlakozó rendszeren kell futtatni, hogy képes legyen automatikusan letölteni a frissítéseket. A TNC javításkezelő szerver Internet-kapcsolat nélküli használatához regisztrálhat egy felhasználó által megadott javításlerakatot a TNC javításkezelő szerveren.

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

Megbízható hálózati kapcsolat kliens:

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

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

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

Megbízható hálózati kapcsolat IP hivatkozó:

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

Megbízható hálózati kapcsolat - biztonságos kommunikáció

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

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

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

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

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

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

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

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

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

Megbízható hálózati kapcsolat protokoll

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

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

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

IMC és IMV modulok

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

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

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

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

Kapcsolódó hivatkozás:

“psconf parancs” oldalszám: 38

Megbízható hálózati kapcsolat telepítése

A Megbízható hálózati kapcsolat (TNC) telepítéséhe el kell végeznie bizonyos lépéseket.

A TNC összetevőinek használatához szükséges beállítások konfigurálásához tegye a következőket:

1. Azonosítsa a rendszerek IP címeit a TNC szerver, a Megbízható hálózati kapcsolat és javításkezelés (TNCPM) szerver, valamint a TNC IP hivatkozó beállításához a Virtuális I/O szerverhez (VIOS).

   Megjegyzés: A TNC szerver nem konfigurálható TNC kliensként.
2. Állítsa be a hálózati telepítéskezelő (NIM) szervert. A szerverként konfigurált rendszer a NIM mester, és a sets:bos.sysmgt.nim.master fájlkészleteket a kliens rendszereken kell telepíteni.
3. Konfigurálja a TNCPM szervert. Ez a konfiguráció a NIM rendszeren állítható be. A TNCPM szerver a SUMA használatával tölti le a javításokat az IBM Fix Central és ECC webhelyekről. A frissítések letöltéséhez a rendszernek csatlakoznia kell az Internethez. Adja ki a következő parancsot a TNCPM szerver konfigurálásához:

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

   Például:

   ```
   pmconf mktncpm pmport=20000 tncserver=1.1.1.1:10000
   ```
4. Konfigurálja az irányelveket a TNC szerveren. A kliensek ellenőrzésére szolgáló irányelvek létrehozását a következő témakör mutatja be: “Irányelvek létrehozása a Megbízható hálózati kapcsolat klienshez” oldalszám: 26.
5. Konfigurálja a TNC IP hivatkozót a VIOS rendszeren. Ez a konfiguráció a VIOS rendszeren aktiválja az ellenőrzést a hálózathoz csatlakozó klienseken. Adja ki a következő parancsot a hivatkozó konfigurálásához:

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

   Például:

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

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

6. Konfigurálja a klienseket a következő parancs használatával:

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

Például:

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

Kapcsolódó hivatkozás:

“psconf parancs” oldalszám: 38

Kapcsolódó tájékoztatás:

“PowerSC Standard Edition 1.1.3 telepítése” oldalszám: 3
A PowerSC Standard Edition minden egyes adott funkciójához telepítenie kell egy fájlkészletet.

Telepítés NIM segítségével

IBM Fix Central

Passport Advantage Online súgóközpont

Megbízható hálózati kapcsolat és javításkezelés konfigurálása

A Megbízható hálózati kapcsolat (TNC) keretrendszert egy javításkezelési démonként kell beállítani. A TNC szerver a SUMA funkcióval integrálva egy átfogó javításkezelési megoldást biztosít.

Megbízható hálózati kapcsolat szerver konfigurálása

Megismerheti a TNC szerver konfigurálásához szükséges lépéseket.

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

```
component = SERVER
```

Egy rendszer konfigurálásához szerverként, adja ki a következő parancsot:

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

Például:

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

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

A rendszer a tncport porthoz 42830 perces, a pmserver porthoz 38240 perces alapértelmezett portértéket használ.

Kapcsolódó hivatkozás:

“psconf parancs” oldalszám: 38

Megbízható hálózati kapcsolat kliens konfigurálása

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

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

```
component = CLIENT
```

Egy rendszer konfigurálásához kliensként, adja ki a következő parancsot:

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

Például:

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

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

Kapcsolódó hivatkozás:

“psconf parancs” oldalszám: 38

Javításkezelő szerver konfigurálása

Megismerheti a lépéseket, amelyekkel javításkezelő szerverként konfigurálhat egy rendszert.

A Megbízható hálózati kapcsolat (TNC) javításkezelő szervert a Hálózati telepítéskezelő (NIM) szerveren kell konfigurálni, így a TNC kliensek frissíthetők.

A TNC javításkezelés javításlerakatainak inicializálásához adja ki a következő parancsot:

```
pmconf init -i <letöltési_időköz> -l
<TL lista> [-A] [-P <letöltési útvonal>][-x <ifix időköz>]
[-K <ifix kulcs>]
```

Példa a **pmconf** parancsra:

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

Az **init** parancs letölti az egyes technológia szintekhez tartozó legfrissebb javítócsomagot, és elérhetővé teszi azt a TNC szerver számára. A frissített javítócsomagok lehetővé teszik, hogy a TNC szerver lefuttasson egy alapsor TNC kliens ellenőrzést, illetve a TNC javításkezelő szerver telepítse a TNC kliensfrissítéseket. Adja meg az **-A** kapcsolót az összes licencszerződés elfogadásához a kliensfrissítések futtatásakor. Alapértelmezés szerint a TNC javításkezelő szerver által letöltött javításlerakatok a /var/tnc/tncpm/fix_repository fájlban találhatók. A **-P** kapcsolóval megadhat egy eltérő könyvtárat.

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

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

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

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

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

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

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

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

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

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

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

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

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

Íme egy példa erre a parancsra:

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

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

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

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

- HIPER
- PE
- Enhancement

A TNC javításkezelő szerver támogatja a **syslog** funkciót a javítócsomag, technológia szint és kliensfrissítések letöltéséhez. A szolgáltatás user, a prioritás pedig info. Egy példa erre a user.info.

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

Kapcsolódó hivatkozás:

“psconf parancs” oldalszám: 38

Kapcsolódó tájékoztatás:

IBM AIX biztonság

Megbízható hálózati kapcsolat szerver e-mail értesítés konfigurálása

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

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

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

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

| Például:

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

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

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

```
psconf
add –e <e-mail_cím>
```

| Például:

```
psconf add –e abc@ibm.com
```

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

Kapcsolódó hivatkozás:

“psconf parancs” oldalszám: 38

IP hivatkozó konfigurálása VIOS rendszeren

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

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

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

Egy rendszert a következő parancs kiadásával konfigurálhat kliensként:

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

Például:

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

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

Kapcsolódó hivatkozás:

“psconf parancs” oldalszám: 38

Megbízható hálózati kapcsolat és javításkezelés kezelése

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

Megbízható hálózati kapcsolat szervernaplók megtekintése

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

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

```
psconf list –H –i <ip |ALL>
```

Kapcsolódó hivatkozás:

“psconf parancs” oldalszám: 38

Irányelvek létrehozása a Megbízható hálózati kapcsolat klienshez

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

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

A következő irányelvek hozhatók létre:

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

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

| Egy IP csoport létrehozásához adja ki a következő parancsot:

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

| Például:

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

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

| Egy fájlkészlet irányelv létrehozásához adja ki a következő parancsot:

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

| Például:

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

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

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

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

| Például:

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

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

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

Például:

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

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

Kapcsolódó hivatkozás:

“psconf parancs” oldalszám: 38

Megbízható hálózati kapcsolat kliens ellenőrzésének elindítása

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

A kliens ellenőrzéséhez a következő módszerek egyikét használhatja:

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

  ```
  tncconsole verify -i <ip>
  ```

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

Kapcsolódó hivatkozás:

“psconf parancs” oldalszám: 38

Megbízható hálózati kapcsolat hitelesítési eredményeinek megtekintése

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

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

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

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

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

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

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

Kapcsolódó hivatkozás:

“psconf parancs” oldalszám: 38

Megbízható hálózati kapcsolat kliens frissítése

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

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

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

Például:

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

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

Kapcsolódó hivatkozás:

“psconf parancs” oldalszám: 38

Javításkezelési irányelvek kezelése

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

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

A javításkezelési irányelv kezeléséhez adja ki a következő parancsot:

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

Például:

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

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

Kapcsolódó hivatkozás:

“pmconf parancs” oldalszám: 34

Megbízható hálózati kapcsolat tanúsítványok importálása

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

A Megbízható hálózati kapcsolat (TNC) démonok a Szállítási réteg biztonsága (TLS) vagy Védett socket réteg (SSL) protokoll használatával támogatott titkosított csatornákon keresztül kommunikálnak. Ez a démon biztosítja, hogy a hálózaton szállított adatok és parancsok hitelesítve és védve legyenek. Minden egyes rendszernek megvan a saját kulcsa és tanúsítványa, amelyek az összetevők inicializálási parancsának futtatásakor kerülnek előállításra. Ez a folyamat az adminisztrátor számára átlátszó, és kevesebb adminisztrátori beavatkozást igényel. Egy kliens első alkalommal történő ellenőrzésekor a kliens tanúsítványa importálásra kerül a szerver adatbázisába. A tanúsítvány kezdetben megbízhatatlanként van megjelölve, és az adminisztrátor a **psconf** parancs futtatásával tekintheti meg és jelölheti meg a megbízhatóként:

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

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

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

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

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

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

Kapcsolódó hivatkozás:

“psconf parancs” oldalszám: 38

TNC szerver jelentéskészítés

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

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

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

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

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

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

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

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

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

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

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

| **Kapcsolódó hivatkozás**:
| “psconf parancs” oldalszám: 38

Megbízható hálózati kapcsolat és javításkezelés hibaelhárítása

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

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

3. táblázat: TNC és javításkezelési rendszer konfigurációs beállításainak hibaelhárítása

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

PowerSC Standard Edition parancsok

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

chvfilt parancs

Cél

Módosítja a meglévő virtuális LAN kereszteződési szűrőszabály értékeit.

Szintaxis

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

Leírás

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

Kapcsolók

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

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

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

-m Megadja a forrás cím maszkját.

-M Megadja a cél cím maszkját.

-n Megadja a módosítandó szűrőszabály szűrőazonosítóját.

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

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

-p Megadja a forrás portot vagy az ICMP típust.

-P Megadja a cél portot vagy az ICMP kódot.

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

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

-z Megadja a forrás logikai partíció virtuális LAN azonosítóját.

-Z Megadja a cél logikai partíció virtuális LAN azonosítóját.

Kilépési állapot

Ez a parancs a következő kilépési értékeket adja vissza:

0 Sikeres befejeződés.

>0 Hiba történt.

Példák

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

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

genvfilt parancs

Cél

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

Szintaxis

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

Leírás

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

Kapcsolók

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

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

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

-m Megadja a forrás cím maszkját

-M Megadja a cél cím maszkját.

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

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

-p Megadja a forrás portot vagy az ICMP típust.

-P Megadja a cél portot vagy az ICMP kódot.

-s A forrás címet adja meg IPv4 vagy IPv6 formátumban.

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

-z Megadja a forrás LPAR virtuális LAN azonosítóját. A virtuális LAN azonosítónak az 1 - 4096 tartományba kell esnie.

-Z Megadja a cél LPAR virtuális LAN azonosítóját. A virtuális LAN azonosítónak az 1 - 4096 tartományba kell esnie.

Kilépési állapot

Ez a parancs a következő kilépési értékeket adja vissza:

0 Sikeres befejeződés.

>0 Hiba történt.

Példák

1. Egy szűrőszabály hozzáadásához, amely engedélyezi a TCP adatokat a 100-as forrás VLAN azonosítóról a 200-as cél VLAN azonosítóra megadott portokon keresztül, írja be a parancsot a következők szerint:

```
genvfilt -v4 -a P -z 100 -Z 200  -o lt -p 345 -O lt -P 345 -c tcp
```

Kapcsolódó hivatkozás:

“mkvfilt parancs” oldalszám: 34

“vlantfw parancs” oldalszám: 44

lsvfilt parancs

Cél

Felsorolja a virtuális LAN kereszteződési szűrőszabályokat a szűrő táblából.

Szintaxis

lsvfilt [**-a**]

Leírás

Az **lsvfilt** parancs arra szolgál, hogy felsorolja a virtuális LAN kereszteződési szűrőszabályokat és azok állapotát.

Kapcsolók

-a Csak az aktív szűrőszabályokat sorolja fel.

Kilépési állapot

Ez a parancs a következő kilépési értékeket adja vissza:

0 Sikeres befejeződés.

>0 Hiba történt.

Példák

1. A kernelben lévő összes aktív szűrőszabály felsorolásához írja be a parancsot a következők szerint:

```
lsvfilt -a
```

Kapcsolódó fogalmak:

“Szabályok deaktiválása” oldalszám: 16
A Megbízható tűzfal szolgáltatásban a VLAN hálózatok közötti továbbítást engedélyező szabályok deaktiválhatók.

mkvfilt parancs
Cél

Aktiválja a **genvfilt** parancs által meghatározott virtuális LAN kereszteződési szűrőszabályokat.

Szintaxis

mkvfilt -u

Leírás

Az **mkvfilt** parancs aktiválja a **genvfilt** parancs által meghatározott virtuális LAN kereszteződési szűrőszabályokat.

Kapcsolók

-u Aktiválja a szűrőszabály táblában lévő szűrőszabályokat.

Kilépési állapot

Ez a parancs a következő kilépési értékeket adja vissza:

0 Sikeres befejeződés.

>0 Hiba történt.

Példák

1. A szűrőszabályok aktiválásához a kernelben, írja be a parancsot a következők szerint:

```
mkvfilt -u
```

Kapcsolódó hivatkozás:

“genvfilt parancs” oldalszám: 32

pmconf parancs
Cél

Jelentéseket készít és felügyeli a Megbízható hálózati kapcsolat javításkezelő (TNCPM) szervert a technológia szintek és TNC szerverek regisztrálásával a legújabb frissítések beszerzéséhez, illetve a TNCPM állapotára vonatkozó jelentések előállításával.

Megjegyzés: A TNCPM szerver csak AIX 7.1 változaton, a 7100-02 technológia szinten futtatható, hogy a javítócsomagok metaadatai letölthetők legyenek.

Szintaxis

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

pmconf rmtncpm

pmconf start

pmconf stop

pmconf init -i <*letöltési időköz*> **-l** <*TL_lista*> **-A** [**-P** <*letöltési_útvonal*>] [**-x** <*ifix időköz*>] [**-K** <*ifix kulcs*>]

pmconf add -l *TL_lista*

pmconf add -p <*SP_lista*> [**-U** <*felhasználó_által_meghatározott_SP_útvonal*>]

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

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

pmconf delete -l *TL_lista*

pmconf delete -p <*SP_lista*>

pmconf delete -p <*SP*>**-e** *ifix_fájl*

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

pmconf list -l *SP*

pmconf list -C

pmconf list -a *SP*

pmconf hist -u

pmconf hist -d

pmconf import -f *tanúsítványfájl_neve* **-k** *kulcsfájl_neve*

pmconf export -f *fájlnév*

pmconf modify -i <*letöltési_időköz*>

pmconf modify -P <*letöltési_útvonal*>

pmconf modify -g <*yes vagy no az összes licenc elfogadásához*>

pmconf modify -t <*APAR_típusok_listája*>

pmconf modify -x <*ifix_időköz*>

pmconf modify -K <*ifix_kulcs*>

pmconf delete -l <*TL_lista*>

pmconf restart

pmconf status

pmconf log loglevel = info | error | none

pmconf chtncpm attribute = *érték*

Leírás

A **pmconf** parancs függvényei a következők:

Javításlerakat kezelése
Technológia szinteket regisztrál vagy megszünteti ezek regisztrálását; megszünteti TNC szerverek regisztrálását. A TNCPM minden olyan technológia szinthez létrehoz egy javításlerakatot, amely a legutóbbi javításokat, **lslpp** információkat (például a telepített fájlkészletekkel vagy fájlkészletfrissítésekkel kapcsolatos információkat), illetve az adott technológia szintre vonatkozó biztonsági javítási információkat tartalmazza.

Jelentéskészítés
Jelentéseket állít elő a TNCPM állapotáról.

A **pmconf** parancs segítségével a következő műveletek hajthatók végre:

Elem	Leírás
add	Regisztrál egy új technológia szintet a TNCPM használatával.
chtncpm	Módosítja a tnccs.conf fájlban lévő attribútumokat. Ahhoz, hogy a módosítások érvénybe lépjenek a TNCPM szerveren, egy kifejezett **start** utasítás kiadása szükséges.
delete	Megszünteti egy technológia szint regisztrálását a TNCPM szerver használatával.
history	Megjeleníti a frissítési és letöltési előzményeket.
list	Megjeleníti a TNCPM információit.
log	Beállítja a TNC összetevők naplózási szintjét.
mktncpm	Létrehozza a TNCPM szervert.
modify	Módosítja a tncpm.conf attribútumokat.
rmtncpm	Eltávolítja a TNCPM szervert.
start	Elindítja a TNCPM szervert.
stop	Leállítja a TNCPM szervert.

Kapcsolók

Elem	Leírás
-A	Elfogadja az összes licencszerződést a kliensfrissítések végrehajtásakor.
-a <tanácsadófájl>	Megadja az **ifix** paraméternek megfelelő tanácsadófájlt. Ha nincs megadva tanácsadófájl, akkor az **ifix** paraméter nem tekinti a köztes javítás Általános sebezhetőségek és veszélyeztetettség (CVE) címeként.
-e <ifix_fájl>	Megadja a TNCPM szerverhez hozzáadott köztes javításokat.
-i *letöltési_időköz*	Megadja az időközt, amely alapján a TNCPM ellenőrzi az új javítócsomagok megjelenését a regisztrált technológia szintekhez. Az időköz egy egész szám érték, amely perceket vagy napokat ábrázol a következő formátumban: **d** (nincs megadva, ha nincsenek napok): **h** (órák): **m** (percek).
-K <ifix_kulcs>	Megadja a tanácsadók és köztes javítások hitelesítéséhez használt IBM AIX Product Security Incident Response Tool (PSIRT) nyilvános kulcsát. Ez a nyilvános kulcs egy PGP nyilvános kulcs szerverről tölthető le, a **0x28BFAA12** azonosító használatával.
-p *SP_lista*	Megadja a letöltendő javítócsomagok listáját. A lista egy REL00-TL-SP formátumú elemekből álló vesszővel elválasztott lista (például 6100-01-04 a 6.1 változat 01-es technológia szintjéhez tartozó 04-es javítócsomagot ábrázolja). Az -U kapcsoló használata esetén csak a javítócsomagot (SP) adja meg.
-t *APAR_típusok_listája*	Megadja az APAR típusokat, amelyeket a TNCPM a kliensfrissítésekhez és TNC szerver felsorolásokhoz támogat. A biztonsági APAR javítások mindig támogatottak. Az APAR_típusok_listája paraméter a következő típusok vesszővel elválasztott listáját tartalmazhatja: HIPER, FileNet Process Engine, Enhancement.
-P *javításlerakat_útvonala*	Megadja a TNCPM által letöltésre kerülő javításlerakatok letöltési könyvtárát. Az alapértelmezett könyvtár a **/var/tnc/tncpm/fix_repository**.
-U *felhasználó_által_megadott_javításlerakat*	Megadja a felhasználó által megadott javításlerakat útvonalát. Adja meg a kliensek ellenőrzéséhez és frissítéseihez használt javításlerakattal társított kiadást, technológia szintet és javítócsomagot.
-s	Előállít egy jelentést a regisztrált javítócsomagokról.
-l *SP*	Előállít egy jelentést a javítócsomag **lslpp** információiról. Az *SP* paraméter formátuma REL00-TL-SP (például 6100-01-04 a 6.1 változat 01-es technológia szintjéhez tartozó 04-es javítócsomagot ábrázolja).
-u	Előállít egy jelentés a kliens frissítési előzményeiről.
-d	Előállít egy jelentés a javítócsomag letöltések előzményeiről.
-C	Előállít egy jelentés a szervertanúsítványról.
-a *SP*	Előállít egy jelentést a javítócsomag biztonsági jogosult programelemzési jelentés (APAR) információiról. Az *SP* paraméter formátuma REL00-TL-SP (például 6100-01-04 a 6.1 változat 01-es technológia szintjéhez tartozó 04-es javítócsomagot ábrázolja).
-f *fájlnév*	Megadja a tanúsítványfáj nevét.
-k *kulcsfájl_neve*	Megadja a fájlt, amelyből a tanúsítványkulcsot egy importálási művelet során be kell olvasni.

Elem	Leírás

-c	Megjeleníti a felhasználói attribútumokat pontosvesszővel elválasztott rekordokban, az alábbiak szerint:
	`# name: attribútum1: attribútum2: ...`
	`policy: érték1: érték2: ...`

-v <*aláírásfájl*>	Megadja az aláírásfájlt az IBM AIX sebezhetőségi tanácsadóhoz.
-y <*tanácsadófájl*>	Megad egy IBM AIX sebezhetőségi tanácsadó fájlt.
-q	Kikapcsolja a fejlécinformációkat.
-x <*ifix_időköz*>	Percekben megadja az időközt, amely szerint új köztes javításokat kell keresni és letölteni. Ha az érték 0-ra van beállítva, akkor a köztes javítások automatikus letöltése és az értesítés le van tiltva. Az alapbeállítás 24 óra.

Kilépési állapot

Ez a parancs a következő kilépési értékeket adja vissza:

Elem	Leírás
0	A parancs sikeresen lefutott, és minden kért módosítás megtörtént.
>0	Hiba történt. A kiírt hibaüzenet további részleteket biztosít a hiba típusáról.

Példák

1. A TNCPM, inicializálásához adja ki a következő parancsot:
   ```
   pmconf init -f 10080 -l 5300-11,6100-00
   ```
2. A TNCPM démon létrehozásához adja ki a következő parancsot:
   ```
   mktncpm pmport=55777 tncserver=11.11.11.11:77555
   ```
3. A szerver elindításához adja ki a következő parancsot:
   ```
   pmconf start
   ```
4. A szerver leállításához adja meg a következő parancsot:
   ```
   pmconf stop
   ```
5. Egy új technológia szint regisztrálásához a TNCPM használatával, adja ki a következő parancsot:
   ```
   pmconf add -l 6100-01
   ```
6. Egy technológia szint regisztrálásának megszüntetéséhez a TNCPM összetevőben, adja ki a következő parancsot:
   ```
   pmconf delete -l 6100-01
   ```
7. Egy 11.11.11.11 IP címmel rendelkező TNC szerver regisztrációjának megszüntetéséhez a TNCPM szerveren, adja ki a következő parancsot:
   ```
   pmconf delete -t 11.11.11.11
   ```
8. Egy korábbi javítócsomag újabb változatának regisztrálásához a TNCPM szerveren, adja ki a következő parancsot:
   ```
   pmconf add -s 6100-01-04
   ```
9. Egy korábbi javítócsomag regisztrálásának megszüntetéséhez a TNCPM összetevőben, adja ki a következő parancsot:
   ```
   pmconf delete -s 6100-01-04
   ```
10. Az egyes regisztrált technológia szintekhez tartozó javításlerakatokról készült jelentés előállításához adja ki a következő parancsot:
    ```
    pmconf list -s
    ```
11. Egy regisztrált technológia szint **lslpp** információiról készült jelentés előállításához adja ki a következő parancsot:
    ```
    pmconf list -l 6100-01-02
    ```
12. A frissítési előzményekből készült jelentés előállításához adja ki a következő parancsot:
    ```
    pmconf hist -u
    ```
13. A letöltési előzményekből készült jelentés előállításához adja ki a következő parancsot:
    ```
    pmconf hist -d
    ```
14. A szervertanúsítványról készült jelentés előállításához adja ki a következő parancsot:

```
pmconf list -C
```

15. Egy javítócsomag biztonsági APAR információiról készült jelentés előállításához adja ki a következő parancsot:
```
pmconf list -a 6100-01-02
```
16. Egy szervertanúsítvány importálásához adja ki a következő parancsot:
```
pmconf import -f /tmp/server.txt -k /tmp/server-cert-key.txt
```
17. Egy szervertanúsítvány exportálásához adja ki a következő parancsot:
```
pmconf export -f /tmp/server.txt
```

psconf parancs

Cél

Jelentéseket készít és felügyeli a Megbízható hálózati kapcsolat (TNC) szervert, a TNC klienst, a TNC IP hivatkozót (IPRef) és a Szolgáltatásfrissítés-kezelő segéd (SUMA) összetevőt. Felügyeli a fájlkészlet és javításkezelési irányelveket a végpont (szerver és kliens) integritása tekintetében a hálózati kapcsolat létrejöttekor vagy az után, hogy megvédje a hálózatot a fenyegetésektől és támadásoktól.

Szintaxis

TNC szerver műveletek:

psconf mkserver [**tncport=**<*port*>] **pmserver=**<*hoszt***:***port*> [tsserver=<hoszt>] [**recheck_interval=**<*idő_percben*> | **d** (nap) : **h** (óra) : **m** (perc)] [**dbpath** = <*felhasználó_által_megadott_könyvtár*>]

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

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

psconf chserver attribute = *érték*

psconf add -F <*FS_irányelv_neve*> -r <*összeépítési_info*> [**apargrp=** [**±**]<*aparcsop1, aparcsop2.. >*] [*ifixgrp*=[+|-]<*ifixcsop1*,*ifixcsop2...*>]

psconf add { **-G** <*ip_csoport_neve*> **ip=**[**±**]<*hoszt1, hoszt2...*> | {**-A**<*apar_csoport*> [**aparlist**=[**±**]*apar1, apar2...* | {**-V** <*ifix_csoport*> [*ifixlist*=[+|-]*ifix1*,*ifix2...*]}

psconf add -P <*irányelvnév*> { **fspolicy=**[**±**]<*f1,f2...*> | **ipgroup=**[**±**]<*g1,g2...*> }

psconf add -e *email_azonosító* [-E FAIL | COMPLIANT | ALL] [**ipgroup=** [**±**]<*g1,g2...*>]

psconf add -I ip= [**±**]<*hoszt1, hoszt2...*>

psconf delete { **-F** <*FS_irányelv_neve*> | **-G** <*ip_csoport_neve*> | **-P** <*irányelvnév*> | **-A** <*apar_csoport*> | **-V** <*ifix_csoport*>}

psconf delete -H -i <*hoszt* | **ALL**> **-D** <*éééé-hh-nn*>

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

psconf certdel -i <*hoszt*>

psconf verify -i <*hoszt*> | **-G** <*ip_csoport*>

psconf update [-p] {**-i**< *hoszt* >| **-G** <*ip_csoport*> [**-r** <*összeépítési_info*> | **-a** <*apar1, apar2...*> | [**-u**] **-v** <*ifix1*, *ifix2*,...>}

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

| **psconf import -C -i** <*hoszt*> **-f** <*fájlnév*> **| –d** <*import_adatbázis_fájlnév*>

| **psconf** { **import -k** <*kulcsfájl_neve*> **| export**} **-S -f** <*fájlnév*>

| **psconf list** { **-S | -G** < *ip_csoport_neve* | **ALL** > | **-F** < *FS_irányelv_neve* | **ALL** > | **-P** < *irányelvnév* | **ALL** > | **-r** <
| *összeépítési_info* | **ALL** > | **-I -i** < *ip* | **ALL** > | **-A** < *apar_csoport* | **ALL** > | **-V** <*ifix_csoport*>} [**-c**] [**-q**]

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

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

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

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

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

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

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

| TNC kliens műveletek:

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

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

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

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

| **psconf chclient** attribute = *érték*

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

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

| **psconf import** { **-S | -C -k** <*kulcsfájl_neve*> } **-f** <*fájlnév*>

| TNC IPRef műveletek:

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

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

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

| **psconf chipref** attribute = *érték*

| **psconf** { **import -k** <*kulcsfájl_neve*> **| export** } **-R -f** <*fájlnév*>

| **psconf list -R**

Leírás

A TNC technológia egy nyílt szabványon alapuló architektúra a végpontok hitelesítéséhez, a platform integritás méréséhez, valamint biztonsági rendszerek integrálásához. A TNC architektúra megvizsgálja a végpontokat (hálózati kliensek és szerverek) a biztonsági irányelveknek való megfelelés tekintetében, mielőtt beengedné azokat a védett hálózatba. A TNC IPRef értesíti a TNC szervert bármilyen új IP címről, amelyet a virtuális I/O szerveren (VIOS) észlel.

A SUMA mentesíti a rendszergazdákat attól, hogy kézzel kelljen letölteniük a webről a karbantartási frissítéseket. Rugalmas beállításokat biztosít, amelyekkel a rendszeradminsztrátor beállíthat egy automatizált felületet a javítások letöltéséhez egy javításterjesztő webhelyről a helyi rendszerekre.

A hálózati szervert és klienseket a **psconf** paranccsal kezelheti: biztonsági irányelveket vehet fel és törölhet, klienseket érvényesíthet megbízhatóként vagy megbízhatatlanként, jelentéseket állíthat elő és frissítheti a szervert és a klienst.

A **psconf** parancs segítségével a következő műveletek hajthatók végre:

Elem	Leírás
add	Hozzáad egy irányelvet, egy klienst vagy az e-mail információkat a TNC szerveren.
apargrp	Megadja a TNC kliensek ellenőrzéséhez használt APAR csoportneveket a fájlkészlet irányelv részeként.
aparlist	Megadja az APAR csoport részét képező APAR jelentések listáját.
certadd	Megbízhatóként vagy megbízhatatlanként jelöli meg a tanúsítványt.
certdel	Törli a kliensinformációkat.
chclient	Módosítja a tnccs.conf fájlban lévő attribútumokat. Ahhoz, hogy a módosítások érvénybe lépjenek a TNC kliensben, egy kifejezett **start** utasítás kiadása szükséges. Az attribútum=érték szintaxis ugyanaz lesz, mint az **mkclient** esetén.
chipref	Módosítja a tnccs.conf fájlban lévő attribútumokat. Ahhoz, hogy a módosítások érvénybe lépjenek az IPRef összetevőben, egy kifejezett **start** utasítás kiadása szükséges. Az attribútum=érték szintaxisa ugyanaz, mint az **mkipref** esetén.
chserver	Módosítja a tnccs.conf fájlban lévő attribútumokat. Ahhoz, hogy a módosítások érvénybe lépjenek a TNC szerveren, egy kifejezett **start** utasítás kiadása szükséges. Az attribútum=érték szintaxisa ugyanaz, mint az **mkserver** esetén. **Megjegyzés:** A **dbpath** attribútum nem módosítható a **chserver** parancs használatával. Ez csak az **mkserver** parancs futtatásakor állítható be.
dbpath	Megadja a TNC adatbázis helyét. Az alapértelmezett érték /var/tnc.
delete	Töröl egy irányelvet vagy a kliensinformációkat.
export	Exportálja a TNC szerveren lévő kliens- vagy szervertanúsítványt, vagy adatbázist.
fspolicy	Megadja a TNC kliensek ellenőrzéséhez használt kiadás, technológia szint és javítócsomag fájlkészlet irányelvét.
import	Importál egy tanúsítványt a kliensen vagy a szerveren, vagy egy adatbázist a TNC szerveren.
ipgroup	Megadja az Internet protokoll (IP) csoportot, amely több kliens IP címet vagy hosztnevet tartalmaz.
list	Megjeleníti a TNC szerver, a TNC kliens vagy a SUMA információit.
log	Beállítja a TNC összetevők naplózási szintjét.
mkclient	Konfigurálja a TNC klienst.
mkipref	Konfigurálja a TNC IPRef összetevőt.
mkserver	Konfigurálja a TNC szervert.
pmport	Megadja a portszámot, amelyen a **pmserver** figyel. Az alapértelmezett érték 38240.
pmserver	Megadja a **suma** parancs hosztnevét vagy IP címét, amely az IBM® ECC webhelyen és az IBM Fix Central webhelyen elérhető legfrissebb javítócsomagokat és biztonsági javításokat tölti le.
recheck_interval	Megadja az időközt percekben vagy d (nap) : h (óra) : m (perc) formátumban a TNC szerver számára a TNC kliensek ellenőrzéséhez. **Megjegyzés:** A **recheck_interval=0** érték azt jelenti, hogy az ütemező nem kezdeményei rendszeres időközönként a kliensek ellenőrzését, és a regisztrált kliensek automatikusan lesznek érvényesítve az indítás során. Ilyen esetekben a kliens kézzel érvényesíthető.
report	Előállít egy .txt vagy .csv fájlkiterjesztéssel rendelkező jelentést.
restart	Újraindítja a TNC klienst, a TNC szervert vagy a TNC TNC IPRef összetevőt.
rmclient	Megszünteti a TNC kliens konfigurációját.
rmipref	Megszünteti a TNC IPRef összetevő konfigurációját.
rmserver	Megszünteti a TNC szerver konfigurációját.
start	Elindítja a TNC klienst, a TNC szervert vagy a TNC TNC IPRef összetevőt.
status	Megjeleníti a TNC konfiguráció állapotát.
stop	Leállítja a TNC klienst, a TNC szervert vagy a TNC TNC IPRef összetevőt.
tncport	Megadja a portszámot, amelyen a TNC szerver figyel. Az alapértelmezett érték 42830.

Elem	Leírás
tncserver	Megadja a TNC szervert, amely a TNC klienseket ellenőrzi vagy frissíti.
tssserver	Megadja a Trusted Surveyor szerver IP címét vagy hosztnevét.
update	Javításokat telepít a kliensen.
verify	A kliens kézi ellenőrzését kezdeményezi.

Kapcsolók

Elem	Leírás
-A <tanácsadó_neve>	Megadja a jelentéshez tartozó tanácsadó nevét.
-B <összeépítési_info>	Megadja az összeépítési információkat egy javítási jelentés előkészítéséhez.

-c	Megjeleníti a felhasználói attribútumokat pontosvesszővel elválasztott rekordokban, az alábbiak szerint:
	`# name: attribútum1: attribútum2: ...`
	`policy: érték1: érték2: ...`

-C	Megadja, hogy a művelet egy klienshez összetevőhöz tartozik.
-d *adatbázis_fájl_helye/ adatbázis_könyvtárútvonala*	Megadja a az adatbázis importálásának fájlútvonalát/megadja az adatbázis exportálásának könyvtárútvonalát.
-D *éééé-hh-nn*	Megadja egy adott kliens bejegyzés dátumát a napló előzményekben; *éééé* az év, *hh* a hónap, *nn* pedig a nap.
-e *email_azonosító* **ipgroup=**[**±**]*g1, g2...*	Megadja az e-mail azonosítót, amelyet egy vesszővel elválasztott IP csoportnévlista követ.
-E | FAIL | COMPLIANT | ALL |	Megadja az eseményt, amelyek esetén az e-maileket el kell küldeni a konfigurált e-mail azonosítóra. FAIL- Akkor küld leveleket, ha a kliens ellenőrzési állapota FAILED (meghiúsult). COMPLIANT- Akkor küld leveleket, ha a kliens ellenőrzési állapota COMPLIANT (megfelelő). ALL - A kliens ellenőrzésének minden állapotáról küld levelet.
-f *fájlnév*	Importálási művelet esetén megadja a fájlt, amelyből a tanúsítványt be kell olvasni, vagy exportálási művelet esetén megadja a helyet, ahová a tanúsítványt írni kell.
-F *fsirányelv_összeépítési_info*	Megadja a fájlrendszer irányelv nevét, amit az összeépítési információk követnek. Az összeépítési információk a következő formátumban adhatók meg: 6100-04-01, ahol 6100 a 6.1-es változatot ábrázolja, a 04 a karbantartási szintet, 01 pedig a javítócsomagot.
-G *ip_csoport_neve* **ip=**[**±**]*ip1, ip2...*	Megadja az IP csoport nevét, utána pedig egy vesszővel elválasztott IP listát.
-H	Felsorolja a történetnaplót.
-i *hoszt*	Megadja az IP címet vagy hosztnevet.
-I ip=[**±**]*ip1, ip2...* | [±] hoszt1,hoszt2...	Megadja az ellenőrzés során mellőzendő IP címeket/hosztneveket.
-k *fájlnév*	Megadja a fájlt, amelyből a tanúsítványkulcsot egy importálási művelet során be kell olvasni.
-p	Megjeleníti a TNC kliens frissítésének előképét.
-P <irányelvnév>	Megadja az irányelv nevét egy kliens irányelv jelentés előkészítéséhez.
-q	Kikapcsolja a fejlécinformációkat.
-r *összeépítési_információk*	Előállítja a jelentést az összeépítési információk alapján. Az összeépítési információk a következő formátumban adhatók meg: 6100-04-01, ahol 6100 a 6.1-es változatot ábrázolja, a 04 a karbantartási szintet, 01 pedig a javítócsomagot.
-R	Megadja, hogy a művelet egy IPRef összetevőhöz tartozik.
-s COMPLIANT | IGNORE | FAILED | ALL	A kliens állapotát jeleníti meg az alábbiak szerint: **COMPLIANT** Az aktív klienseket jeleníti meg. **IGNORE** A mindenfajta ellenőrzésből kizárt klienseket jeleníti meg. **FAILED** Azokat a klienseket jeleníti meg, melyek ellenőrzése a konfigurált irányelvet illetően meghiúsult. **ALL** Az összes klienst jeleníti meg, tekintet nélkül azok állapotára.
-S <hoszt>	Megadja a hosztnevet egy kliens biztonsági javítás jelentés előkészítéshez.
-t TRUSTED | UNTRUSTED	Megbízhatóként vagy megbízhatatlanként jelöli meg a megadott klienst. **Megjegyzés:** Csak rendszeradminisztrátorok igazolhatják a szervert vagy klienst megbízhatóként vagy megbízhatatlanként.

Elem	Leírás
-T	Megadja, hogy a kliens elfogadhat-e kéréseket bármely, érvényes tanúsítvánnyal rendelkező TS szerverről.
-u	Eltávolítja a TNC kliensen telepített köztes javítást.
-v	Megadja a köztes javítások vesszővel elválasztott listáját.
-V	Megadja a köztes javítás csoport nevét.

Kilépési állapot

Ez a parancs a következő kilépési értékeket adja vissza:

Elem	Leírás
0	A parancs sikeresen lefutott, és minden kért módosítás megtörtént.
>0	Hiba történt. A kiírt hibaüzenet további részleteket biztosít a hiba típusáról.

Példák

1. A TNC szerver elindításához írja be a következő parancsot:
   ```
   psconf start server
   ```
2. Egy 71D_latest nevű fájlrendszer irányelv hozzáadásához a 7100-04-02 összeépítéshez, írja be a következő parancsot:
   ```
   psconf add -F 71D_latest 7100-04-02
   ```
3. Egy 71D_old nevű fájlrendszer irányelv törléséhez írja be a következő parancsot:
   ```
   psconf delete -F 71D_old
   ```
4. Annak ellenőrzéséhez, hogy a 11.11.11.11 IP címmel rendelkező kliens **megbízható**-e írja be a következő parancsot:
   ```
   psconf certadd -i 11.11.11.11 -t TRUSTED
   ```
5. A 11.11.11.11 IP címmel rendelkező kliens törléséhez a szerverről, írja be a következő parancsot:
   ```
   psconf certdel -i 11.11.11.11
   ```
6. A 11.11.11.11 IP címmel rendelkező kliens információinak ellenőrzéséhez írja be a következő parancsot:
   ```
   psconf verify -i 11.11.11.11
   ```
7. A 11.11.11.11 IP címmel rendelkező kliens információinak megjelenítéséhez írja be a következő parancsot:
   ```
   psconf list -i 11.11.11.11
   ```
8. A **COMPLAINT** (megfelel) állapotban lévő kliensekre vonatkozó jelentés előállításához írja be a következő parancsot:
   ```
   psconf list -s CPMPLIANT -i ALL
   ```
9. A 7100-04-02 összeépítésre vonatkozó jelentés előállításához írja be a következő parancsot:
   ```
   psconf list -r 7100-04-02
   ```
10. A 11.11.11.11 IP címmel rendelkező kliens csatlakozási előzményeinek megjelenítéséhez írja be a következő parancsot:
    ```
    psconf list -H -i 11.11.11.11
    ```
11. A 11.11.11.11 IP címmel rendelkező kliens bejegyzésének törléséhez a 2009. február 1-i vagy ennél régebbi naplóelőzményekből, írja be a következő parancsot:
    ```
    psconf delete -H -i 11.11.11.11 -D 2009-02-01
    ```
12. A 11.11.11.11 IP címmel rendelkező kliens klienstanúsítványának importálásához a szerverről, írja be a következő parancsot:
    ```
    psconf import -C -i 11.11.11.11 -f /tmp/client.txt
    ```
13. A szervertanúsítvány exportálásához egy kliensből, adja ki a következő parancsot:
    ```
    psconf export -S -f /tmp/server.txt
    ```
14. A 11.11.11.11 IP címmel rendelkező kliens frissítéséhez egy megfelelő szintre a szerverről, írja be a következő parancsot:

```
psconf update -i 11.11.11.11
```

15. A kliensállapotok megjelenítéséhez írja be a következő parancsot:
```
psconf status
```
16. A klienstanúsítványok megjelenítéséhez írja be a következő parancsot:
```
psconf list -C
```
17. A kliens indításához írja be a következő parancsot:
```
psconf start client
```

Biztonság

RBAC felhasználók és Megbízható AIX felhasználók figyelmébe:

A parancs privilegizált műveleteket is végrehajthat. A privilegizált műveleteket csak a megfelelő jogosultságokkal rendelkező felhasználók futtathatják. A jogosultságokról és privilégiumokról további információkat a Biztonság című rész Privilegizált parancsok adatbázisa szakaszában talál. A parancsra vonatkozó privilégiumok és jogosultságok listáját az **lssecattr** parancsnál vagy a **getcmdattr** alparancsnál találja

rmvfilt parancs

Cél

Eltávolítja a virtuális LAN kereszteződési szűrőszabályokat a szűrőtáblázatból.

Szintaxis

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

Leírás

Az **rmvfilt** parancs arra szolgál, hogy eltávolítsa a virtuális LAN kereszteződési szűrőszabályokat a szűrő táblából.

Kapcsolók

-n Megadja az eltávolítandó szűrőszabály azonosítóját. Az **all** paraméter használatával az összes szűrőszabály eltávolítható.

Kilépési állapot

Ez a parancs a következő kilépési értékeket adja vissza:

0 Sikeres befejeződés.

>0 Hiba történt.

Példák

1. Az összes szűrőszabály eltávolításához, vagy a kernelben lévő összes szűrőszabály deaktiválásához írja be a parancsot a következők szerint:
```
rmvfilt -n all
```

Kapcsolódó fogalmak:

“Szabályok deaktiválása” oldalszám: 16
A Megbízható tűzfal szolgáltatásban a VLAN hálózatok közötti továbbítást engedélyező szabályok deaktiválhatók.

vlantfw parancs

Cél

Megjeleníti vagy törli az IP és Adathordozó hozzáférés-felügyelet (MAC) leképezési információkat, és vezérli a naplózási funkciót.

Szintaxis

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

Leírás

A **vlantfw** parancs megjeleníti vagy törli az IP és MAC leképezési bejegyzéseket. Biztosítja továbbá a Megbízható tűzfal szolgáltatás elindításának vagy leállításának képességét.

Kapcsolók

-d Megjeleníti az összes IP leképezési információt.

-D Megjeleníti az összegyűjtött kapcsolatadatokat.

-E Megjeleníti a logikai partíciók (LPAR) közötti kapcsolatadatokat a különböző központi feldolgozó komplexumokhoz.

-f Eltávolítja az összes IP leképezési információt.

-F Kiüríti a kapcsolatadatok gyorsítótárát.

-G Megjeleníti a szűrőszabályokat, amelyek beállíthatók úgy, hogy a forgalom belsőleg, a Megbízható tűzfal szolgáltatás használatával legyen továbbítva.

-I Megjeleníti az azonos központi feldolgozó komplexumokhoz tartozó, de különböző VLAN azonosítókkal társított logikai partíciók közötti kapcsolatadatokat.

-l Elindítja a Megbízható tűzfal naplózási szolgáltatást.

-L Leállítja a Megbízható tűzfal naplózási szolgáltatást, és átirányítja a nyomkövetési fájlok tartalmát a /home/padmin/svm/svm.log fájlba.

-m Engedélyezi a Megbízható tűzfal megfigyelést.

-M Letiltja a Megbízható tűzfal megfigyelést.

-q Lekérdezi a biztonságos virtuális gép állapotot.

-s Elindítja a Megbízható tűzfal szolgáltatást.

-t Leállítja a Megbízható tűzfal szolgáltatást.

Paraméterek

-N *egész_szám*
Megjeleníti a megadott egész számnak megfelelő szűrőszabályt.

Kilépési állapot

Ez a parancs a következő kilépési értékeket adja vissza:

0 Sikeres befejeződés.

>0 Hiba történt.

Példák

1. Az összes IP leképezés megjelenítéséhez adja ki a parancsot a következők szerint:
   ```
   vlantfw -d
   ```
2. Az összes IP leképezés eltávolításához adja ki a parancsot a következők szerint:
   ```
   vlantfw -f
   ```
3. A Megbízható tűzfal naplózási funkció elindításához adja ki a parancsot a következők szerint:
   ```
   vlantfw -l
   ```
4. Egy biztonságos virtuális gép állapotának ellenőrzéséhez adja ki a parancsot a következők szerint:
   ```
   vlantfw -q
   ```
5. A Megbízható tűzfal elindításához adja ki a parancsot a következők szerint:
   ```
   vlantfw -s
   ```
6. A Megbízható tűzfal leállításához adja ki a parancsot a következők szerint:
   ```
   vlantfw -t
   ```
7. A forgalmat a központi feldolgozó komplexumon belül továbbító szűrők előállításához használható megfelelő szabályok megjelenítéséhez adja ki a parancsot a következők szerint:
   ```
   vlantfw -G
   ```

Kapcsolódó hivatkozás:

“genvfilt parancs” oldalszám: 32

Nyilatkozatok

Ezek az információk az Egyesült Államokban forgalmazott termékekre és szolgáltatásokra vonatkoznak.

Elképzelhető, hogy a dokumentumban szereplő termékeket, szolgáltatásokat vagy lehetőségeket az IBM más országokban nem forgalmazza. Az adott országokban rendelkezésre álló termékekről és szolgáltatásokról a helyi IBM képviseletek szolgálnak felvilágosítással. Az IBM termékekre, programokra vagy szolgáltatásokra vonatkozó hivatkozások sem állítani, sem sugallni nem kívánják, hogy az adott helyzetben csak az IBM termékeit, programjait vagy szolgáltatásait lehet alkalmazni. Minden olyan működésében azonos termék, program vagy szolgáltatás alkalmazható, amely nem sérti az IBM szellemi tulajdonjogát. A nem IBM termékek, programok és szolgáltatások működésének megítélése és ellenőrzése természetesen a felhasználó felelőssége.

A dokumentum tartalmával kapcsolatban az IBM-nek bejegyzett vagy bejegyzés alatt álló szabadalmai lehetnek. Jelen dokumentum nem ad semmiféle jogos licencet ezen szabadalmakhoz. A licenckérelmeket írásban a következő címre küldheti:

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

Ha duplabyte-os (DBCS) információkkal kapcsolatban van szüksége licencre, akkor lépjen kapcsolatban az országában az IBM szellemi tulajdon osztállyal, vagy írjon a következő címre:

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

A következő bekezdés nem vonatkozik az Egyesült Királyságra, valamint azokra az országokra, amelyeknek jogi szabályozása ellentétes a bekezdés tartalmával: AZ INTERNATIONAL BUSINESS MACHINES CORPORATION AZ INFORMÁCIÓKAT "JELENLEGI ÁLLAPOTUKBAN", BÁRMIFÉLE KIFEJEZETT VAGY VÉLELMEZETT GARANCIA NÉLKÜL ADJA KÖZRE, IDEÉRTVE, DE NEM KIZÁRÓLAG A JOGSÉRTÉS KIZÁRÁSÁRA, A KERESKEDELMI ÉRTÉKESÍTHETŐSÉGRE ÉS BIZONYOS CÉLRA VALÓ ALKALMASSÁGRA VONATKOZÓ VÉLELMEZETT GARANCIÁT. Bizonyos államok nem engedélyezik egyes tranzakciók kifejezett vagy vélelmezett garanciáinak kizárását, így elképzelhető, hogy az előző bekezdés Önre nem vonatkozik.

Jelen dokumentum tartalmazhat technikai, illetve szerkesztési hibákat. Az itt található információk bizonyos időnként módosításra kerülnek; a módosításokat a kiadvány új kiadásai tartalmazzák. Az IBM mindennemű értesítés nélkül fejlesztheti és/vagy módosíthatja a kiadványban tárgyalt termékeket és/vagy programokat.

A kiadványban a nem IBM webhelyek megjelenése csak kényelmi célokat szolgál, és semmilyen módon nem jelenti ezen webhelyek előnyben részesítését másokhoz képest. Az ilyen webhelyeken található anyagok nem képezik az adott IBM termék dokumentációjának részét, így ezek használata csak saját felelősségre történhet.

IBM belátása szerint bármilyen formában felhasználhatja és továbbadhatja a felhasználóktól származó adatokat anélkül, hogy ebből a felhasználók felé bármilyen kötelezettsége származna.

A programlicenc azon birtokosainak, akik információkat kívánnak szerezni a programról (i) a függetlenül létrehozott programok vagy más programok (beleértve ezt a programot is) közti információcseréhez, illetve (ii) a kicserélt

információk kölcsönös használatához, fel kell venniük a kapcsolatot az alábbi címmel:

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

Az ilyen információk bizonyos feltételek és kikötések mellett állnak rendelkezésre, ideértve azokat az eseteket is, amikor ez díjfizetéssel jár.

Az IBM a dokumentumban tárgyalt licencprogramokat és a hozzájuk kapcsolódó licenc anyagokat IBM Vásárlói megállapodás, IBM Nemzetközi programlicenc szerződés vagy a felek azonos tartalmú megállapodása alapján biztosítja.

A dokumentumban található teljesítményadatok ellenőrzött környezetben kerültek meghatározásra. Ennek következtében a más működési körülmények között kapott adatok jelentősen különbözhetnek a dokumentumban megadottaktól. Egyes mérések fejlesztői szintű rendszereken kerültek végrehajtásra, így nincs garancia arra, hogy ezek a mérések azonosak az általánosan hozzáférhető rendszerek esetében is. Továbbá bizonyos mérések következtetés útján kerültek becslésre. A tényleges eredmények különbözhetnek. A dokumentum felhasználóinak ellenőrizni kell az adatok alkalmazhatóságát az adott környezetben.

A nem IBM termékekre vonatkozó információk a termékek szállítóitól, illetve azok publikált dokumentációiból, valamint egyéb nyilvánosan hozzáférhető forrásokból származnak. Az IBM nem tesztelte ezeket a termékeket, így az IBM a nem IBM termékek esetében nem tudja megerősíteni a teljesítményre és kompatibilitásra vonatkozó, valamint az egyéb állítások pontosságát. A nem IBM termékekkel kapcsolatos kérdéseivel forduljon az adott termék szállítóihoz.

Az IBM jövőbeli tevékenységére vagy szándékaira vonatkozó állításokat az IBM mindennemű értesítés nélkül módosíthatja vagy visszavonhatja, azok csak célokat jelentenek.

A feltüntetett árak az IBM által javasolt aktuális kiskereskedelmi árak, és ezek értesítés nélkül változhatnak. Az egyes forgalmazók árai eltérhetnek.

Ezek az információk csak tervezési célt szolgálnak. Az itt közölt információk változhatnak a leírt termékek elérhetővé válása előtt.

Az információk között példaként napi üzleti tevékenységekhez kapcsolódó jelentések és adatok lehetnek. A valóságot a lehető legjobban megközelítő illusztráláshoz a példákban egyének, vállalatok, márkák és termékek nevei szerepelnek. Minden ilyen név a képzelet szüleménye, és valódi üzleti vállalkozások neveivel és címeivel való bármilyen hasonlóságuk teljes egészében a véletlen műve.

SZERZŐI JOGI LICENC:

Jelen kiadvány forrásnyelvi minta alkalmazásokat tartalmaz, amelyek a programozási technikák bemutatására szolgálnak a különböző működési környezetekben. A példaprogramokat tetszőleges formában, az IBM-nek való díjfizetés nélkül másolhatja, módosíthatja és terjesztheti fejlesztési, használati, marketing célból, illetve olyan alkalmazási programok terjesztése céljából, amelyek megfelelnek azon operációs rendszer alkalmazásprogram illesztőjének, ahol a példaprogramot írta. Ezek a példák nem kerültek minden körülmények között alapos tesztelésre. Az IBM így nem tudja garantálni a megbízhatóságukat, javíthatóságukat, de még a programok funkcióit sem. A mintaprogramok "ÖNMAGUKBAN", mindenféle garancia nélkül állnak rendelkezésre. Az IBM nem felelős a mintaprogramok használatából eredő esetleges károkért.

E mintaprogramok minden másolatának vagy részének, illetve minden származtatott munkának tartalmaznia kell a következő jogi nyilatkozatot:

© (cégnév) (évszám). A kód bizonyos részei az IBM Corp. példaprogramjaiból származnak. © Copyright IBM Corp. (évszám vagy évszámok).

Elképzelhető, hogy a dokumentum elektronikus példányaiban a fotók és a színes ábrák nem jelennek meg.

Adatvédelmi irányelv szempontok

Az IBM szoftvertermékek, a szolgáltatási megoldásként használt szoftvereket (“Szoftver termékajánlatok”) is beleértve, cookie-k és más technológiák használatával begyűjthetik a termék használatával kapcsolatos információkat, aminek célja a végfelhasználói élmény tökéletesítése, a végfelhasználókkal folytatott együttműködés személyre szabása, stb. A Szoftver termékajánlatok a legtöbb esetben nem gyűjtenek személyesen azonosítható információkat. Néhány Szoftver termékajánlatunk segíthet személyesen azonosítható információk begyűjtésének engedélyezésében. Ha az adott Szoftver termékajánlat a személyesen azonosítható információk gyűjtéséhez cookie-kat használ, akkor a termékajánlat cookie használatára vonatkozó információkat az alábbiakban megtalálja.

Ez a Szoftver termékajánlat nem használ cookie-kat vagy más technológiákat személyes azonosításra alkalmas információk összegyűjtéséhez.

Ha a Szoftver termékajánlat telepített konfigurációi Önnek, mint ügyfélnek biztosítják azt a képességet, hogy személyesen azonosítható információkat gyűjtsön be a végfelhasználóktól cookie-kon és egyéb technológiákon keresztül, akkor Önnek kell az ilyen adatgyűjtésre vonatkozó törvényi szabályozással kapcsolatos információkat beszereznie, beleértve a nyilatkozatokkal és hozzájárulásokkal kapcsolatos követelményeket is.

A különféle technológiák (a cookie-kat is beleértve) ilyen célra való felhasználásával kapcsolatos további információkat a következő helyeken talál: IBM online adatvédelmi tájékoztató - kivonat (http://www.ibm.com/privacy) és IBM online adatvédelmi tájékoztató (http://www.ibm.com/privacy/details), valamint a “Cookies, Web Beacons and Other Technologies” és az “IBM Software Products and Software-as-a-Service Privacy Statement” részek a http://www.ibm.com/software/info/product-privacy webhelyen.

Védjegyek

Az IBM, az IBM logó és az ibm.com az International Business Machines Corp védjegye vagy bejegyzett védjegye a világ számos országában. Más termékek és szolgáltatások nevei az IBM vagy más cégek védjegyei lehetnek. Az IBM védjegyek aktuális listája a Copyright and trademark information weboldalon érhető el az alábbi címen: www.ibm.com/legal/copytrade.shtml.

A Linux Linus Torvalds bejegyzett védjegye az Egyesült Államokban és/vagy más országokban.

A Java és minden Java alapú védjegy és logó az Oracle és/vagy társvállalatai védjegye vagy bejegyzett védjegye.

Tárgymutató

R

S

SZ

T

V

Nyomtatva Dániában