IBM PowerSC

Standard Edition

เวอร์ชัน 1.1.3

PowerSC Standard Edition

IBM PowerSC

Standard Edition

เวอร์ชัน 1.1.3

PowerSC Standard Edition

หมายเหตุ

ก่อนการใช้ข้อมูลนี้และผลิตภัณฑ์ที่ข้อมูลนี้สนับสนุน โปรดอ่าน ข้อมูลใน “คำประกาศ” ในหน้า 53

เอดิชันนี้จะใช้กับ IBM PowerSC เวอร์ชัน 1.1.3 และ การแก้ไข และรีลีสต่อมาทั้งหมดจนกว่าจะมีการระบุไว้เป็นอย่างอื่น ในเอดิชันใหม่

สารบัญ

เกี่ยวกับเอกสารนี้

เอกสารนี้จะมีผู้ดูแลระบบที่มีข้อมูลที่สมบูรณ์ เกี่ยวกับไฟล์ ระบบ และการรักษาความปลอดภัยเครือข่าย

การไฮไลต์

มีการใช้แบบแผน การไฮไลต์ต่อไปนี้ในเอกสารนี้:

ตัวหนา	ระบุคำสั่ง รูทีนย่อย คีย์เวิร์ด ไฟล์ โครงสร้าง ไดเร็กทอรี และไอเท็มอื่นที่มีชื่อซึ่งระบบกำหนดไว้ล่วงหน้า นอกจากนี้ ยังระบุอ็อบเจ็กต์แบบกราฟิก เช่น ปุ่ม เลเบล และไอคอนที่ผู้ใช้เลือก
ตัวเอียง	ระบุพารามิเตอร์ที่ชื่อจริง หรือค่าจะมีการระบุโดยผู้ใช้
`ช่องว่างเดียว`	ระบุตัวอย่างของค่าข้อมูลเฉพาะ ตัวอย่างของข้อความที่คล้ายกับที่คุณอาจเห็นแสดงขึ้น ตัวอย่าง ของส่วนของโปรแกรมโค้ดที่คล้ายกับที่คุณอาจเขียนในฐานะโปรแกรมเมอร์ ข้อความจากระบบ หรือข้อมูลที่คุณควรจะพิมพ์จริง

การตรงตามตัวพิมพ์ใน AIX®

ทุกสิ่งในระบบปฏิบัติการ AIX เป็นแบบตรงตามตัวพิมพ์ ซึ่งหมายความว่ามีการแยกความแตกต่าง ระหว่างตัวอักษรพิมพ์ใหญ่และพิมพ์เล็ก ตัวอย่างเช่น คุณสามารถใช้คำสั่ง **ls** เพื่อแสดงรายการไฟล์ หากคุณพิมพ์ `LS` ระบบจะตอบกลับ คำสั่งนั้นว่า `not found` ในลักษณะคล้ายกัน `FILEA`, `FiLea` และ `filea` คือชื่อไฟล์สามชื่อที่แตกต่างกัน แม้ว่า ไฟล์เหล่านั้นอยู่ในไดเร็กทอรีเดียวกัน เพื่อหลีกเลี่ยงการทำแอ็คชันที่ ไม่ต้องการ ควรตรวจสอบให้แน่ใจเสมอว่าคุณใช้ตัวพิมพ์ที่ถูกต้อง

ISO 9000

ระบบรับรองคุณภาพที่ลงทะเบียน ISO 9000 ใช้ในการพัฒนาและการผลิตผลิตภัณฑ์นี้

IBM PowerSC Standard Edition 1.1.3

IBM® PowerSC™ Standard Editionจะมี คุณลักษณะ Trusted Boot, Trusted Firewall, Trusted Logging, Trusted Network Connect and Patch management และ Security and Compliance Automation

มีอะไรใหม่ใน PowerSC Standard Edition 1.1.3

อ่านเกี่ยวกับข้อมูลใหม่หรือข้อมูลสำคัญที่มีการเปลี่ยนแปลงสำหรับ ชุดหัวข้อ PowerSC Standard Edition เวอร์ชัน 1.1.3

ในไฟล์ PDF นี้ คุณอาจเห็นแถบ การแก้ไข (|) ในขอบด้านซ้ายที่ระบุข้อมูลใหม่ และข้อมูลที่เปลี่ยนแปลง

ธันวาคม 2013

- อัพเดตข้อกำหนดของระบบใน "แนวคิด PowerSC Standard Edition 1.1.3" ในหน้า 2
- ระบุการเปลี่ยนไฟล์ Trusted Boot ที่จำเป็นเมื่อคุณติดตั้ง ระบบปฏิบัติการ AIX ใหม่อีกครั้งใน "ข้อกำหนดเบื้องต้นของ Trusted Boot" ในหน้า 5
- เพิ่มข้อมูลเกี่ยวกับฟังก์ชันการมอนิเตอร์ Trusted Firewall ใน "การมอนิเตอร์ Trusted Firewall" ในหน้า 14
- เพิ่มข้อมูลเกี่ยวกับฟังก์ชันการบันทึก Trusted Firewall ใน "การบันทึกล็อก Trusted Firewall" ในหน้า 14
- เพิ่มหัวข้อ "การติดตั้ง Trusted Logging" ในหน้า 20
- เพิ่มข้อมูลเกี่ยวกับการอัพเดตโปรแกรมแก้ไขปัญหาระหว่างเวอร์ชันสำหรับ Trusted Network Connect ใน "การกำหนดค่าคอนฟิกเซิร์ฟเวอร์การจัดการแพทช์" ในหน้า 27
- เพิ่มข้อมูลเกี่ยวกับการสร้างรายงานของเซิร์ฟเวอร์ Trusted Network Connect ใน "การสร้างรายงานของเซิร์ฟเวอร์ TNC" ในหน้า 34
- เพิ่มข้อมูลเกี่ยวกับการติดตั้งตัวตรวจสอบ Trusted Network Connect ใน "การติดตั้งตัวตรวจสอบ" ในหน้า 7
- เพิ่มคำสั่ง Trusted Firewall ใน "คำสั่ง PowerSC Standard Edition" ในหน้า 35
- เปลี่ยนชื่อคำสั่ง **tscpmconsole** เป็นคำสั่ง **pmconf** และเพิ่มข้อมูลใน "คำสั่ง pmconf" ในหน้า 40
- เปลี่ยนชื่อคำสั่ง **tscconsole** เป็นคำสั่ง **psconf** และเพิ่มข้อมูลใน "คำสั่ง psconf" ในหน้า 44
- อัพเดตข้อมูลเกี่ยวกับอ็อพชันสำหรับคำสั่ง **vlantfw** ใน "คำสั่ง vlantfw" ในหน้า 51

พฤศจิกายน 2012

อัพเดตข้อมูลในหัวข้อ "การจัดการ Trusted Network Connect และ Patch" ในหน้า 23

พฤษภาคม 2012

เพิ่มเอกสารสำหรับ คุณลักษณะใหม่สำหรับ "Trusted Firewall" ในหน้า 11

แนวคิด PowerSC Standard Edition 1.1.3

ภาพรวมนี้ของ PowerSC Standard Edition จะอธิบาย คุณลักษณะ คอมโพเนนต์ และการสนับสนุนทางฮาร์ดแวร์ที่เกี่ยวข้องกับคุณลักษณะ PowerSC Standard Edition

PowerSC Standard Edition จะมี การรักษาความปลอดภัย และการควบคุมของระบบปฏิบัติการภายในคลาวด์ หรือใน ศูนย์ข้อมูลเสมือน และมีมุมมององค์กร และความสามารถ ในการจัดการ PowerSC Standard Edition เป็นชุดของคุณลักษณะที่มี Security and Compliance Automation, Trusted Boot, Trusted Firewall, Trusted Logging และการจัดการ Trusted Network Connect และ Patch เทคโนโลยีการรักษาความปลอดภัยที่ วางอยู่ภายในเลเยอร์เสมือนจะมีการรักษาความปลอดภัยเพิ่มเติมในระบบแบบสแตนอะโลน

ตารางต่อไปนี้จะมีรายละเอียดเกี่ยวกับเอดิชัน คุณลักษณะ ที่มีอยู่ในเอดิชัน คอมโพเนนต์ และฮาร์ดแวร์ของ ตัวประมวลผลที่ซึ่งแต่ละคอมโพเนนต์มีอยู่

ตารางที่ 1. คอมโพเนนต์ PowerSC Standard Edition , คำอธิบาย , การสนับสนุนของระบบปฏิบัติการ และการสนับสนุนทางฮาร์ดแวร์

คอมโพเนนต์	คำอธิบาย	ระบบปฏิบัติการที่สนับสนุน	ฮาร์ดแวร์ที่สนับสนุน
Security and Compliance Automation	การตั้งค่าโดยอัตโนมัติ, การมอนิเตอร์ และการตรวจสอบ คอนฟิกูเรชันของการรักษาความปลอดภัย และการปฏิบัติตามข้อบังคับสำหรับมาตรฐานต่อไปนี้: • Payment Card Industry Data Security Standard (PCI DSS) • มาตรฐาน Sarbanes-Oxley Act และ COBIT (SOX/COBIT) • U.S. Department of Defense (DoD) STIG • Health Insurance Portability and Accountability Act (HIPAA)	• AIX 5.3 • AIX 6.1 • AIX 7.1	• POWER5 • POWER6® • POWER7®
Trusted Boot	วัดค่าอิมเมจการบูต, ระบบปฏิบัติการ และ แอ็พพลิเคชัน และยืนยันความไว้วางใจโดยการใช้เทคโนโลยี Virtual Trusted Platform Module (TPM)	• AIX 6 ที่มี 6100-07 หรือใหม่กว่า • AIX 7 ที่มี 7100-01 หรือใหม่กว่า	POWER7 เฟิร์มแวร์ eFW7.4 หรือใหม่กว่า
Trusted Firewall	ประหยัดเวลา และทรัพยากรโดยการเปิดใช้การกำหนดเส้นทางโดยตรงระหว่าง Virtual LANs (VLANs) ที่ระบุที่ถูกควบคุม โดย Virtual I/O Server เดียวกัน	• AIX 6.1 • AIX 7.1 • VIOS เวอร์ชัน 2.2.1.4 หรือใหม่กว่า	• POWER6 • POWER7 • Virtual I/O Server เวอร์ชัน 6.1S หรือใหม่กว่า
Trusted Logging	ล็อกของ AIX ในปัจจุบันจะอยู่บน Virtual I/O Server (VIOS) ในแบบเรียลไทม์ คุณลักษณะนี้จะมีการบันทึกแบบ Tamper Proof และมีการจัดการและการแบ็กอัพล็อกที่สะดวก	• AIX 5.3 • AIX 6.1 • AIX 7.1	• POWER5 • POWER6 • POWER7

ตารางที่ 1. คอมโพเนนต์ PowerSC Standard Edition , คำอธิบาย , การสนับสนุนของระบบปฏิบัติการ และการสนับสนุนทางฮาร์ดแวร์ (ต่อ)

คอมโพเนนต์	คำอธิบาย	ระบบปฏิบัติการที่สนับสนุน	ฮาร์ดแวร์ที่สนับสนุน
การจัดการ Trusted Network Connect และแพตช์	ตรวจสอบว่าระบบ AIX ทั้งหมดในสภาพแวดล้อมเสมือนจะอยู่ที ซอฟต์แวร์ ที่ระบุ และระดับแพตช์ และมีเครื่องมือการจัดการเพื่อให้แน่ใจว่า ระบบ AIX ทั้งหมดจะอยู่ที่ระดับซอฟต์แวร์ ที่ระบุ มีการแจ้งเตือนหากมีการเพิ่มระบบเสมือนระดับล่าง ไปยังเครือข่าย หรือหากแพ็กทช์การรักษาความปลอดภัยที่ส่งออกมามีผลกระทบ กับระบบ	• AIX 5.3 • AIX 6.1 • AIX 7.1 ไคลเอ็นต์ Trusted Network Connect ต้องการ หนึ่งในคอมโพเนนต์ต่อไปนี้: • AIX 6.1 ที่มี 6100-06 หรือ ใหม่กว่า • ระบบคอนโซล AIX เวอร์ชัน 7.1 Service Update Management Assistant (SUMA) ภายในสภาพแวดล้อม SUMA สำหรับการจัดการแพตช์	• POWER5 • POWER6 • POWER7

การติดตั้ง PowerSC Standard Edition 1.1.3

คุณต้องติดตั้ง fileset สำหรับแต่ละฟังก์ชันเฉพาะของ PowerSC Standard Edition

filesets ต่อไปนี้จะสามารถใช้ได้สำหรับ PowerSC Standard Edition:

- `powerscExp.ice`: ติดตั้งบนระบบ AIX ที่ต้องการคุณลักษณะ Security and Compliance Automation ของ PowerSC Standard Edition
- `powerscStd.vtpm`: ติดตั้งบนระบบ AIX ที่ต้องการคุณลักษณะ Trusted Boot ของ PowerSC Standard Edition
- `powerscStd.vlog`: ติดตั้งบนระบบ AIX ที่ต้องการคุณลักษณะ Trusted Logging ของ PowerSC Standard Edition
- `powerscStd.tnc_pm`: ติดตั้ง บน AIX เวอร์ชัน 6.1 ที่มีระดับเทคโนโลยี 6100-06 หรือสูงกว่า หรือบนระบบคอนโซล AIX เวอร์ชัน 7.1 Service Update Management Assistant (SUMA) ภายในสภาพแวดล้อม SUMA สำหรับการจัดการแพตช์
- `powerscStd.svm`: ติดตั้งบนระบบ AIX ที่อาจเป็นประโยชน์จากการเรียกใช้ คุณลักษณะของ PowerSC Standard Edition

ติดตั้ง PowerSC Standard Edition โดยใช้หนึ่งในอินเตอร์เฟสต่อไปนี้:

- คำสั่ง **installp** จากอินเตอร์เฟส บรรทัดคำสั่ง (CLI)
- อินเตอร์เฟส SMIT

เพื่อติดตั้ง PowerSC Standard Edition โดยใช้อินเตอร์เฟส SMIT ให้ดำเนินการขั้นตอนต่อไปนี้:

1. รันคำสั่งต่อไปนี้:

   ```
   % smitty installp
   ```

2. เลือกอ็อพชัน **Install Software**

3. เลือกไดเร็กทอรี หรืออุปกรณ์อินพุทสำหรับซอฟต์แวร์เพื่อระบุ ตำแหน่งและไฟล์ติดตั้งของอิมเมจการติดตั้ง IBM Compliance Expert ตัวอย่างเช่น หากอิมเมจการติดตั้งมีพาธไดเร็กทอรี และชื่อไฟล์ `/usr/sys/inst.images/powerscStd.vtpm` คุณต้องระบุพาธไฟล์ในฟิลด์ **INPUT**
4. ดูและยอมรับข้อการตกลงการใช้ซอฟต์แวร์ ยอมรับข้อตกลงการใช้ซอฟต์แวร์โดยใช้ลูกศรชี้ลงเพื่อเลือก **ACCEPT new license agreements** และกดคีย์ Tab เพื่อเปลี่ยนค่าเป็น **Yes**
5. กด **Enter** เพื่อเริ่มต้นการติดตั้ง
6. ตรวจสอบว่าสถานะคำสั่งคือ **OK** หลังจากการติดตั้ง เสร็จสมบูรณ์

การดูไลเซนส์ซอฟต์แวร์

ไลเซนส์ของซอฟต์แวร์สามารถดูได้ใน CLI โดยใช้คำสั่ง ต่อไปนี้:

```
% installp -lE -d path/filename
```

โดย *path/filename* จะระบุอิมเมจการติดตั้ง PowerSC Standard Edition

ตัวอย่างเช่น คุณสามารถป้อนคำสั่งต่อไปนี้โดยใช้ CLI เพื่อระบุข้อมูลไลเซนส์ที่เกี่ยวข้องกับ PowerSC Standard Edition:

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

หลักการที่เกี่ยวข้อง:

"แนวคิด PowerSC Standard Edition 1.1.3" ในหน้า 2
ภาพรวมนี้ของ PowerSC Standard Edition จะอธิบาย คุณลักษณะ คอมโพเนนต์ และการสนับสนุนทางฮาร์ดแวร์ที่เกี่ยวข้องกับคุณลักษณะ PowerSC Standard Edition

"การติดตั้ง Trusted Boot" ในหน้า 7
มีการกำหนดค่าคอนฟิกทางฮาร์ดแวร์และซอฟต์แวร์บางอย่าง ที่จำเป็นในการติดตั้ง Trusted Boot

"การติดตั้ง Trusted Network Connect" ในหน้า 25
การติดตั้งคอมโพเนนต์ของ Trusted Network Connect (TNC) ต้องการให้คุณดำเนินการบางขั้นตอน

งานที่เกี่ยวข้อง:

"การติดตั้ง Trusted Firewall" ในหน้า 13
การติดตั้ง PowerSC Trusted Firewall จะคล้ายกับการติดตั้งคุณลักษณะ PowerSC อื่นๆ

"การติดตั้ง Trusted Logging" ในหน้า 20
คุณสามารถติดตั้งคุณลักษณะ PowerSC Trusted Logging โดยใช้อินเตอร์เฟสบรรทัดคำสั่ง หรือเครื่องมือ SMIT

Trusted Boot

คุณลักษณะ Trusted Boot จะใช้ Virtual Trusted Platform Module (VTPM) ซึ่งเป็นอินสแตนซ์เสมือนของ TPM ของ Trusted Computing Group VTPM จะถูกใช้เพื่อจัดเก็บการตรวจวัดของ การบูตระบบสำหรับการตรวจสอบในอนาคตอย่างปลอดภัย

แนวคิด Trusted Boot

เป็นสิ่งสำคัญที่ต้องเข้าใจบูรณภาพของกระบวนการ บูต และวิธีในการแบ่งแยกบูตเป็นการบูตที่ไว้วางใจได้ และการบูต ที่ไม่ไว้วางใจ

คุณสามารถกำหนดค่าคอนฟิกโลจิคัลพาร์ติชันที่เปิดใช้ VTPM ได้สูงสุด 60 พาร์ติชัน (LPAR) สำหรับระบบทางกายภาพแต่ละระบบโดยใช้ Hardware Management Console (HMC) เมื่อ มีการกำหนดค่าคอนฟิกแล้ว VTPM จะไม่ซ้ำกันในแต่ละ LPAR เมื่อใช้กับเทคโนโลยี AIX Trusted Execution VTPM จะให้ความปลอดภัยและการรับประกันในพาร์ติชันต่อไปนี้:

- อิมเมจบูตบนดิสก์
- ระบบปฏิบัติการทั้งหมด
- เลเยอร์แอ็พพลิเคชัน

ผู้ดูแลระบบสามารถดูระบบที่ไว้วางใจได้และไม่ไว้วางใจจาก คอนโซลศูนย์กลางที่ติดตั้งด้วยตัวตรวจสอบ **openpts** ที่มีอยู่ในแพ็กส่วนขยาย AIX คอนโซล **openpts** จะจัดการ หนึ่งเซิร์ฟเวอร์ Power Systems™ หรือมากกว่า และมอนิเตอร์หรือยืนยันสถานะที่ไว้วางใจได้ของระบบ AIX ทั่วทั้ง ศูนย์ข้อมูล การยืนยันเป็นกระบวนการที่ตัวตรวจสอบจะระบุ (หรือยืนยัน ว่าตัวรวบรวมมีการดำเนินการบูตที่ไว้วางใจได้

สถานะการบูตที่ไว้วางใจได้

พาร์ติชันจะถูกระบุว่า ไว้วางใจได้หากตัวตรวจสอบยืนยันบูรณภาพของ ตัวรวบรวมสำเร็จ ตัวตรวจสอบคือพาร์ติชันแบบรีโมทที่ระบุ ว่าตัวรวบรวมมีการดำเนินการบูตที่ไว้วางใจได้ ตัวรวบรวมคือพาร์ติชัน AIX ที่มีการต่อพ่วง Virtual Trusted Platform Module (VTPM) และติดตั้ง Trusted Software Stack (TSS) ซึ่งแสดงให้เห็นว่าการวัดค่าที่ถูกบันทึก ภายใน VTPM ตรงกับชุดอ้างอิงที่จัดเก็บโดยตัวตรวจสอบ สถานะการบูต ที่ไว้วางใจได้จะระบุว่าพาร์ติชันถูกบูตในลักษณะที่ไว้วางใจได้หรือไม่ คำสั่งนี้จะเกี่ยวข้องกับบูรณภาพของกระบวนการบูตของระบบ และ ไม่ได้บ่งบอกถึงระดับที่ต่อเนื่องหรือระดับปัจจุบันของการรักษาความปลอดภัยของ ระบบ

สถานะการบูตที่ไม่ไว้วางใจ

พาร์ติชันเข้าสู่ สถานะที่ไม่ไว้วางใจหากตัวตรวจสอบไม่สามารถยืนยันบูรณภาพ ของกระบวนการบูตได้สำเร็จ สถานะที่ไม่ไว้วางใจบ่งบอกว่า บางลักษณะของกระบวนการบูตไม่สอดคล้องกับข้อมูลอ้างอิง ที่จัดเก็บโดยตัวตรวจสอบ สาเหตุที่เป็นไปได้สำหรับการยืนยันที่ล้มเหลว ได้แก่ การบูตจากอุปกรณ์บูตที่ต่างกัน , การบูตอิมเมจ เคอร์เนลที่ต่างกัน และการเปลี่ยนแปลงอิมเมจการบูตที่มีอยู่

หลักการที่เกี่ยวข้อง:

"การแก้ไขปัญหา Trusted Boot" ในหน้า 9
มีขั้นตอนการแก้ไข และสถานการณ์บางอย่าง ที่จำเป็นในการระบุสาเหตุของการยืนยันที่ล้มเหลว เมื่อใช้ Trusted Boot

การวางแผนสำหรับ Trusted Boot

ศึกษาเกี่ยวกับคอนฟิกูเรชันของฮาร์ดแวร์และซอฟต์แวร์ที่ จำเป็นในการติดตั้ง Trusted Boot

ข้อกำหนดเบื้องต้นของ Trusted Boot

การติดตั้ง Trusted Boot จะเกี่ยวข้องกับการกำหนดค่าคอนฟิก ตัวรวบรวมและตัวตรวจสอบ

| เมื่อคุณเตรียมที่จะติดตั้งระบบปฏิบัติการ AIX อีกครั้งบนระบบที่มีการติดตั้ง Trusted Boot อยู่แล้ว คุณต้องสำเนา ไฟล์ `/var/`
| `tss/lib/tpm/system.data` และใช้ เพื่อเขียนทับไฟล์ในตำแหน่งเดียวกันหลังจากการติดตั้งใหม่เสร็จสมบูรณ์ หากคุณไม่ได้
| สำเนาไฟล์นี้ไว้ คุณต้องลบ Trusted Platform Module เสมือนจริงจากคอนโซลการจัดการและติดตั้งอีกครั้งบน พาร์ติชัน

ตัวรวบรวม

ข้อกำหนดของการกำหนดค่าคอนฟิก เพื่อติดตั้งตัวรวบรวมจะเกี่ยวข้องกับข้อกำหนดเบื้องต้นต่อไปนี้:

- ฮาร์ดแวร์ POWER7 ที่รันบนรีลีสเฟริมแวร์ 740
- ติดตั้ง IBM AIX 6 ที่มีเทคโนโลยีระดับ 7 หรือติดตั้ง IBM AIX 7 ที่มีเทคโนโลยีระดับ 1
- ติดตั้ง Hardware Management Console (HMC) เวอร์ชัน 7.4 หรือใหม่กว่า
- กำหนดค่าคอนฟิกพาร์ติชันด้วย VTPM และมีหน่วยความจำต่ำสุด 1 GB
- ติดตั้ง Secure Shell (SSH) โดยเฉพาะ OpenSSH หรือเทียบเท่า

ตัวตรวจสอบ

ตัวตรวจสอบ **openpts** สามารถเข้าถึงได้จากอินเตอร์เฟสบรรทัดคำสั่ง และอินเตอร์เฟสผู้ใช้ แบบกราฟิกที่ถูกออกแบบมาเพื่อรันบนแพล็ตฟอร์มที่หลากหลาย เวอร์ชัน AIX ของตัวตรวจสอบ OpenPTS จะมีอยู่บนแพ็กส่วนขยายของ AIX เวอร์ชันของตัวตรวจสอบ OpenPTS สำหรับ Linux และแพล็ตฟอร์มอื่นๆ จะหาได้จากเว็บ ดาวน์โหลด ข้อกำหนดของการกำหนดค่าคอนฟิกจะมีข้อกำหนดเบื้องต้น ต่อไปนี้:

- ติดตั้ง SSH โดยเฉพาะ OpenSSH หรือเทียบเท่า
- สร้างการเชื่อมต่อเครือข่าย (ผ่าน SSH) กับตัวรวบรวม
- ติดตั้ง Java™ 1.6 หรือใหม่กว่า เพื่อเข้าถึงคอนโซล **openpts** จากอินเตอร์เฟส แบบกราฟิก

การจัดเตรียมสำหรับการแก้ไข

ข้อมูล Trusted Boot ที่อธิบายไว้ในที่นี้จะทำหน้าที่เป็น แนวทางในการระบุสถานการณ์ที่อาจต้องแก้ไข ซึ่งไม่มีผลกับกระบวนการบูต

มีสถานการณ์ต่างๆ ที่สามารถทำให้การยืนยันล้มเหลว และยากต่อการคาดการณ์สถานการณ์ที่คุณอาจพบ คุณต้องตัดสินใจเกี่ยวกับการดำเนินการที่เหมาะสมขึ้นกับสถานการณ์ อย่างไรก็ตาม วิธีการที่ดีที่สุดคือการเตรียมพร้อมสำหรับสถานการณ์ที่รุนแรงบางอย่าง และมีนโยบาย หรือเวิร์กโฟลว์เพื่อช่วยคุณในการจัดการแต่ละเหตุการณ์ที่เกิดขึ้น การแก้ไขเป็นการดำเนินการที่ถูกต้องที่ต้องดำเนินการเมื่อการยืนยัน รายงานว่ามีหนึ่งตัวรวบรวมหรือมากกว่าที่ไม่ไว้วางใจ

ตัวอย่างเช่น หากการยืนยันล้มเหลวเนื่องจากอิมเมจการบูต แตกต่างจากการอ้างอิงของตัวตรวจสอบ ให้พิจารณาถึงคำตอบในคำถามต่อไปนี้:

- คุณสามารถตรวจสอบว่าภัยคุกคามมีความเชื่อถือได้อย่างไร
- มีการบำรุงรักษาที่วางแผนไว้ที่ดำเนินการแล้ว เช่น การอัพเกรด AIX หรือฮาร์ดแวร์ใหม่ ที่มีการติดตั้งล่าสุดหรือไม่
- คุณสามารถติดต่อผู้ดูแลระบบที่มีสิทธิ์เข้าถึงข้อมูลนี้หรือไม่
- เมื่อไรที่ระบบมีการบูตล่าสุดในสถานะที่ไว้วางใจได้
- หากภัยคุกคามความปลอดภัยมีลักษณะที่ถูกต้อง คุณจะใช้การดำเนินการใด (คำแนะนำ ได้แก่ เก็บรวบรวมล็อกการตรวจสอบ, ตัดการเชื่อมต่อระบบ จากเครือข่าย, ปิดการทำงานของระบบ และแจ้งเตือนผู้ใช้)
- มีระบบอื่นๆ ที่ถูกบุกรุกที่ต้องถูกตรวจสอบหรือไม่

หลักการที่เกี่ยวข้อง:

"การแก้ไขปัญหา Trusted Boot" ในหน้า 9
มีขั้นตอนการแก้ไข และสถานการณ์บางอย่าง ที่จำเป็นในการระบุสาเหตุของการยืนยันที่ล้มเหลว เมื่อใช้ Trusted Boot

สิ่งที่ต้องพิจารณาในการโอนย้าย

พิจารณาข้อกำหนดเบื้องต้นเหล่านี้ก่อนที่คุณจะโอนย้ายพาร์ติชัน ที่เปิดใช้งานสำหรับ Virtual Trusted Platform Module (VTPM)

ประโยชน์ของ VTPM บน TPM ทางกายภาพก็คือจะอนุญาตให้ พาร์ติชันสามารถย้ายระหว่างระบบขณะที่ยังคงรักษา VTPM เพื่อการโอนย้าย โลจิคัลพาร์ติชันอย่างปลอดภัย เฟิร์มแวร์จะเข้ารหัสข้อมูล VTPM ก่อนทำการส่ง เพื่อให้แน่ใจว่าการโอนย้ายปลอดภัย ต้องปรับใช้มาตรการ การรักษาความปลอดภัยต่อไปนี้ก่อนทำการโอนย้าย:

- เปิดใช้ IPSEC ระหว่าง Virtual I/O Server (VIOS) นั้นคือ การดำเนินการโอนย้าย
- ตั้งค่าคีย์ระบบที่ไว้วางใจได้ผ่าน Hardware Management Console (HMC) เพื่อควบคุม ระบบที่ถูกจัดการที่มีความสามารถในการถอดรหัสข้อมูล VTPM หลังจาก โอนย้าย ระบบปลายทางของการโอนย้ายต้องมีคีย์เดียวกันกับ ระบบต้นทางเพื่อให้การโอนย้ายข้อมูลสำเร็จ

ข้อมูลที่เกี่ยวข้อง:

การใช้ HMC

การโอนย้าย VIOS

การติดตั้ง Trusted Boot

มีการกำหนดค่าคอนฟิกทางฮาร์ดแวร์และซอฟต์แวร์บางอย่าง ที่จำเป็นในการติดตั้ง Trusted Boot

ข้อมูลที่เกี่ยวข้อง:

"การติดตั้ง PowerSC Standard Edition 1.1.3" ในหน้า 3
คุณต้องติดตั้ง fileset สำหรับแต่ละฟังก์ชันเฉพาะของ PowerSC Standard Edition

การติดตั้งตัวรวบรวม

คุณต้องติดตั้งตัวรวบรวมโดยการใช้ fileset จาก ซีดีพื้นฐานของ AIX

เพื่อติดตั้งตัวรวบรวม ให้ติดตั้งแพ็กเกจ `powerscStd.vtpm` และ `openpts.collector` ซึ่งอยู่ใน ซีดีพื้นฐาน โดยใช้คำสั่ง **smit** หรือ **installp**

การติดตั้งตัวตรวจสอบ

คอมโพเนนต์ตัวตรวจสอบ OpenPTS จะรันบนระบบปฏิบัติการ AIX และบนแพล็ตฟอร์มอื่นๆ

เวอร์ชัน AIX ของตัวตรวจสอบสามารถติดตั้งจาก fileset โดยใช้แพ็คส่วนขยาย AIX เพื่อติดตั้งตัวตรวจสอบบนระบบปฏิบัติการ AIX ให้ติดตั้งแพ็กเกจ `openpts.verifier` จากแพ็กส่วนขยาย AIX โดยใช้คำสั่ง **smit** หรือ **installp** ซึ่ง จะติดตั้งทั้งเวอร์ชันบรรทัดคำสั่ง และอินเตอร์เฟสแบบกราฟิกของ ตัวตรวจสอบ

ตัวตรวจสอบ OpenPTS สำหรับระบบปฏิบัติการอื่นๆ สามารถดาวน์โหลดได้จาก ดาวน์โหลด `Linux OpenPTS Verifier` สำหรับ ใช้กับ `AIX Trusted Boot`

ข้อมูลที่เกี่ยวข้อง:

 ดาวน์โหลด Linux OpenPTS Verifier สำหรับใช้กับ AIX Trusted Boot

การกำหนดค่าคอนฟิก Trusted Boot

ศึกษาขั้นตอนเพื่อลงทะเบียนระบบ และเพื่อยืนยัน ระบบสำหรับ Trusted Boot

การลงทะเบียนระบบ

ศึกษาขั้นตอนเพื่อลงทะเบียนระบบกับตัวตรวจสอบ

การลงทะเบียนระบบคือกระบวนการระบุชุดเริ่มต้นของ การวัดค่าในตัวตรวจสอบ ซึ่งจะสร้างพื้นฐานสำหรับคำขอการยืนยันต่อมา เพื่อลงทะเบียนระบบจากบรรทัดคำสั่ง ให้ใช้ คำสั่งต่อไปนี้จากตัวตรวจสอบ:

```
openpts -i <hostname>
```

ข้อมูลเกี่ยวกับพาร์ติชันที่ลงทะเบียนจะอยู่ในไดเร็กทอรี `$HOME/.openpts` พาร์ติชันใหม่แต่ละพาร์ติชันจะถูกกำหนด ด้วยตัวระบบที่ไม่ซ้ำกันระหว่างกระบวนการลงทะเบียน และข้อมูลที่เชื่อมโยงกับพาร์ติชันที่ลงทะเบียนจะถูกจัดเก็บในไดเร็กทอรีที่สอดคล้องกับ ID เฉพาะ

เพื่อลงทะเบียนระบบจากอินเตอร์เฟสแบบกราฟิก ให้ดำเนินการขั้นตอน ต่อไปนี้:

1. เริ่มต้นอินเตอร์เฟสแบบกราฟิกโดยใช้คำสั่ง **/opt/ibm/openpts_gui/openpts_GUI.sh**
2. เลือก **Enroll** จากเมนูการนำทาง
3. ป้อนชื่อโฮสต์ และข้อมูลประจำตัว SSH ของระบบ
4. คลิก **Enroll**

หลักการที่เกี่ยวข้อง:

“การยืนยันระบบ”
ศึกษาขั้นตอนเพื่อยืนยันระบบจากบรรทัดคำสั่ง และโดยใช้อินเตอร์เฟสกราฟิก

การยืนยันระบบ

ศึกษาขั้นตอนเพื่อยืนยันระบบจากบรรทัดคำสั่ง และโดยใช้อินเตอร์เฟสกราฟิก

เพื่อเคียวรีบูรณภาพของการบูตระบบ ใช้คำสั่งต่อไปนี้ จากตัวตรวจสอบ:

```
openpts <hostname>
```

เพื่อยืนยันระบบจากอินเตอร์เฟสแบบกราฟิก ให้ดำเนินการขั้นตอน ต่อไปนี้:

1. เลือกหมวดหมู่จากเมนูการนำทาง
2. เลือกหนึ่งระบบหรือมากกว่าเพื่อยืนยัน
3. คลิก **ยืนยัน**

การลงทะเบียนและการยืนยันระบบโดยไม่ต้องมี รหัสผ่าน

การร้องขอการยืนยันจะถูกส่งผ่าน Secure Shell (SSH) ติดตั้งใบรับรองของตัวตรวจสอบบนตัวรวบรวมเพื่อ อนุญาตให้เชื่อมต่อ SSH โดยไม่ต้องมีรหัสผ่าน

เพื่อติดตั้งใบรับรอง ของตัวตรวจสอบบนระบบของตัวรวบรวม ให้ดำเนินการขั้นตอนต่อไปนี้ :

- บนตัวตรวจสอบ ให้รันคำสั่งต่อไปนี้:

```
ssh-keygen    # No passphrase
scp ~/.ssh/id_rsa.pub <collector>:/tmp
```

- บนตัวรวบรวม ให้รันคำสั่งต่อไปนี้:

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

การจัดการ Trusted Boot

ศึกษาขั้นตอนในการจัดการผลลัพธ์การยืนยันของ Trusted Boot

การตีความผลลัพธ์การยืนยัน

ศึกษาขั้นตอนเพื่อดูและทำความเข้าใจการยืนยัน ผลลัพธ์

การยืนยันสามารถให้ผลลัพธ์เป็นหนึ่งในสถานะต่อไปนี้:

1. คำร้องขอการยืนยันล้มเหลว: คำร้องขอการยืนยันไม่ ไม่เสร็จสมบูรณ์ โปรดดูส่วน การแก้ไขปัญหา เพื่อ ทำความเข้าใจสาเหตุที่เป็นไปได้สำหรับความล้มเหลว
2. บูรณภาพของระบบถูกต้อง: การยืนยันประสบความเร็จ และการบูตของระบบตรงกับข้อมูลอ้างอิงที่จัดเก็บไว้โดยตัวตรวจสอบ ซึ่งระบุว่าเป็น Trusted Boot ที่สำเร็จ
3. บูรณภาพของระบบที่ไม่ถูกต้อง: คำร้องขอการยืนยันเสร็จสมบูรณ์ แต่ ตรวจพบข้อแตกต่างระหว่างข้อมูลที่รวบรวมไว้ระหว่างการบูตระบบ และข้อมูลอ้างอิงที่จัดเก็บไว้โดย ตัวตรวจสอบ ซึ่งระบุว่าเป็นการบูตที่ไม้วางใจ

การยืนยันยังรายงานว่ามีการปรับใช้การอัพเดต ในตัวรวบรวมโดยใช้ข้อความต่อไปนี้:

มีการอัพเดตระบบ: ข้อความนี้ระบุว่ามีการปรับใช้การอัพเดต บนตัวรวบรวม และชุดของข้อมูลอ้างอิงที่อัพเดตที่พร้อมใช้งานที่จะมีผลสำหรับการบูตครั้งถัดไป ผู้ใช้จะได้รับพร้อมต์ บนตัวตรวจสอบเพื่อยอมรับ หรือปฏิเสธการอัพเดต ตัวอย่างเช่น ผู้ใช้สามารถเลือกที่จะยอมรับการอัพเดตเหล่านี้หากผู้ใช้ตระหนักถึง การบำรุงรักษาที่เกิดขึ้นบนตัวรวบรวม

เพื่อตรวจสอบการยืนยันที่ล้มเหลวโดยใช้อินเตอร์เฟสแบบกราฟิก ให้ดำเนินการขั้นตอนต่อไปนี้:

1. เลือกหมวดหมู่จากเมนูการนำทาง
2. เลือกระบบที่จะตรวจสอบ
3. ดับเบิลคลิกรายการที่สอดคล้องกับระบบ หน้าต่างคุณสมบัติ จะแสดงขึ้น หน้าต่างนี้จะมีข้อมูลล็อกเกี่ยวกับ การยืนยันที่ล้มเหลว

การลบระบบ

ศึกษาขั้นตอนเพื่อลบระบบออกจากฐานข้อมูล ของตัวตรวจสอบ

เพื่อลบระบบออกจากฐานข้อมูลของตัวตรวจสอบ ให้รันคำสั่ง ต่อไปนี้:

```
openpts -r <hostname>
```

การแก้ไขปัญหา Trusted Boot

มีขั้นตอนการแก้ไข และสถานการณ์บางอย่าง ที่จำเป็นในการระบุสาเหตุของการยืนยันที่ล้มเหลว เมื่อใช้ Trusted Boot

คำสั่ง **openpts** จะระบุว่าระบบไม่ถูกต้อง หากสถานะการบูตในปัจจุบันของระบบไม่ตรงกับข้อมูลอ้างอิง ที่จัดเก็บไว้บนตัวตรวจสอบ คำสั่ง **openpts** ระบุสาเหตุที่เป็นไปได้สำหรับบูรณภาพที่ไม่ถูกต้อง มีตัวแปรต่างๆ ในการบูต AIX เต็มรูปแบบ และการยืนยันที่ล้มเหลวต้องมีการวิเคราะห์เพื่อระบุ สาเหตุของความล้มเหลว

ตารางต่อไปนี้จะแสดงสถานการณ์จำลองบางอย่าง และขั้นตอนการแก้ไข เพื่อระบุสาเหตุของความล้มเหลว:

ตารางที่ 2. การแก้ไขปัญหาสถานการณ์จำลองบางอย่างสำหรับความล้มเหลว

สาเหตุของความล้มเหลว	สาเหตุที่เป็นไปได้ของความล้มเหลว	การแก้ไขที่แนะนำ

การยืนยันไม่สมบูรณ์	• ชื่อโฮสต์ไม่ถูกต้อง
	• ไม่มีเส้นทางเครือข่ายระหว่างต้นทางและปลายทาง
	• ข้อมูลประจำตัวการรักษาความปลอดภัยไม่ถูกต้อง
		ตรวจสอบการเชื่อม Secure Shell (SSH) โดยใช้ คำสั่งต่อไปนี้:
		`ssh ptsc@hostname`
		หาก การเชื่อมต่อ SSH ประสบสำเร็จ ให้ตรวจสอบสาเหตุต่อไปนี้ สำหรับการยืนยันที่ล้มเหลว:
		• ระบบที่กำลังถูกยืนยันไม่ได้รัน **tcsd** daemon
		• ระบบที่กำลังถูกยืนยันไม่ได้เริ่มต้นด้วยคำสั่ง **ptsc** กระบวนการนี้ควรเกิดขึ้นโดยอัตโนมัติระหว่าง การเริ่มต้นระบบแต่จะตรวจสอบการมีอยู่ของไดเร็กทอรี `/var/ptsc/` บนตัวรวบรวม หากไดเร็กทอรี `/var/ptsc/` ไม่มีอยู่ ให้รันคำสั่งต่อไปนี้บนตัวรวบรวม:
		`ptsc -i`

เฟิร์มแวร์ CEC มีการเปลี่ยนแปลง	• ใช้เฟิร์มแวร์ที่อัพเกรด • LPAR ถูกโอนย้ายไปยังระบบที่รันเวอร์ชันที่แตกต่าง ของเฟิร์มแวร์	ตรวจสอบระดับเฟิร์มแวร์ของระบบที่โฮสต์ LPAR
รีซอร์สที่จัดสรรให้กับ LPAR มีการเปลี่ยนแปลง	CPU หรือหน่วยความจำที่จัดสรรให้กับ LPAR มีการเปลี่ยนแปลง	ตรวจสอบโปรไฟล์ของพาร์ติชันใน HMC
เฟิร์มแวร์มีการเปลี่ยนแปลงสำหรับอะแด็ปเตอร์ที่มีอยู่ใน LPAR	อุปกรณ์ฮาร์ดแวร์ถูกเพิ่มหรือลบออกจาก LPAR	ตรวจสอบโปรไฟล์พาร์ติชันใน HMC
รายการอุปกรณ์ที่ต่อพ่วงกับ LPAR มีการเปลี่ยนแปลง	อุปกรณ์ฮาร์ดแวร์ถูกเพิ่มหรือลบออกจาก LPAR	ตรวจสอบโปรไฟล์พาร์ติชันใน HMC
อิมเมจการบูตมีการเปลี่ยนแปลง ซึ่งรวมถึงเคอร์เนลของ ระบบปฏิบัติการ	• ใช้การอัพเดต AIX และตัวตรวจสอบไม่ได้รับรู้ถึงการอัพเดต • คำสั่ง **bosboot** รันอยู่	• ตรวจสอบกับผู้ดูแลระบบว่ามีการดำเนินการบำรุงรักษาใดๆ หรือไม่ ก่อนดำเนินการรีบูตครั้งล่าสุด • ตรวจสอบล็อกบนตัวรวบรวมสำหรับกิจกรรมการบำรุงรักษา
LPAR ถูกบูตจากอุปกรณ์อื่น	• การลงทะเบียนถูกดำเนินการทันทีหลังจากการติดตั้งเครือข่าย • ระบบถูกบูตจากอุปกรณ์การบำรุงรักษา	สามารถตรวจสอบแฟล็ก และอุปกรณ์การบูตโดยใช้คำสั่ง **bootinfo** หากการลงทะเบียนถูกดำเนินการทันที หลังจากการติดตั้ง Network Installation Management (NIM) และก่อน ทำการรีบูต รายละเอียดที่ลงทะเบียนไว้จะเกี่ยวข้องกับการติดตั้งเครือข่าย และไม่ใช่การบูตด้วยดิสก์ในครั้งถัดไป การลงทะเบียนนี้สามารถ แก้ไขโดยการลบการลงทะเบียน และทำการลงทะเบียนโลจิคัลพาร์ติชันใหม่

ตารางที่ 2. การแก้ไขปัญหาสถานการณ์จำลองบางอย่างสำหรับความล้มเหลว (ต่อ)

สาเหตุของความล้มเหลว	สาเหตุที่เป็นไปได้ของความล้มเหลว	การแก้ไขที่แนะนำ
เมนูบูต System Management Services (SMS) แบบโต้ตอบถูกเรียกใช้		กระบวนการบูตจะต้องรันอย่างต่อเนื่องโดยไม่ต้องมีการโต้ตอบของผู้ใช้ สำหรับระบบที่ไว้วางใจได้ การเข้าสู่เมนูการบูต SMS จะทำให้ การบูตไม่ถูกต้อง
ฐานข้อมูล Trusted Execution (TE) ถูกแก้ไข	• ไฟล์ไบนารีจะถูกเพิ่ม หรือลบออกจากฐานข้อมูล TE • ไฟล์ไบนารีในฐานข้อมูลถูกอัพเดต	รันคำสั่ง **trustchk** เพื่อตรวจสอบฐานข้อมูล

หลักการที่เกี่ยวข้อง:

"การจัดเตรียมสำหรับการแก้ไข" ในหน้า 6
ข้อมูล Trusted Boot ที่อธิบายไว้ในที่นี้จะทำหน้าที่เป็น แนวทางในการระบุสถานการณ์ที่อาจต้องแก้ไข ซึ่งไม่มีผลกับกระบวนการบูต

"แนวคิด Trusted Boot" ในหน้า 4
เป็นสิ่งสำคัญที่ต้องเข้าใจบูรณภาพของกระบวนการ บูต และวิธีในการแบ่งแยกบูตเป็นการบูตที่ไว้วางใจได้ และการบูต ที่ไม่ไว้วางใจ

ข้อมูลที่เกี่ยวข้อง:

การใช้ HMC

Trusted Firewall

คุณลักษณะ Trusted Firewall จะมีเวอร์ชวลไลเซชันเลเยอร์ ที่ปลอดภัยที่ช่วยเพิ่มประสิทธิภาพการทำงาน และประสิทธิภาพของรีซอร์สเมื่อสื่อสาร ระหว่างโซนการรักษาความปลอดภัยของ Virtual LAN (VLAN) ที่ต่างกันบนเซิร์ฟเวอร์ Power Systems เดียวกัน Trusted Firewall จะลดโหลดบนเครือข่ายภายนอกโดยการย้าย ความสามารถในการกรองของแพ็กเกจไฟลวอลล์ที่ตรงตามกฎที่กำหนดไปยัง เวอร์ชวลไลเซชันเลเยอร์ ความสามารถในการกรองนี้จะถูกควบคุม โดยกฎตัวกรองเครือข่ายที่กำหนด ซึ่งอนุญาตให้ทราฟฟิกของเครือข่าย ที่ไว้วางใจได้สามารถสื่อสารข้ามระหว่างโซนการรักษาความปลอดภัยของ VLAN โดยไม่ต้องออกจากสภาพแวดล้อม เสมือน Trusted Firewall จะปกป้อง และกำหนดเส้นทางทราฟฟิกเครือข่าย ภายในระหว่างระบบปฏิบัติการ AIX, IBM i และ Linux

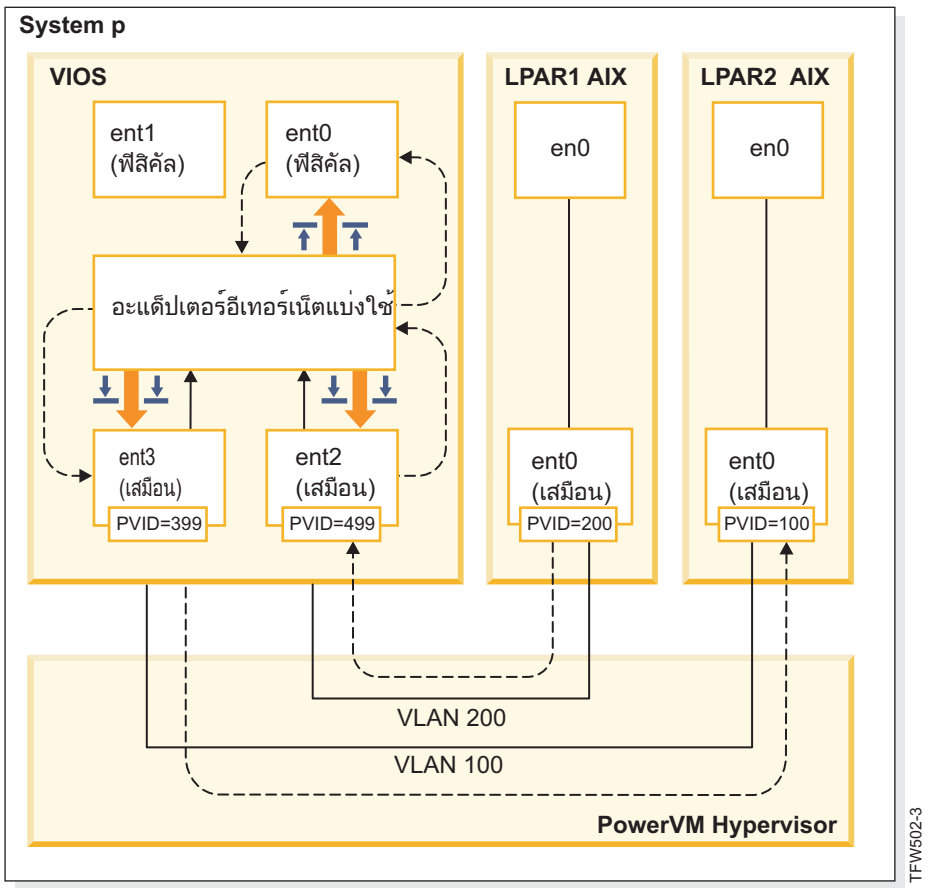
แนวคิด Trusted Firewall

มีแนวคิดพื้นฐานบางอย่างที่ต้องเข้าใจเมื่อใช้ Trusted Firewall

ฮาร์ดแวร์ Power Systems สามารถกำหนดค่าคอนฟิก ให้มีโซนการรักษาความปลอดภัย LAN เสมือน (VLAN) หลายโซน นโยบายที่กำหนดค่าคอนฟิกโดยผู้ใช้ซึ่งถูกสร้างเป็นกฎตัวกรอง Trusted Firewall จะอนุญาตให้ทราฟฟิกเครือข่ายที่ไว้ใจได้บางทราฟฟิกเพื่อสามารถข้ามระหว่างโซนการรักษาความปลอดภัย VLAN และยังคงอยู่ภายในเวอร์ชวลไลเซชันเลเยอร์ ซึ่งจะคล้ายกับ การเพิ่มไฟล์วอลล์ทางกายภาพที่ต่อกับเครือข่ายไปยังสภาพแวดล้อม เสมือนจริง ซึ่งมีวิธีการที่ช่วยเพิ่มประสิทธิภาพการทำงานเพิ่มขึ้น ในการปรับใช้ความสามารถไฟล์วอลล์สำหรับศูนย์ข้อมูลเสมือนจริง

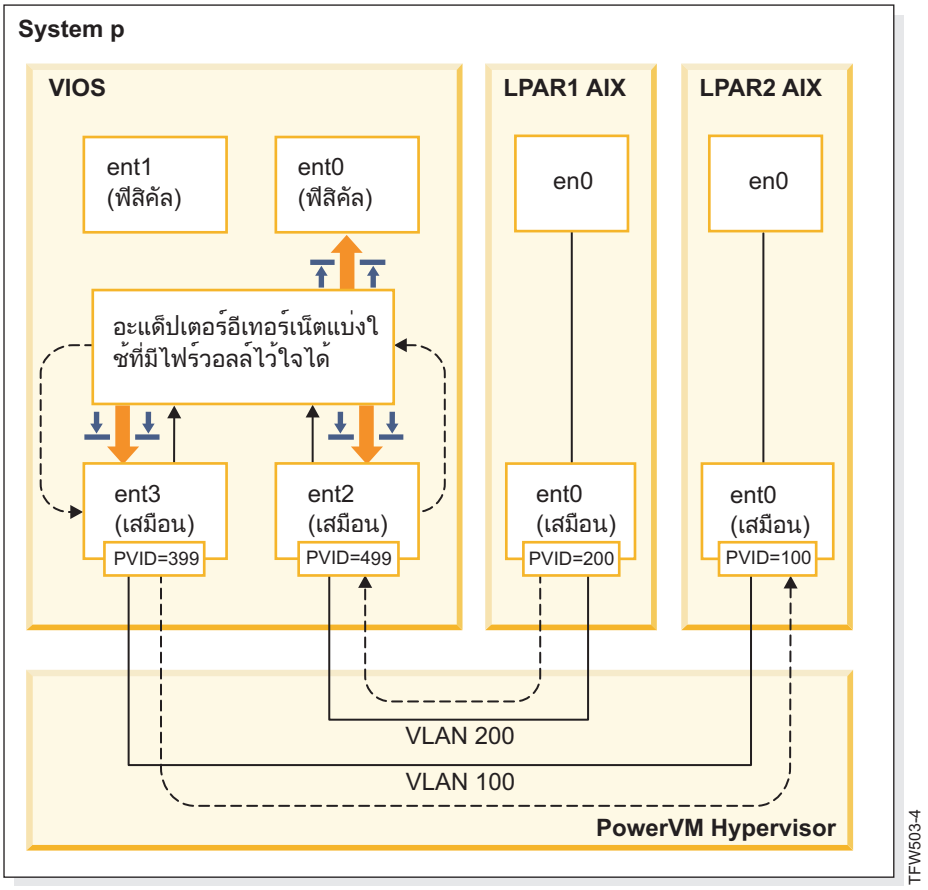
ด้วย Trusted Firewall คุณสามารถกำหนดค่าคอนฟิกกฎเพื่ออนุญาตให้ทราฟฟิก บางชนิดถ่ายโอนโดยตรงจากหนึ่ง VLAN บน Virtual I/O Server (VIOS) ไปยัง VLAN อื่นบน VIOS เดียวกัน ขณะที่ยังคงรักษาระดับการรักษาความปลอดภัยที่สูงโดยการจำกัด ทราฟฟิกชนิดอื่นๆ ซึ่งเป็นไฟล์วอลล์ที่สามารถกำหนดค่าคอนฟิกได้ภายในเวอร์ชวลไลเซชันเลเยอร์ ของเซิร์ฟเวอร์ Power Systems

การใช้ตัวอย่างใน รูปที่ 1เป้าหมายคือสามารถถ่ายโอน ข้อมูลที่มีความปลอดภัย และมีประสิทธิภาพจาก LPAR1 บน VLAN 200 และจาก LPAR2 บน VLAN 100 ข้อมูลที่กำหนดเป้าหมาย ไปยัง LPAR2 จาก LPAR1 จะถูกส่งจากเครือข่ายอินเตอร์เน็ตไปยังเราเตอร์ ซึ่งจะกำหนดเส้นทางข้อมูลกลับไปที่ LPAR2 โดยไม่ต้องใช้ Trusted Firewall



รูปที่ 1. ตัวอย่างของการถ่ายโอนข้อมูลข้าม VLAN โดยไม่ต้องใช้ Trusted Firewall

การใช้ Trusted Firewall คุณสามารถกำหนดค่าคอนฟิกกฎเพื่ออนุญาตให้ข้อมูล ส่งจาก LPAR1 ไปยัง LPAR2 โดยไม่ต้องออกจากเครือข่ายอินเตอร์เน็ต เส้นทางนี้จะถูกแสดงใน รูปที่ 2 ในหน้า 13



รูปที่ 2. ตัวอย่าง ของการถ่ายโอนข้อมูลข้าม VLAN ด้วย Trusted Firewall

การกำหนดค่าคอนฟิกกฎจะอนุญาตให้บางข้อมูลที่จะถูกส่ง ข้าม VLANs ไปยังปลายทางในเส้นทางที่สั้นลง Trusted Firewall จะใช้ส่วนขยายเคอร์เนล Shared Ethernet Adapter (SEA) และ Security Virtual Machine (SVM) เพื่อเปิดใช้การสื่อสาร

Shared Ethernet Adapter

SEA คือตำแหน่งที่การกำหนดเส้นทางเริ่มต้น และสิ้นสุด เมื่อ SVM ถูกลงทะเบียน SEA จะได้รับแพ็กเกจและส่งต่อไปยัง SVM หาก SVM ระบุว่าแพ็กเกจมีไว้สำหรับ LPAR บนเซิร์ฟเวอร์ Power Systems เดียวกัน SVM จะอัพเดตส่วนหัวของเลเยอร์ 2 ของแพ็กเกจ แพ็กเกจจะถูกส่งกลับไปยัง SEA สำหรับการส่งต่อไปยังปลายทางสุดท้ายภายในระบบ หรือบนเครือข่ายภายนอก

Security Virtual Machine

SVM คือตำแหน่งที่ใช้กฎตัวกรอง กฎตัวกรอง เป็นสิ่งจำเป็นเพื่อรักษาความปลอดภัยบนเครือข่ายภายใน หลังจากการลงทะเบียน SVM กับ SEA แพ็กเกจจะถูกส่งต่อ ไปยัง SVM ก่อนจะถูกส่งไปยังเครือข่ายภายนอก ขึ้นอยู่กับ กฎตัวกรองที่ใช้งาน SVM จะตรวจสอบว่าแพ็กเกจอยู่ใน เครือข่ายภายใน หรือย้ายไปยังเครือข่ายภายนอก

การติดตั้ง Trusted Firewall

การติดตั้ง PowerSC Trusted Firewall จะคล้ายกับการติดตั้งคุณลักษณะ PowerSC อื่นๆ

ข้อกำหนดเบื้องต้น:

- เวอร์ชันของ PowerSC ก่อน 1.1.1.0 จะไม่มี fileset ที่จำเป็นในการติดตั้ง Trusted Firewall ตรวจสอบให้แน่ใจว่าคุณมีซีดีการติดตั้ง PowerSC สำหรับเวอร์ชัน 1.1.1.0 หรือใหม่กว่า

- เพื่อใช้ประโยชน์ของ Trusted Firewall คุณต้องมีการใช้ Hardware Management Console (HMC) หรือ Virtual I/O Server (VIOS) อยู่แล้วเพื่อกำหนดค่าคอนฟิก Virtual LANs (VLANs) ของคุณ

Trusted Firewall จะถูกระบุเป็น fileset เพิ่มเติมใน แผ่นซีดีการติดตั้ง PowerSC Standard Edition ชื่อไฟล์คือ `powerscStd.svm.rte` คุณสามารถเพิ่ม Trusted Firewall ไปยังอินสแตนซ์ที่มีอยู่ของ PowerSC เวอร์ชัน 1.1.0.0 หรือใหม่กว่า หรือติดตั้งเป็นส่วนหนึ่งของการติดตั้งใหม่ของ PowerSC เวอร์ชัน 1.1.1.0 หรือใหม่กว่า

เพื่อเพิ่มฟังก์ชัน Trusted Firewall ไปยังอินสแตนซ์ PowerSC ที่มีอยู่:

1. ตรวจสอบให้แน่ใจว่าคุณรัน VIOS เวอร์ชัน 2.2.1.4 หรือใหม่กว่า
2. ใส่แผ่นซีดีการติดตั้ง PowerSC เวอร์ชัน 1.1.1.0 หรือดาวน์โหลดอิมเมจของ ซีดีการติดตั้ง
3. ใช้คำสั่ง **oem_setup_env** สำหรับการเข้าถึง รูท
4. ใช้คำสั่ง **installp** หรือเครื่องมือ SMIT เพื่อติดตั้ง fileset ใน `PowerscStd.svm.rte`

ข้อมูลที่เกี่ยวข้อง:

"การติดตั้ง PowerSC Standard Edition 1.1.3" ในหน้า 3
คุณต้องติดตั้ง fileset สำหรับแต่ละฟังก์ชันเฉพาะของ PowerSC Standard Edition

การกำหนดค่าคอนฟิก Trusted Firewall

ต้องมีการตั้งค่าคอนฟิกูเรชันเพิ่มเติมสำหรับ คุณลักษณะ Trusted Firewall หลังจากที่มีการติดตั้ง

การมอนิเตอร์ Trusted Firewall

การมอนิเตอร์ Trusted Firewall จะวิเคราะห์ทราฟฟิกของระบบจาก โลจิคัลพาร์ติชัน (LPARs) ที่แตกต่างกันเพื่อระบุข้อมูลที่เป็นประโยชน์ เพื่อตรวจสอบว่าการรัน Trusted Firewall ช่วยให้มีประสิทธิภาพของระบบที่ดีขึ้นหรือไม่

หากฟังก์ชันการมอนิเตอร์ Trusted Firewall บันทึกปริมาณที่สำคัญ ของทราฟฟิกจาก LANs เสมือน (VLANs) ที่ต่างกันที่อยู่บน คอมเพล็กซ์อิเล็กทรอนิกส์กลางเดียวกัน การเปิดใช้ Trusted Firewall ควร จะมีประโยชน์กับระบบของคุณ

เพื่อเปิดใช้การมอนิเตอร์ Trusted Firewall ให้ป้อนคำสั่งต่อไปนี้:

```
vlantfw -m
```

เพื่อแสดงผลลัพธ์ของการมอนิเตอร์ Trusted Firewall ให้ป้อน คำสั่งต่อไปนี้:

```
vlantfw -D
```

เพื่อปิดใช้การมอนิเตอร์ Trusted Firewall ให้ป้อนคำสั่งต่อไปนี้:

```
vlantfw -M
```

การบันทึกล็อก Trusted Firewall

การบันทึกล็อก Trusted Firewall จะรวบรวมรายการเส้นทางทราฟฟิกเครือข่าย ภายในคอมเพล็กซ์อิเล็กทรอนิกส์กลาง รายการจะแสดงตัวกรอง ที่ Trusted Firewall ใช้เพื่อกำหนดเส้นทางทราฟฟิก

เมื่อการมอนิเตอร์ Trusted Firewall ระบุว่าเส้นทางทราฟฟิก ภายในทำให้มีประสิทธิภาพที่ดีขึ้น การบันทึกล็อก Trusted Firewall จะเก็บรักษา รายการเส้นทางไว้ในไฟล์ `svm.log` ขีดจำกัด ของขนาดไฟล์ `svm.log` เท่ากับ 16 MB หากรายการ เกินกว่าขีดจำกัด 16 MB รายการที่เก่าที่สุดจะถูกลบออกจากล็อก ไฟล์

เพื่อสตาร์ทการบันทึกล็อก Trusted Firewall ให้ป้อนคำสั่งต่อไปนี้:

```
vlantfw -l
```

เพื่อหยุดการบันทึกล็อก Trusted Firewall ให้ป้อนคำสั่งต่อไปนี้:

```
vlantfw -L
```

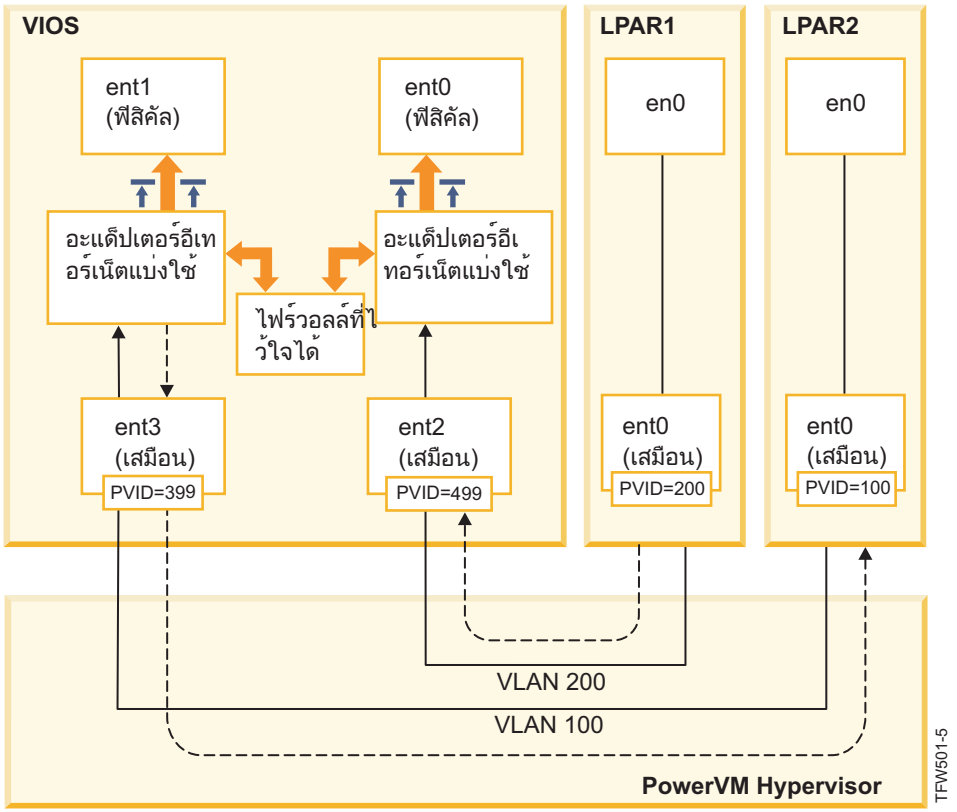
คุณสามารถดูล็อกไฟล์ที่ตำแหน่ง ต่อไปนี้: `/home/padmin/svm/svm.log`

หลาย Shared Ethernet Adapters

คุณสามารถกำหนดค่าคอนฟิก Trusted Firewall บนระบบที่ใช้ หลาย Shared Ethernet Adapters

บางคอนฟิกูเรชันจะใช้หลาย Shared Ethernet Adapters (SEAs) บน Virtual I/O Server (VIOS) เดียวกัน หลาย SEAs สามารถให้ประโยชน์ในการป้องกันการ Failover และ การปรับระดับรีซอร์ส Trusted Firewall สนับสนุนการกำหนดเส้นทางข้ามหลาย SEAs ซึ่งจะมีอยู่บน VIOS เดียวกัน

รูปที่ 3แสดง สภาพแวดล้อมที่ใช้หลาย SEAs



รูปที่ 3. การกำหนดค่าคอนฟิกเพื่อใช้หลาย Shared Ethernet Adapters บน VIOS เดียว

ต่อไปนี้คือตัวอย่างของหลายคอนฟิกูเรชัน SEA ที่ สนับสนุนโดย Trusted Firewall:

- SEAs จะถูกกำหนดค่าคอนฟิกด้วยอะแด็ปเตอร์ Trunk บน Hypervisor Virtual Switch ของ Power® เดียวกัน คอนฟิกูเรชันนี้ได้รับการสนับสนุนเนื่องจากแต่ละ SEA จะได้รับทราฟฟิก เครือข่ายที่มี VLAN IDs ที่ต่างกัน

- SEAs ถูกกำหนดค่าคอนฟิกด้วยอะแด็ปเตอร์ Trunk บน Hypervisor Virtual Switch ของ Power ที่ต่างกัน และแต่ละ Trunk Adapters อยู่บน VLAN ID ที่ต่างกัน ในคอนฟิกูเรชันนี้ แต่ละ SEA ยังคงได้รับทราฟฟิกเครือข่ายโดยใช้ VLAN IDs ที่ต่างกัน
- SEAs ถูกกำหนดค่าคอนฟิกด้วยอะแด็ปเตอร์ Trunk บน Hypervisor Virtual Switch ของ Power ที่ต่างกัน และนำ VLAN IDs เดียวกันกลับมาใช้บนสวิตช์เสมือน ในกรณีนี้ ทราฟฟิกสำหรับทั้งสอง SEAs จะมี VLAN IDs เดียวกัน

  ตัวอย่าง ของคอนฟิกูเรชันนี้จะมี LPAR2 บน VLAN200 ที่มีสวิตช์เสมือน 10 และ LPAR3 บน VLAN200 ที่มีสวิตช์เสมือน 20 เนื่องจากทั้งสอง LPARs และ SEAs ที่สอดคล้องกันจะใช้ VLAN ID เดียวกัน (VLAN200) ทั้งสอง SEAs จะมีสิทธิ์ในการเข้าถึงแพ็กเกจด้วย VLAN ID นั้น

คุณไม่สามารถเปิดใช้การเชื่อมกันมากกว่าหนึ่ง VIOS ด้วยเหตุผลนี้ หลายคอนฟิกูเรชัน SEA ต่อไปนี้จะไม่ได้รับการสนับสนุนโดย Trusted Firewall:

- หลาย VIOS และหลายไดร์เวอร์ SEA
- การแบ่งใช้โหลด SEA สำรอง: อะแด็ปเตอร์ Trunk ที่ถูกกำหนดค่าคอนฟิก สำหรับการกำหนดเส้นทางทราฟฟิกระหว่าง VLAN ไม่สามารถแยกระหว่างเซิร์ฟเวอร์ VIOS

การลบ Shared Ethernet Adapters

ขั้นตอนในการลบอุปกรณ์ Shared Ethernet Adapter ออกจาก ระบบต้องดำเนินการในลำดับเฉพาะ

เพื่อลบ Shared Ethernet Adapter (SEA) ออกจากระบบของคุณ ให้ดำเนินการ ขั้นตอนต่อไปนี้:

1. ลบ Security Virtual Machine ที่เชื่อมโยงกับ SEA โดยการป้อนคำสั่งต่อไปนี้:

   ```
   rmdev -dev svm
   ```

2. ลบ SEA โดยการป้อนคำสั่งต่อไปนี้:

   ```
   rmdev -dev shared ethernet adapter ID
   ```

หมายเหตุ: ลบ SEA ก่อนทำการลบ SVM อาจทำให้ ระบบล้มเหลว

การสร้างกฎ

คุณสามารถสร้างกฎเพื่อเปิดใช้การกำหนดเส้นทาง Trusted Firewall ข้าม VLAN

เพื่อเปิดใช้คุณลักษณะการกำหนดเส้นทางของ Trusted Firewall คุณต้องสร้าง กฎที่ระบุการสื่อสารที่อนุญาต เพื่อความปลอดภัยเพิ่มขึ้น มีกฎเดียวที่อนุญาตให้สื่อสารระหว่าง VLANs ทั้งหมดบนระบบ แต่ละการเชื่อมต่อที่ได้รับอนุญาตต้องมีกฎของตัวเอง แม้ว่าแต่ละกฎที่เปิดใช้งานจะอนุญาตให้มีการสื่อสารทั้งสองทิศทาง สำหรับเป้าหมายที่ระบุ

เนื่องจากการสร้างกฎถูกสร้างขึ้นในอินเตอร์เฟส Virtual I/O Server (VIOS) ข้อมูลเพิ่มเติมเกี่ยวกับคำสั่งจะมีอยู่ในชุดหัวข้อ VIOS ใน Power Systems Hardware Information Center

เพื่อสร้างกฎ ให้ดำเนินการขั้นตอนต่อไปนี้:

1. เปิดอินเตอร์เฟสบรรทัดคำสั่ง VIOS
2. เริ่มต้นไดร์เวอร์ SVM โดยการป้อนคำสั่งต่อไปนี้:

   ```
   mksvm
   ```

3. สตาร์ท Trusted Firewall โดยการป้อนคำสั่งสตาร์ท:

   ```
   vlantfw -s
   ```

4. เพื่อแสดง LPAR IP และ MAC แอดเดรสที่รู้จักทั้งหมด ให้ป้อนคำสั่งต่อไปนี้:

   ```
   vlantfw -d
   ```

   คุณต้องมี IP และ MAC แอดเดรสของโลจิคัลพาร์ติชัน (LPARs) ที่ คุณสร้างกฎ
5. สร้างกฎตัวกรองเพื่ออนุญาตให้มีการสื่อสารระหว่างสอง LPARs (LPAR1 และ LPAR2) โดยการป้อนหนึ่งในคำสั่งต่อไปนี้:
   - `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`

   หมายเหตุ: หนึ่งกฎตัวกรองจะอนุญาตให้สื่อสารได้ทั้งสองทิศทาง โดยดีฟอลต์ขึ้นอยู่กับรายการพอร์ตและโปรโตคอล ตัวอย่างเช่น คุณ สามารถเปิดใช้ Telnet สำหรับ LPAR1 ไปยัง LPAR2 โดยการรันคำสั่งต่อไปนี้:

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

   ```
   mkvfilt -u
   ```

หมายเหตุ: ขั้นตอนนี้จะเปิดใช้กฎนี้ และกฎตัวกรองใดๆ ที่มีอยู่บนระบบ

ตัวอย่างเพิ่มเติม

ตัวอย่างต่อไปนี้ แสดงกฎตัวกรองอื่นๆ บางกฎที่คุณสามารถสร้างโดยการใช้ Trusted Firewall

- เพื่ออนุญาตให้ Secure Shell สื่อสารจาก LPAR บน VLAN 100 ไปยัง LPAR บน VLAN 200 ให้ป้อนคำสั่งต่อไปนี้:

  ```
  genvfilt -v4 -a P -z 100 -Z 200 -o any -p 0 -O eq -P 22 -c tcp
  ```
- เพื่ออนุญาตให้มีทราฟฟิกระหว่างพอร์ตทั้งหมดคือ 0 – 499 ให้ป้อนคำสั่ง ต่อไปนี้:

  ```
  genvfilt -v4 -a P -z 100 -z 200 -o lt -p 500 -O lt -P 500 -c tcp
  ```
- เพื่ออนุญาตให้มีทราฟฟิก TCP ทั้งหมดระหว่าง LPARs ให้ป้อนคำสั่ง ต่อไปนี้:

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

  หากคุณไม่ได้ระบุพอร์ตใดๆ หรือพอร์ตในการดำเนินการทราฟฟิกจะสามารถ ใช้พอร์ตทั้งหมด
- เพื่ออนุญาตให้ Internet Control Message Protocol ส่งข้อความระหว่าง LPARs, ให้ป้อนคำสั่งต่อไปนี้:

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

หลักการที่เกี่ยวข้อง:

"การปิดใช้งานกฎ"

คุณสามารถปิดใช้งานกฎที่เปิดใช้การกำหนดเส้นทางข้าม VLAN ในคุณลักษณะ Trusted Firewall

สิ่งอ้างอิงที่เกี่ยวข้อง:

"คำสั่ง genvfilt" ในหน้า 37

"คำสั่ง mkvfilt" ในหน้า 39

"คำสั่ง vlantfw" ในหน้า 51

ข้อมูลที่เกี่ยวข้อง:


Virtual I/O Server (VIOS)

การปิดใช้งานกฎ

คุณสามารถปิดใช้งานกฎที่เปิดใช้การกำหนดเส้นทางข้าม VLAN ในคุณลักษณะ Trusted Firewall

เนื่องจากกฎถูกปิดใช้งานในอินเตอร์เฟส Virtual I/O Server (VIOS) ข้อมูลเพิ่มเติมเกี่ยวกับคำสั่งและกระบวนการจะมีอยู่ในชุดหัวข้อ VIOS ใน Power Systems Hardware Information Center

เพื่อปิดใช้งานกฎ ให้ดำเนินการขั้นตอนต่อไปนี้:

1. เปิดอินเตอร์เฟสบรรทัดคำสั่ง VIOS
2. เพื่อแสดงกฎตัวกรองที่เปิดใช้งานทั้งหมด ให้ป้อน คำสั่งต่อไปนี้:

   ```
   lsvfilt -a
   ```

   คุณสามารถข้าม แฟล็ก **-a** เพื่อแสดงกฎตัวกรองทั้งหมด ที่จัดเก็บไว้ใน Object Data Manager
3. จดบันทึกหมายเลขประจำตัวสำหรับกฎ ตัวกรองที่คุณปิดใช้งาน สำหรับตัวอย่างนี้ หมายเลขประจำตัว ของกฎตัวกรองคือ 23
4. ปิดใช้งานกฎตัวกรองหมายเลข 23 เมื่อมีการใช้ในเคอร์เนลโดยการป้อน คำสั่งต่อไปนี้:

   ```
   rmvfilt -n 23
   ```

   เพื่อปิดใช้งาน กฎตัวกรองทั้งหมดในเคอร์เนล ให้ป้อนคำสั่งต่อไปนี้:

   ```
   rmvfilt -n all
   ```

หลักการที่เกี่ยวข้อง:

"การสร้างกฎ" ในหน้า 16
คุณสามารถสร้างกฎเพื่อเปิดใช้การกำหนดเส้นทาง Trusted Firewall ข้าม VLAN

สิ่งอ้างอิงที่เกี่ยวข้อง:

"คำสั่ง lsvfilt" ในหน้า 39

"คำสั่ง rmvfilt" ในหน้า 50

Trusted Logging

PowerVM® Trusted Logging จะทำให้ AIX LPAR เขียนไปยังล็อกไฟล์ที่ ถูกจัดเก็บไว้บน Virtual I/O Server (VIOS) ที่ต่อพ่วง ข้อมูล ถูกส่งไปยัง VIOS โดยตรง ผ่าน Hypervisor และไม่ต้องมีการเชื่อมต่อเครือข่ายระหว่าง LPAR ไคลเอ็นต์และ VIOS.

ล็อกเสมือน

ผู้ดูแลระบบ Virtual I/O Server (VIOS) จะสร้างและจัดการล็อกไฟล์ และ จะถูกแสดงในระบบปฏิบัติการ AIX เป็นอุปกรณ์บันทึกเสมือนในไดเร็กทอรี /dev คล้ายกับดิสก์เสมือน หรืออ็อฟติคัลมีเดียเสมือน

การจัดเก็บล็อกไฟล์เป็นล็อกเสมือนจะเพิ่มระดับของความไว้วางใจ ในเร็กคอร์ดเนื่องจากไม่สามารถเปลี่ยนแปลงโดยผู้ใช้ทีมีสิทธิ์ รูทบนไคลเอ็นต์ LPAR ที่สร้างขึ้น สามารถต่อพ่วงอุปกรณ์ล็อกเสมือนได้หลายอุปกรณ์ กับไคลเอ็นต์ LPAR เดียวกันและแต่ละล็อกจะเป็นไฟล์ที่ต่างกันในไดเร็กทอรี /dev

Trusted Logging ทำให้ข้อมูลล็อกจากหลายไคลเอ็นต์ LPAR ถูกรวบรวมเข้าใน ระบบไฟล์เดียว ซึ่งสามารถเข้าถึงได้จาก VIOS ดังนั้น VIOS จะมีเพียงตำแหน่งเดียวบนระบบสำหรับการจัดเก็บและวิเคราะห์ล็อก ผู้ดูแลระบบ LPAR ไคลเอ็นต์ สามารถกำหนดค่าคอนฟิกแอ็พพลิเคชันและระบบปฏิบัติการ AIX เพื่อเขียนข้อมูลไปยังอุปกรณ์บันทึกล็อกเสมือน ซึ่งจะคล้ายกับการเขียนข้อมูลไปยังโลคัลไฟล์ ระบบย่อย AIX Audit สามารถถูกกำหนดค่าคอนฟิก เพื่อบันทึกการตรวจสอบโดยตรงไปยังล็อกเสมือน และเซอร์วิส AIX อื่นๆ เช่น syslog จะทำงานร่วมกับ คอนฟิกูเรชันที่มีอยู่เพื่อบันทึกข้อมูลไปยังล็อกเสมือน

เพื่อกำหนดค่าคอนฟิกล็อกเสมือน ผู้ดูแลระบบ VIOS ต้องระบุชื่อสำหรับล็อกเสมือน ซึ่งมีองค์ประกอบที่แยกจากกัน ต่อไปนี้:

- ชื่อไคลเอ็นต์
- ชื่อล็อก

ชื่อของทั้งสององค์ประกอบสามารถกำหนดโดยผู้ดูแลระบบ VIOS เป็นค่าใดๆ แต่โดยปกติชื่อไคลเอ็นต์จะเป็นชื่อเดียวกันสำหรับล็อก เสมือนทั้งหมดที่ต่อพ่วงกับ LPAR ที่กำหนด (ตัวอย่างเช่น ชื่อโฮสต์ของ LPAR) ชื่อล็อก จะถูกใช้เพื่อระบุวัตถุประสงค์ของล็อก (ตัวอย่างเช่น การตรวจสอบ หรือ syslog)

บน AIX LPAR อุปกรณ์ล็อกเสมือนแต่ละอุปกรณ์ จะแสดงเป็นสองไฟล์ที่ทำงานได้เทียบเท่ากันในระบบไฟล์ /dev ไฟล์แรกจะถูกตั้งชื่อต่อจากอุปกรณ์ ตัวอย่างเช่น /dev/vlog0 และไฟล์ที่สองจะถูกตั้งชื่อด้วยคำนำหน้า vl และตามด้วยชื่อล็อกและหมายเลข อุปกรณ์ ตัวอย่างเช่น หากอุปกรณ์ล็อกเสมือน vlog0 มี audit เป็นชื่อล็อก จะแสดงในระบบไฟล์ /dev ทั้ง vlog0 และ vlaudit0

ข้อมูลที่เกี่ยวข้อง:

การสร้างล็อกเสมือน

การตรวจจับอุปกรณ์บันทึกเสมือน

หลังจากผู้ดูแลระบบ VIOS มีการสร้างอุปกรณ์บันทึกเสมือน และต่อพ่วงเข้ากับไคลเอ็นต์ LPAR ต้องรีเฟรชคอนฟิกูเรชันอุปกรณ์ LPAR ของไคลเอ็นต์เพื่อให้สามารถมองเห็นอุปกรณ์

ผู้ดูแลระบบ LPAR ไคลเอ็นต์ จะรีเฟรชการตั้งค่าโดยการใช้หนึ่งในวิธีการต่อไปนี้:

- การรีบูตไคลเอ็นต์ LPAR
- การรันคำสั่ง **cfgmgr**

รันคำสั่ง **lsdev** เพื่อแสดงอุปกรณ์บันทึก เสมือน อุปกรณ์จะนำหน้าด้วย `vlog` โดย ดีฟอลต์ ตัวอย่างของเอาท์พุทคำสั่ง **lsdev** บน AIX LPAR ที่มีสองอุปกรณ์บันทึกเสมือน จะเป็นดังต่อไปนี้:

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

ตรวจสอบคุณสมบัติของอุปกรณ์บันทึกเสมือนแต่ละตัวโดยใช้ คำสั่ง `lsattr -El <device name>` ซึ่งจะสร้างเอาท์พุทที่คล้ายกับต่อไปนี้ :

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

เอาท์พุทนี้จะแสดงชื่อไคลเอ็นต์, ชื่ออุปกรณ์และ ปริมาณข้อมูลล็อกที่ VIOS สามารถจัดเก็บ

บันทึกเสมือนจะจัดเก็บข้อมูลล็อกสองประเภท คือ:

- ข้อมูลล็อก: ข้อมูลล็อกล์ที่ยังไม่ได้ผ่านกรรมวิธีใดๆที่สร้างขึ้นโดยแอ็พพลิเคชันบน AIX LPAR
- ข้อมูลสถานะ: ข้อมูลจะเกี่ยวกับเมื่ออุปกรณ์ถูกกำหนดคอนฟิก เปิด, ปิด และการดำเนินการอื่นๆ ที่ใช้เพื่อวิเคราะห์กิจกรรม ล็อก

ผู้ดูแลระบบ VIOS ระบุจำนวนของ **ข้อมูลล็อก** และ **ข้อมูลสถานะ** ที่สามารถจัดเก็บสำหรับไฟล์ล็อกเสมือนแต่ละไฟล์ และจำนวน ที่ระบุโดยแอ็ตทริบิวต์ `max_log_size` และ `max_state_size` เมื่อจำนวนข้อมูลที่จัดเก็บเกินกว่าขีดจำกัดที่ระบุไว้ ข้อมูลที่บันทึกไว้ก่อนหน้าจะถูกเขียนทับ ผู้ดูแลระบบ VIOS ต้องแน่ใจว่าข้อมูลล็อกมีการรวบรวมและจัดเก็บอยู่เสมอ เพื่อเก็บรักษาล็อกไว้

การติดตั้ง Trusted Logging

คุณสามารถติดตั้งคุณลักษณะ PowerSC Trusted Logging โดยใช้อินเตอร์เฟสบรรทัดคำสั่ง หรือเครื่องมือ SMIT

| ข้อกำหนดเบื้องต้นสำหรับการติดตั้ง Trusted Logging คือต้องมี VIOS 2.2.1.0 หรือใหม่กว่า และ IBM AIX 6 ที่มีเทคโนโลยี
| ระดับ 7 หรือ IBM AIX 7 ที่มีเทคโนโลยีระดับ 1

| ชื่อไฟล์สำหรับการติดตั้งคุณลักษณะ Trusted Logging คือ `powerscStd.vlog` ซึ่งจะรวมอยู่ในซีดีการติดตั้ง PowerSC
| Standard Edition

| เพื่อติดตั้งฟังก์ชัน Trusted Logging :
| 1. ตรวจสอบให้แน่ใจว่าคุณรัน VIOS เวอร์ชัน 2.2.1.0 หรือใหม่กว่า
| 2. ใส่ซีดีการติดตั้ง PowerSC หรือดาวน์โหลดอิมเมจของซีดีการติดตั้ง
| 3. ใช้คำสั่ง **installp** หรือเครื่องมือ SMIT เพื่อติดตั้ง fileset ของ `powerscStd.vlog`
| **ข้อมูลที่เกี่ยวข้อง**:
| “การติดตั้ง PowerSC Standard Edition 1.1.3” ในหน้า 3
| คุณต้องติดตั้ง fileset สำหรับแต่ละฟังก์ชันเฉพาะของ PowerSC Standard Edition

การกำหนดค่าคอนฟิก Trusted Logging

ศึกษาขั้นตอนเพื่อกำหนดค่าคอนฟิก Trusted Logging บนระบบย่อย AIX Audit และ syslog

การกำหนดค่าคอนฟิกระบบย่อย AIX Audit

สามารถกำหนดค่าคอนฟิกระบบย่อย AIX Audit เพื่อเขียนข้อมูลไบนารีไปยังอุปกรณ์บันทึกล็อกเสมือน นอกเหนือจากการเขียนล็อกไปยังระบบไฟล์แบบโลคัล

หมายเหตุ: ก่อนที่คุณจะกำหนดค่าคอนฟิกระบบย่อย AIX Audit คุณต้องดำเนินการขั้นตอนใน “การตรวจจับอุปกรณ์บันทึกเสมือน” ในหน้า 20

เพื่อกำหนดค่าคอนฟิกระบบย่อย AIX Audit ให้ดำเนินการขั้นตอนต่อไปนี้:

1. กำหนดค่าคอนฟิกระบบย่อย AIX Audit ไปยังข้อมูลล็อกในโหมดไบนารี (`auditbin`)
2. เปิดใช้งาน Trusted Logging สำหรับการตรวจสอบ AIX โดยการแก้ไขไฟล์คอนฟิกูเรชัน `/etc/security/audit/config`
3. เพิ่มพารามิเตอร์ `virtual_log = /dev/vlog0` ไปยัง `bin:` stanza

   หมายเหตุ: คำแนะนำจะสามารถใช้ได้หากผู้ดูและระบบ LPAR ต้องการเขียนข้อมูล `auditbin` ไปยัง `/dev/vlog0`
4. รีสตาร์ทระบบย่อย AIX Audit ตามลำดับต่อไปนี้:

```
audit shutdown
audit start
```

เร็กคอร์ดการแก้ไขจะถูกเขียนไปยัง Virtual I/O Server (VIOS) ผ่าน อุปกรณ์บันทึกล็อกเสมือนที่ระบุนอกเหนือจากการเขียนไปยัง ระบบไฟล์แบบโลคัล ล็อกจะถูกเก็บอยู่ภายใต้การควบคุมของพารามิเตอร์ `bin1` และ `bin2` ที่มีอยู่ใน `bin:` stanza ของไฟล์คอนฟิกูเรชัน `/etc/security/audit/config`

ข้อมูลที่เกี่ยวข้อง:

ระบบย่อยการตรวจสอบ

การกำหนดค่าคอนฟิก syslog

สามารถกำหนดค่าคอนฟิก Syslog เพื่อเขียนข้อความไปยังอุปกรณ์บันทึกล็อกเสมือน โดยการเพิ่มกฎไปยังไฟล์ /etc/syslog.conf

หมายเหตุ: ก่อนที่คุณจะกำหนดค่าคอนฟิกไฟล์ /etc/syslog.conf คุณต้องดำเนินการขั้นตอนใน “การตรวจจับอุปกรณ์บันทึกเสมือน” ในหน้า 20

คุณสามารถแก้ไขไฟล์ /etc/syslog.conf ให้ตรง กับข้อความล็อก ซึ่งจะขึ้นกับเกณฑ์ต่อไปนี้:

- แฟซิลิตี้
- ระดับของลำดับความสำคัญ

เพื่อใช้ล็อกเสมือนสำหรับข้อความ syslog ต้องกำหนดค่าคอนฟิกไฟล์ /etc/syslog.conf ด้วยกฎเพื่อเขียนข้อความที่ต้องการ ไปยังล็อกเสมือนที่เหมาะสมในไดเร็กทอรี /dev

ตัวอย่างเช่น เพื่อส่งข้อความระดับการดีบักที่สร้างขึ้นโดย แฟซิลิตี้ใดๆ ไปยังล็อกเสมือน vlog0 ให้เพิ่มบรรทัดต่อไปนี้ ไปยังไฟล์ /etc/syslog.conf :

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

หมายเหตุ: อย่าใช้แฟซิลิตี้การหมุนเวียนล็อกที่มีอยู่ใน syslogd daemon สำหรับคำสั่งใดๆ ที่เขียน ข้อมูลไปยังล็อกเสมือน ไฟล์ในระบบไฟล์ /dev ไม่ใช้ไฟล์ทั่วไป และไม่สามารถลบหรือเปลี่ยนชื่อได้ ผู้ดูแลระบบ VIOS ต้องกำหนดค่าคอนฟิกการหมุนเวียนล็อกเสมือนภายใน VIOS

ต้องรีสตาร์ท syslogd daemon หลังจาก กำหนดค่าคอนฟิกโดยใช้คำสั่งต่อไปนี้:

```
refresh -s syslogd
```

ข้อมูลที่เกี่ยวข้อง:

syslogd Daemon

การเขียนข้อมูลไปยังอุปกรณ์ล็อกเสมือน

ข้อมูลที่ไม่มีกฎเกณฑ์จะถูกเขียนไปยังอุปกรณ์ล็อกเสมือนโดยการเปิด ไฟล์ที่เหมาะสมในไดเร็กทอรี /dev และ เขียนข้อมูลไปยังไฟล์ สามารถเปิดล็อกเสมือนโดยหนึ่งกระบวนการ ในแต่ละครั้ง

ตัวอย่าง :

เพื่อเขียนข้อความไปยังอุปกรณ์ล็อกเสมือนโดยการใช้คำสั่ง **echo** ให้ป้อนคำสั่งต่อไปนี้:

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

เพื่อจัดเก็บไฟล์ไปยังอุปกรณ์ล็อกเสมือนโดยการใช้คำสั่ง **cat** ให้ป้อนคำสั่งต่อไปนี้:

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

ขนาด ของการเขียนแต่ละไฟล์สูงสุดจะถูกจำกัดที่ 32 KB และโปรแกรมที่ พยายามจะเขียนข้อมูลเพิ่มเติมในการเขียนหนึ่งครั้ง จะได้รับ ข้อผิดพลาด I/O (EIO) ยูทิลิตี้อินเตอร์เฟสบรรทัดคำสั่ง (CLI) เช่น คำสั่ง **cat** จะหยุดการถ่ายโอนที่การเขียน 32 KB โดยอัตโนมัติ

การจัดการ Trusted Network Connect และ Patch

Trusted Network Connect (TNC) เป็นส่วนหนึ่งของกลุ่มการคำนวณ ที่ไว้วางใจได้ (TCG) ที่มีข้อมูลจำเพาะในการตรวจสอบบูรณภาพของจุดสิ้นสุด TNC มีสถาปัตยกรรมโซลูชันแบบเปิดที่กำหนดไว้ที่ช่วยผู้ดูแลระบบ บังคับใช้นโยบายที่มีประสิทธิภาพในการควบคุมการเข้าถึงโครงสร้างพื้นฐานของเครือข่าย

แนวคิด Trusted Network Connect

ศึกษาเกี่ยวกับคอมโพเนนต์, การกำหนดค่าคอนฟิกการสื่อสารที่ปลอดภัย และระบบการจัดการแพตช์ของ Trusted Network Connect (TNC)

คอมโพเนนต์ของ Trusted Network Connect

ศึกษาเกี่ยวกับคอมโพเนนต์ของเฟรมเวิร์ก Trusted Network Connect (TNC)

โมเดล TNC จะประกอบด้วยคอมโพเนนต์ต่อไปนี้:

เซิร์ฟเวอร์ Trusted Network Connect:

เซิร์ฟเวอร์ Trusted Network Connect (TNC) จะระบุ ไคลเอ็นต์ที่เพิ่มไปยังเครือข่าย และเริ่มต้นการตรวจสอบ บนไคลเอ็นต์

ไคลเอ็นต์ TNC จะมีข้อมูลระดับ fileset ที่จำเป็น ในเซิร์ฟเวอร์สำหรับการตรวจสอบ เซิร์ฟเวอร์จะตรวจสอบว่า ไคลเอ็นต์อยู่ที่ระดับที่กำหนดค่าคอนฟิกไว้โดยผู้ดูแลระบบหรือไม่ หาก ไคลเอ็นต์ไม่เป็นไปตามมาตรฐาน เซิร์ฟเวอร์ TNC จะแจ้งเตือนผู้ดูแลระบบ เกี่ยวกับวิธีแก้ไขที่จำเป็น

เซิร์ฟเวอร์ TNC จะเริ่มต้นการตรวจสอบบนไคลเอ็นต์ที่ พยายามเข้าถึงเครือข่าย เซิร์ฟเวอร์ TNC จะโหลดชุดของ Integrity Measurement Verifiers (IMVs) ที่สามารถร้องขอการวัดบูรณภาพ จากไคลเอ็นต์ และตรวจสอบ AIX จะมี IMV ดีฟอลต์ ซึ่งตรวจสอบระดับ fileset และแพตช์ ที่ปลอดภัยของระบบ เซิร์ฟเวอร์ TNC คือเฟรมเวิร์กซึ่งโหลดและ จัดการโมดูล IMV หลายโมดูล สำหรับการตรวจสอบไคลเอ็นต์ จะใช้ IMVs เพื่อร้องขอข้อมูลจากไคลเอ็นต์ และตรวจสอบไคลเอ็นต์

การจัดการ Patch:

เซิร์ฟเวอร์ Trusted Network Connect (TNC) จะรวมเข้ากับ SUMA เพื่อให้มีโซลูชันการจัดการแพทช์

AIX SUMA จะดาวน์โหลด เซอร์วิสแพ็คล่าสุดและโปรแกรมแก้ไขที่ปลอดภัยที่มีอยู่ใน IBM ECC and Fix Central daemon การจัดการแพ็กทช์และ TNC จะใส่ข้อมูลที่อัพเดตล่าสุดไปยังเซิร์ฟเวอร์ TNC ซึ่ง ทำหน้าที่เป็น fileset พื้นฐานในการตรวจสอบไคลเอ็นต์

tncpmd daemon ต้องถูกกำหนดค่าคอนฟิก เพื่อจัดการการดาวน์โหลด Service Update Management Assistant (SUMA) และเพื่อใส่ข้อมูล fileset ไปยังเซิร์ฟเวอร์ TNC daemon นี้ต้อง ถูกโอสต์บนระบบที่เชื่อมต่อกับอินเตอร์เน็ตเพื่อให้สามารถ ดาวน์โหลดการอัพเดตโดยอัตโนมัติ เพื่อใช้เซิร์ฟเวอร์การจัดการแพตช์ TNC โดยไม่ต้องเชื่อมต่อกับอินเตอร์เน็ต คุณสามารถลงทะเบียนที่เก็บโปรแกรมแก้ไข ที่ผู้ใช้กำหนดกับเซิร์ฟเวอร์การจัดการแพตช์ TNC

หมายเหตุ: เซิร์ฟเวอร์ TNC และ **tncpmd** daemon สามารถโฮสต์อยู่บน ระบบเดียวกัน

ไคลเอ็นต์ Trusted Network Connect:

ไคลเอ็นต์ Trusted Network Connect (TNC) จะมีข้อมูล ที่จำเป็นสำหรับเซิร์ฟเวอร์ TNC สำหรับการตรวจสอบ

เซิร์ฟเวอร์จะตรวจสอบว่าไคลเอ็นต์อยู่ที่ระดับที่กำหนดค่าคอนฟิกไว้โดยผู้ดูแลระบบหรือไม่ หากไคลเอ็นต์ไม่เป็นไปตามมาตรฐาน เซิร์ฟเวอร์ TNC จะแจ้งเตือนผู้ดูแลระบบเกี่ยวกับการอัพเดตที่จำเป็น

ไคลเอ็นต์ TNC จะโหลด IMCs เมื่อเริ่มต้นการทำงานและใช้ IMCs เพื่อรวบรวม ข้อมูลที่จำเป็น

ตัวอ้าง IP ของ Trusted Network Connect:

เซิร์ฟเวอร์ Trusted Network Connect (TNC) สามารถเริ่มต้นการตรวจสอบ บนไคลเอ็นต์ที่เป็นส่วนหนึ่งของเครือข่ายได้โดยอัตโนมัติ ตัวอ้างอิง IP ที่รันบนพาร์ติชัน Virtual I/O Server (VIOS) ตรวจพบไคลเอ็นต์ใหม่ที่ให้บริการโดย VIOS และส่ง IP แอดเดรสไปยังเซิร์ฟเวอร์ TNC เซิร์ฟเวอร์ TNC จะตรวจสอบ ไคลเอ็นต์ตามนโยบายที่กำหนด

การสื่อสารที่ปลอดภัย Trusted Network Connect

การสื่อสาร Trusted Network Connect (TNC) daemons บน ช่องทางที่เข้ารหัสไว้ที่เปิดใช้งานโดย Transport Layer Security (TLS) หรือ Secure Sockets Layer (SSL)

การสื่อสารที่ปลอดภัยทำให้แน่ใจว่าข้อมูลและคำสั่ง ที่อยู่ในเครือข่ายจะได้รับการพิสูจน์ตัวตน และมีความปลอดภัย แต่ละระบบ ต้องมีใบรับรองและคีย์ของตัวเอง ซึ่งถูกสร้างขึ้นเมื่อ รันคำสั่งเริ่มต้นสำหรับคอมโพเนนต์ กระบวนการนี้ จะโปร่งใสอย่างสมบูรณ์ต่อผู้ดูแลระบบ และต้องการความเกี่ยวข้องจาก ผู้ดูแลระบบลดลง

เพื่อตรวจสอบไคลเอ็นต์ใหม่ ใบรับรองของไคลเอ็นต์ ต้องถูกอิมพอร์ตไปยังฐานข้อมูลของเซิร์ฟเวอร์ ใบรับรอง จะถูกทำเครื่องหมายเป็นไม่ไว้วางใจในตอนเริ่มแรก จากนั้นผู้ดูแลระบบจะใช้ คำสั่ง **psconf** เพื่อดูและทำเครื่องหมายใบรับรอง เป็นไว้วางใจได้โดยการป้อนคำสั่งต่อไปนี้:

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

เพื่อใช้คีย์และใบรับรองที่ต่างกัน คำสั่ง **psconf** จะมีอ็อพชันเพื่ออิมพอร์ตใบรับรอง

เพื่ออิมพอร์ตใบรับรองจากเซิร์ฟเวอร์ให้ป้อน คำสั่งต่อไปนี้:

```
psconf import  -S -k<key filename> -f<key filename>
```

เพื่ออิมพอร์ตใบรับรองจากไคลเอ็นต์ให้ป้อน คำสั่งต่อไปนี้:

```
psconf import -C -k<key filename> -f<key filename>
```

โปรโตคอล Trusted Network Connect

โปรโตคอล Trusted Network Connect (TNC) จะถูกใช้กับ เฟรมเวิร์ก TNC เพื่อรักษาบรูณภาพของเครือข่าย

TNC จะมีข้อมูลจำเพาะเพื่อตรวจสอบบูรณภาพของอุปกรณ์ปลายทาง อุปกรณ์ปลายทางที่ร้องขอการเข้าถึงจะถูกเข้าถึงตามการวัดค่า บูรณภาพของคอมโพเนนต์ที่สำคัญที่อาจมีผลกระทบกับสภาพแวดล้อม การทำงาน เฟรมเวิร์ก TNC จะทำให้ผู้ดูแลระบบสามารถมอนิเตอร์ บูรณภาพของระบบในเครือข่าย TNC จะถูกรวมเข้ากับ โครงสร้างพื้นฐานการกระจายแพตช์ AIX เพื่อสร้างโซลูชันการจัดการแพตช์ที่สมบูรณ์

ข้อกำหนดของ TNC ต้องสนองความต้องการของสถาปัตยกรรมระบบ AIX และ ตระกูล POWER® คอมโพเนนต์ของ TNC ถูกออกแบบมาเพื่อให้โซลูชันการจัดการแพตช์ ที่สมบูรณ์บนระบบปฏิบัติการ AIX การกำหนดค่าคอนฟิกนี้จะช่วยให้ผู้ดูแลระบบสามารถจัดการ การกำหนดค่าคอนฟิกซอฟต์แวร์บนการปรับใช้ AIX ได้อย่างมีประสิทธิภาพ โดยจะมีเครื่องมือเพื่อตรวจสอบ ระดับแพตช์ของระบบ และสร้างรายงานบนไคลเอ็นต์ที่ไม่ปฏิบัติตามมาตรฐาน นอกจากนี้ การจัดการแพตช์ยังทำให้กระบวนการดาวน์โหลดแพ็ก และการติดตั้งง่ายขึ้น

โมดูล IMC และ IMV

ไคลเอ็นต์ หรือเซิร์ฟเวอร์ Trusted Network Connect (TNC) ภายใน จะใช้โมดูล integrity measurement collector (IMC) และ integrity measurement verifier (IMV) สำหรับการตรวจสอบเซิร์ฟเวอร์

เฟรมเวิร์กนี้จะช่วยให้สามารถโหลดโมดูล IMC และ IMV ไปยังเซิร์ฟเวอร์และไคลเอ็นต์ได้หลายโมดูล โดมูลที่ดำเนินการตรวจสอบ ระบบปฏิบัติการ (OS) และระดับ fileset จะมาพร้อมกับ ระบบปฏิบัติการ AIX โดย ดีฟอลต์ เพื่อเข้าถึงโมดูลที่มาพร้อมกับระบบปฏิบัติการ AIX ให้ใช้หนึ่งในพาธ ต่อไปนี้:

- `/usr/lib/security/tnc/libfileset_imc.a`: รวบรวม ระดับ OS และข้อมูลเกี่ยวกับ fileset ที่ถูกติดตั้งจาก ระบบไคลเอ็นต์ และส่งไปยัง IMV (เซิร์ฟเวอร์ TNC) สำหรับการตรวจสอบ
- `/usr/lib/security/tnc/libfileset_imv.a`: ขอ ข้อมูลระดับ OS และ fileset จากไคลเอ็นต์และเปรียบเทียบ ข้อมูลพื้นฐาน และยังอัพเดตสถานะของ ไคลเอ็นต์ไปยังฐานข้อมูลของเซิร์ฟเวอร์ TNC เพื่อดูสถานะ ให้ป้อนคำสั่งต่อไปนี้:

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

สิ่งอ้างอิงที่เกี่ยวข้อง:

"คำสั่ง psconf" ในหน้า 44

การติดตั้ง Trusted Network Connect

การติดตั้งคอมโพเนนต์ของ Trusted Network Connect (TNC) ต้องการให้คุณดำเนินการบางขั้นตอน

เพื่อกำหนดคอนฟิกการตั้งค่าสำหรับการใช้คอมโพเนนต์ของ TNC ให้ดำเนินการ ขั้นตอนต่อไปนี้:

1. ระบุ IP แอดเดรสของระบบเพื่อตั้งค่าเซิร์ฟเวอร์ TNC , เซิร์ฟวอร์ Trusted Network Connect และ Patch Management (TNCPM) และ ตัวอ้างอิง TNC IP สำหรับ Virtual I/O Server (VIOS)

   หมายเหตุ: เซิร์ฟเวอร์ TNC ไม่สามารถกำหนดค่าคอนฟิกเป็นไคลเอ็นต์ TNC
2. ตั้งค่าเซิร์ฟเวอร์การจัดการการติดตั้งเครือข่าย (NIM) ระบบ ที่กำหนดค่าคอนฟิกเป็นเซิร์ฟเวอร์คือ NIM หลัก และ filesets ของ `sets:bos.sysmgt.nim.master` ต้องถูกติดตั้งบน ระบบไคลเอ็นต์
3. กำหนดค่าคอนฟิกเซิร์ฟเวอร์ TNCPM คอนฟิกูเรชันนี้สามารถตั้งค่าบน ระบบ NIM เซิร์ฟเวอร์ TNCPM จะใช้ SUMA เพื่อ ดาวน์โหลดแพตช์จากเว็บไซต์ IBM Fix Central และ ECC เพื่อดาวน์โหลดการอัพเดต ต้อง เชื่อมต่อระบบกับอินเตอร์ ป้อนคำสั่งต่อไปนี้เพื่อ กำหนดค่าคอนฟิกเซิร์ฟเวอร์ TNCPM :

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

   ตัวอย่าง:

   ```
   pmconf mktncpm pmport=20000 tncserver=1.1.1.1:10000
   ```
4. กำหนดค่าคอนฟิกนโยบายบนเซิร์ฟเวอร์ TNC เพื่อสร้างนโยบาย สำหรับการตรวจสอบไคลเอ็นต์ โปรดดู "การสร้างนโยบายสำหรับไคลเอ็นต์ Trusted Network Connect" ในหน้า 30

5. การกำหนดค่าคอนฟิกตัวอ้างอิง TNC IP บน VIOS การกำหนดค่าคอนฟิกนี้บน VIOS จะทริกเกอร์ การตรวจสอบบนไคลเอ็นต์ที่เชื่อมต่อกับเครือข่าย ป้อนคำสั่งต่อไปนี้เพื่อกำหนดค่าคอนฟิกตัวอ้างอิง:

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

   ตัวอย่าง :

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

   หมายเหตุ: ค่าของพอร์ตเซิร์ฟเวอร์ และพอร์ต TNC ซึ่งเป็นพอร์ต ไคลเอ็นต์ ต้องเป็นค่าเดียวกัน

6. กำหนดค่าคอนฟิกไคลเอ็นต์โดยการใช้คำสั่งต่อไปนี้:

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

   ตัวอย่าง:

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

สิ่งอ้างอิงที่เกี่ยวข้อง:

"คำสั่ง psconf" ในหน้า 44

ข้อมูลที่เกี่ยวข้อง:

"การติดตั้ง PowerSC Standard Edition 1.1.3" ในหน้า 3

คุณต้องติดตั้ง fileset สำหรับแต่ละฟังก์ชันเฉพาะของ PowerSC Standard Edition

การติดตั้งด้วย NIM

IBM Fix Central

Passport Advantage Online Help Center

การกำหนดค่าคอนฟิกการจัดการ Trusted Network Connect และ Patch

คุณต้องกำหนดค่าคอนฟิก Trusted Network Connect (TNC) เป็น daemon การจัดการแพทช์ เซิร์ฟเวอร์ TNC จะรวมเข้ากับ SUMA เพื่อให้มีโซลูชันการจัดการแพทช์ที่ครอบคลุม

การกำหนดค่าคอนฟิกเซิร์ฟเวอร์ Trusted Network Connect

ศึกษาขั้นตอนเพื่อกำหนดค่าคอนฟิกเซิร์ฟเวอร์ TNC

เพื่อกำหนดค่าคอนฟิกเซิร์ฟเวอร์ TNC ไฟล์ `/etc/tnccs.conf` ต้องมีค่าดังต่อไปนี้:

```
component = SERVER
```

เพื่อกำหนดค่าคอนฟิกอระบบเป็นเซิร์ฟเวอร์ให้ป้อนคำสั่งต่อไปนี้:

```
psconf mkserver tncport=<port> pmserver=<ip|hostname[,ip2|hostname2..]:port>
[recheck_interval=<time in mins>]
```

ตัวอย่าง:

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

| **หมายเหตุ:** พอร์ต tncport และพอร์ต pmserver ต้องมีการกำหนดค่า ที่ต่างกัน และหากค่าของพารามิเตอร์
| recheck_interval ไม่ถูกระบุจะใช้ค่าดีฟอลต์ ซึ่งเท่ากับ 1440 นาที

ค่าพอร์ตดีฟอลต์คือ 42830 นาทีจะถูกใช้ สำหรับพอร์ต tncport และค่าดีฟอลต์เท่ากับ 38240 นาทีจะถูกใช้สำหรับพอร์ต pmserver

สิ่งอ้างอิงที่เกี่ยวข้อง:

"คำสั่ง psconf" ในหน้า 44

การกำหนดค่าคอนฟิกไคลเอ็นต์ Trusted Network Connect

ศึกษาขั้นตอนเพื่อกำหนดค่าคอนฟิกไคลเอ็นต์ Trusted Network Connect (TNC) และตั้งค่าคอนฟิกูเรชันที่จำเป็นสำหรับการติดตั้ง

เพื่อกำหนดค่าคอนฟิกไคลเอ็นต์ TNC ไฟล์ /etc/tnccs.conf ต้องมีค่าดังต่อไปนี้ :

```
component = CLIENT
```

เพื่อกำหนดค่าคอนฟิกระบบเป็นไคลเอ็นต์ ให้ป้อนคำสั่งต่อไปนี้:

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

ตัวอย่าง:

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

หมายเหตุ: ค่าพอร์ตของเซิร์ฟเวอร์ และ tncport ที่เป็นพอร์ตไคลเอ็นต์ต้องเป็นค่าเดียวกัน

สิ่งอ้างอิงที่เกี่ยวข้อง:

"คำสั่ง psconf" ในหน้า 44

การกำหนดค่าคอนฟิกเซิร์ฟเวอร์การจัดการแพทช์

ศึกษาขั้นตอนเพื่อกำหนดค่าคอนฟิกระบบเป็นเซิร์ฟเวอร์การจัดการ แพทช์

เซิร์ฟเวอร์การจัดการแพทช์ Trusted Network Connect (TNC) ต้อง ถูกกำหนดค่าคอนฟิกบนเซิร์ฟเวอร์ Network Installation Management (NIM) เพื่อที่จะสามารถอัพเดตไคลเอ็นต์ TNC

| เพื่อเริ่มต้นที่เก็บโปรแกรมฟิกซ์สำหรับการจัดการแพตช์ TNC ให้ป้อนคำสั่งต่อไปนี้:

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

| ตัวอย่างของคำสั่ง **pmconf** มีดังนี้:

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

คำสั่ง **init** จะดาวน์โหลดเซอร์วิสแพ็ค ล่าสุดสำหรับแต่ละ Technology Level และทำให้พร้อมใช้งานสำหรับเซิร์ฟเวอร์ TNC เซอร์วิสแพ็คที่อัพเดตจะทำให้เซิร์ฟเวอร์ TNC สามารถรันการตรวจสอบ ไคลเอ็นต์ TNC พื้นฐาน และเพื่อให้เซิร์ฟเวอร์การจัดการแพตช์ TNC ติดตั้งการอัพเดตไคลเอ็นต์ TNC ระบุแฟล็ก **-A** เพื่อยอมรับข้อตกลงการใช้ซอฟต์แวร์ทั้งหมดเมื่อรันการอัพเดตไคลเอ็นต์โดยดีฟอลต์ ที่เก็บโปรแกรมแก้ไขที่ดาวน์โหลดโดยเซิร์ฟเวอร์การจัดการแพตช์ TNC จะอยู่ในไฟล์ /var/tnc/tncpm/fix_repository ใช้แฟล็ก **-P** เพื่อระบุไดเร็กทอรี ที่ต่างกัน

เพื่อเปิดใช้ IBM Security Advisory และดาวน์โหลดโปรแกรมแก้ไขปัญหาระหว่างเวอร์ชัน คุณสามารถระบุ ระยะเวลาการแก้ไขปัญหาระหว่างเวอร์ชัน คุณลักษณะนี้จะมีการแจ้งเตือนโดยอัตโนมัติ ของโปรแกรมแก้ไขปัญหาระหว่างเวอร์ชันที่มีความปลอดภัยที่เผยแพร่ใหม่ และตัวระบุ Common Vulnerabilities and Exposures (CVE) ที่เกี่ยวข้อง แอดไวเซอร์ที่ปลอดภัย และโปรแกรมแก้ไขปัญหา ระหว่างเวอร์ชันทั้งหมดจะถูกตรวจสอบก่อนที่จะลงทะเบียนกับ TNC คีย์พับลิกที่มีช่องโหว่ของ IBM AIX ซึ่งจำเป็นในการดาวน์โหลด โปรแกรมแก้ไขปัญหาระหว่างเวอร์ชันโดยอัตโนมัติ จะมีอยู่ที่เว็บไซต์ IBM AIX Security การดาวน์โหลดเซอร์วิสแพ็ค และโปรแกรมแก้ไขปัญหาระหว่างเวอร์ชันโดยอัตโนมัติ จะถูกปิดใช้งานจากการตั้งค่าช่วงเวลาการดาวน์โหลด และช่วงเวลาการแก้ไขปัญหาระหว่างเวอร์ชัน ให้เป็น 0

คุณยังสามารถอัพเดตเซอร์วิสแพ็ก และโปรแกรมแก้ไขปัญหาระหว่างเวอร์ชันด้วยตัวเอง เพื่อลงทะเบียน IBM Security Advisory ด้วยตัวเองพร้อมกับโปรแกรมแก้ไขปัญหาระหว่างเวอร์ชันที่สอดคล้องกัน ให้ป้อนคำสั่ง ต่อไปนี้:

```
pmconf add -y <advisory file> -v <signature file>  -e <ifix tar file>
```

เพื่อลงทะเบียนโปรแกรมแก้ไขปัญหาระหว่างเวอร์ชันแบบสแตนอะโลนด้วยตัวเอง ให้ป้อนคำสั่งต่อไปนี้:

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

เพื่อลงทะเบียน Technology Level ใหม่และเพื่อดาวน์โหลดเซอร์วิสแพ็ค ล่าสุด ให้ป้อนคำสั่งต่อไปนี้:

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

เพื่อดาวน์โหลดเซอร์วิสแพ็คที่ไม่ใช่เวอร์ชันปัจจุบันล่าสุด หรือเพื่อดาวน์โหลด Technology Level ที่จะใช้สำหรับการตรวจสอบและ อัพเดตไคลเอ็นต์ ให้ป้อนคำสั่งต่อไปนี้:

```
pmconf add -l <TL list> -d
pmconf add -s <SP List>
```

เพื่อลงทะเบียนเซอร์วิสแพ็ค หรือที่เก็บโปรแกรมแก้ไขของ Technology Level ที่ มีอยู่บนระบบ ให้ป้อนคำสั่งต่อไปนี้:

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

เพื่อกำหนดค่าคอนฟิกระบบที่จะทำหน้าที่เป็นเซิร์ฟเวอร์การจัดการแพตช์ ให้ป้อน คำสั่งต่อไปนี้:

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

ตัวอย่างของคำสั่งนี้มีดังนี้:

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

เซิร์ฟเวอร์การจัดการแพตช์ TNC จะสนับสนุนการจัดการ Authorized Problem Analysis Reports (APARs) ที่มีความปลอดภัยตลอดเวลา ป้อน คำสั่งต่อไปนี้เพื่อกำหนดค่าคอนฟิกการจัดการแพตช์ TNC เพื่อจัดการ ชนิดอื่นๆ ของ APAR:

```
pmconf add -t <APAR_type_list>
```

ในตัวอย่างก่อนหน้า <APAR_type_list> คือรายการที่คั่นด้วยเครื่องหมายคอมม่า ที่มีชนิดของ APAR ต่อไปนี้:

- HIPER
- PE
- Enhancement

เซิร์ฟเวอร์การจัดการแพตช์ TNC สนับสนุน **syslog** สำหรับการดาวน์โหลดเซอร์วิสแพ็ค Technology Level และการอัพเดตไคลเอ็นต์ แฟซิลิตี้คือ `user` และลำดับความสำคัญคือ `info` ตัวอย่างนี้คือ `user.info`

เซิร์ฟเวอร์การจัดการแพตช์ TNC ยังเก็บรักษาล็อกที่มีการอัพเดต ไคลเอ็นต์ทั้งหมดในไดเร็กทอรี `/var/tnc/tncpm/log/update/<ip>/<timestamp>`

สิ่งอ้างอิงที่เกี่ยวข้อง:

"คำสั่ง psconf" ในหน้า 44

ข้อมูลที่เกี่ยวข้อง:

IBM AIX Security

การกำหนดค่าคอนฟิกการแจ้งเตือนทางอีเมลของเซิร์ฟเวอร์ Trusted Network Connect

ศึกษาขั้นตอนเพื่อกำหนดค่าคอนฟิกการแจ้งเตือนทางอีเมลสำหรับ เซิร์ฟเวอร์ Trusted Network Connect (TNC)

เซิร์ฟเวอร์ TNC จะดูระดับแพทช์ของไคลเอ็นต์และหากเซิร์ฟเวอร์ TNC พบว่าไคลเอ็นต์ไม่ปฏิบัติตามมาตรฐาน จะส่งอีเมลไปยัง ผู้ดูแลระบบถึงผลลัพธ์และวิธีแก้ไขที่จำเป็น

| เพื่อกำหนดค่าคอนฟิกอีเมลแอดเดรสของผู้ดูแลระบบ ให้ป้อนคำสั่งต่อไปนี้:

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

| ตัวอย่าง :

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

| ในตัวอย่างก่อนหน้า อีเมลสำหรับกลุ่ม IP *vayugrp1* และ *vayugrp2* จะถูกส่งไปยังอีเมลแอดเดรส abc@ibm.com

| เพื่อส่งอีเมลไปยังอีเมลแอดเดรสแบบโกลบอลสำหรับ กลุ่ม IP ที่ไม่มีอีเมลแอดเดรสที่กำหนดไปยังกลุ่ม ให้ป้อน คำสั่งต่อไปนี้:

```
| psconf add -e <mailaddress>
```

| ตัวอย่าง :

```
| psconf add -e abc@ibm.com
```

| ใน ตัวอย่างก่อนหน้า หากกลุ่ม IP ไม่มี อีเมลแอดเดรสที่กำหนดไปยังกลุ่ม เมล์จะถูกไปยังอีเมลแอดเดรส abc@ibm.com ซึ่งทำหน้าที่เป็นอีเมลแอดเดรสโกลบอล

สิ่งอ้างอิงที่เกี่ยวข้อง:

"คำสั่ง psconf" ในหน้า 44

การกำหนดค่าคอนฟิกตัวอ้างอิง IP บน VIOS

ศึกษาวิธีในการกำหนดค่าคอนฟิกตัวอ้างอิง IP บน Virtual I/O Server (VIOS) เพื่อเริ่มการตรวจสอบ โดยอัตโนมัติ

หมายเหตุ: คุณต้องกำหนดค่าคอนฟิกส่วนขยายเคอร์เนล SVM บน Virtual I/O Server (VIOS) ก่อนการกำหนดค่าคอนฟิกตัวอ้างอิง IP

เพื่อกำหนดค่าคอนฟิก TNC IP Referrer ไฟล์คอนฟิกูเรชัน `/etc/tnccs.conf` ต้องมีการตั้งค่าที่คล้ายกับต่อไปนี้ `component = IPREF`

| คุณสามารถกำหนดค่าคอนฟิกระบบเป็นไคลเอ็นต์โดยการป้อนคำสั่ง ต่อไปนี้:

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

| ตัวอย่าง :

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

| ค่าของพอร์ต `tncserver` และ `tncport`, ซึ่งเป็นพอร์ตไคลเอ็นต์ต้องเป็นค่าเดียวกัน

สิ่งอ้างอิงที่เกี่ยวข้อง:

"คำสั่ง psconf" ในหน้า 44

การบริหารจัดการ Trusted Network Connect และ Patch

ศึกษาวิธีจัดการ Trusted Network Connect (TNC) เพื่อใช้ งานต่างๆ เช่น การเพิ่มไคลเอ็นต์ นโยบาย ล็อก ผลลัพธ์การตรวจสอบ การอัพเดตไคลเอ็นต์ และใบรับรองที่เกี่ยวข้องกับ TNC

การดูล็อกเซิร์ฟเวอร์ Trusted Network Connect

ศึกษาวิธีดูล็อกของเซิร์ฟเวอร์ Trusted Network Connect (TNC)

| เซิร์ฟเวอร์ TNC จะบันทึกผลลัพธ์การตรวจสอบของไคลเอ็นต์ ทั้งหมด เพื่อดูล็อก ให้รันคำสั่ง **psconf** :

| `psconf list -H -i <ip |ALL>`

| **สิ่งอ้างอิงที่เกี่ยวข้อง:**

"คำสั่ง psconf" ในหน้า 44

การสร้างนโยบายสำหรับไคลเอ็นต์ Trusted Network Connect

ศึกษาวิธีการตั้งค่านโยบายที่เชื่อมโยงกับไคลเอ็นต์ Trusted Network Connect (TNC)

| คอนโซล `psconf` จะมี อินเตอร์เฟสที่จำเป็นในการจัดการนโยบาย TNC แต่ละไคลเอ็นต์หรือกลุ่ม ของไคลเอ็นต์สามารถเชื่อม
| โยงกับนโยบาย

สามารถสร้างนโยบายต่อไปนี้:

- กลุ่ม Internet Protocol (IP) มีหลาย IP แอดเดรสของไคลเอ็นต์
- แต่ละ IP ของไคลเอ็นต์สามารถเป็นสมาชิกได้เพียงกลุ่มเดียว
- กลุ่ม IP จะเชื่อมโยงกับกลุ่มนโยบาย
- กลุ่มนโยบายจะมีประเภทของนโยบายที่ต่างกัน ตัวอย่างเช่น นโยบาย Fileset ที่ระบุว่าอะไรคือระดับของระบบปฏิบัติการของไคลเอ็นต์ (นั้นคือ รีลีส ระดับเทคโนโลยี และเซอร์วิสแพ็ค) สามารถมีโยบาย Fileset ได้หลายนโยบายในกลุ่มนโยบาย และไคลเอ็นต์ ที่อ้างถึงนโยบายนี้ต้องอยู่ที่ระดับที่ระบุไว้โดยหนึ่งใน นโยบาย Fileset

คำสั่งต่อไปนี้แสดงวิธีการสร้างกลุ่ม IP , กลุ่มนโยบาย และนโยบาย Fileset

| เพื่อสร้างกลุ่ม IP ให้ป้อนคำสั่งต่อไปนี้:

| psconf add -G <ipgrpname> ip=[±]<ip1,ip2,ip3 ...>

| ตัวอย่าง :

| psconf add -G myipgrp ip=1.1.1.1,2.2.2.2

| **หมายเหตุ:** สำหรับกลุ่ม ต้องระบุอย่างน้อยหนึ่ง IP ต้องแยกแต่ละ IPs ด้วยเครื่องหมายคอมม่า

| เพื่อสร้างนโยบาย fileset ให้ป้อนคำสั่งต่อไปนี้:

| psconf add -F <fspolicyname> <rel00-TL-SP>

| ตัวอย่าง:

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

| **หมายเหตุ:** ข้อมูลบิลด์ต้องอยู่ในรูปแบบ <rel00-TL-sp>

| เพื่อสร้างนโยบาย และเพื่อกำหนดกลุ่ม IP ให้ป้อน คำสั่งต่อไปนี้:

| psconf add -P <policyname> ipgroup=[±] <ipgrp1, ipgrp2 ...]

| ตัวอย่าง:

| psconf add -P mypol ipgroup=myipgrp,myipgrp1

เพื่อกำหนดนโยบาย fileset ให้กับนโยบาย ให้ป้อนคำสั่งต่อไปนี้:

```
psconf add -P <policyname> fspolicy=[±]<fspol1, fspol2 ...>
```

ตัวอย่าง:

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

หมายเหตุ: หากมีการระบุนโยบาย fileset หลายนโยบาย ระบบจะบังคับ ใช้นโยบายที่ตรงกันที่ดีที่สุดบนไคลเอ็นต์ ตัวอย่าง เช่น หากไคลเอ็นต์ อยู่บน 6100-02-01 และคุณระบุนโยบาย fileset เป็น 7100-03-04 และ 6100-02-03 ดังนั้น 6100-02-03 จะถูกบังคับใช้บนไคลเอ็นต์

สิ่งอ้างอิงที่เกี่ยวข้อง:

"คำสั่ง psconf" ในหน้า 44

การเริ่มต้นตรวจสอบไคลเอ็นต์ Trusted Network Connect

ศึกษาวิธีตรวจสอบไคลเอ็นต์ Trusted Network Connect (TNC)

ใช้หนึ่งในวิธีการต่อไปนี้สำหรับการตรวจสอบไคลเอ็นต์:

- daemon ของตัวอ้างอิง IP บน Virtual I/O Server (VIOS) จะส่งต่อ IP ของไคลเอ็นต์ไปยังเซิร์ฟเวอร์ TNC : ไคลเอ็นต์ LPAR ได้รับ IP และพยายาม ที่จะเข้าถึงเครือข่าย daemon ของตัวอ้างอิง IP บน VIOS ตรวจพบ IP แอดเดรสใหม่ และจะส่งต่อไปยังเซิร์ฟเวอร์ TNC : เซิร์ฟเวอร์ TNC จะเริ่มการตรวจสอบเมื่อได้รับ IP แอดเดรสใหม่
- เซิร์ฟเวอร์ TNC จะตรวจสอบไคลเอ็นต์เป็นระยะๆ : ผู้ดูแลระบบ สามารถเพิ่ม IP ของไคลเอ็นต์ที่จะถูกตรวจสอบในฐานข้อมูลนโยบาย TNC เซิร์ฟเวอร์ TNC จะตรวจสอบไคลเอ็นต์ที่อยู่ในฐานข้อมูล การตรวจสอบใหม่ จะเกิดขึ้นโดยอัตโนมัติในช่วงเวลาปกติด้วยการอ้างอิง ถึงค่าแอ็ตทริบิวต์ recheck_interval ที่ระบุใน ไฟล์คอนฟิกูเรชัน /etc/tnccs.conf

- ผู้ดูแลระบบจะเริ่มต้นการตรวจสอบไคลเอ็นต์ด้วยตัวเอง: ผู้ดูแลระบบสามารถเริ่มการตรวจสอบด้วยตัวเองเพื่อตรวจสอบว่าไคลเอ็นต์ถูกเพิ่มไปยังเครือข่ายหรือไม่โดยการรรันคำสั่ง ต่อไปนี้:

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

หมายเหตุ: สำหรับรีซอร์สที่ไม่ได้เชื่อมต่อกับ VIOS สามารถตรวจสอบ และอัพเดตไคลเอ็นต์เมื่อถูกเพิ่มไปยังเซิร์ฟเวอร์ TNC ด้วยตัวเอง

สิ่งอ้างอิงที่เกี่ยวข้อง:

"คำสั่ง psconf" ในหน้า 44

การดูผลลัพธ์การตรวจสอบของ Trusted Network Connect

ศึกษาขั้นตอนเพื่อดูผลลัพธ์การตรวจสอบ ไคลเอ็นต์ Trusted Network Connect (TNC)

| เพื่อดูผลลัพธ์การตรวจสอบของไคลเอ็นต์ในเครือข่าย ให้ป้อนคำสั่งต่อไปนี้:

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

| คำสั่งนี้จะแสดงไคลเอ็นต์ทั้งหมดที่มีสถานะ **IGNORED, COMPLIANT** หรือ **FAILED**

- **IGNORED**: IP ไคลเอ็นต์ถูกข้ามในรายการ IP (นั้นคือ ไคลเอ็นต์อาจได้รับการยกเว้นจากการตรวจสอบ)
- **COMPLIANT**: ไคลเอ็นต์ผ่านการตรวจสอบ (นั้นคือ ไคลเอ็นต์เป็นไปตามนโยบาย)
- **FAILED**: ไคลเอ็นต์ไม่ผ่านการตรวจสอบ (นั้นคือ ไคลเอ็นต์ ไม่เป็นไปตามโยบาย และต้องมีการดำเนินการของผู้ดูแลระบบ)

| เพื่อตรวจหาสาเหตุของความล้มเหลว ให้รันคำสั่ง **psconf** ที่มี IP ไคลเอ็นต์ที่ล้มเหลว:

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

สิ่งอ้างอิงที่เกี่ยวข้อง:

"คำสั่ง psconf" ในหน้า 44

การอัพเดตไคลเอ็นต์ Trusted Network Connect

เซิร์ฟเวอร์ Trusted Network Connect (TNC) จะตรวจสอบไคลเอ็นต์ และอัพเดตฐานข้อมูลด้วยสถานะของไคลเอ็นต์ และผลลัพธ์ ของการตรวจสอบ ผู้ดูแลระบบสามารถดูผลลัพธ์ และดำเนินการ อัพเดตไคลเอ็นต์

| เพื่ออัพเดตไคลเอ็นต์ที่อยู่ที่ระดับก่อนหน้า ให้ป้อนคำสั่ง ต่อไปนี้:

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

| ตัวอย่าง :

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

คำสั่ง **psconf** จะอัพเดตไคลเอ็นต์ด้วย การติดตั้งบิลด์ และ APAR หากไม่ถูกติดตั้งไว้

สิ่งอ้างอิงที่เกี่ยวข้อง:

"คำสั่ง psconf" ในหน้า 44

การจัดการนโยบายการจัดการแพตช์

| คำสั่ง **pmconf** จะถูกใช้เพื่อกำหนดค่าคอนฟิกนโยบายการจัดการแพตช์

นโยบายการจัดการแพตช์จะมีข้อมูล เช่น IP แอดเดรสของเซิร์ฟเวอร์ TNC และช่วงเวลาในการเริ่มต้นการอัพเดต SUMA

| เพื่อจัดการนโยบายการจัดการแพตช์ให้ป้อนคำสั่งต่อไปนี้:

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

| ตัวอย่าง :

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

หมายเหตุ: พอร์ต `pmport` และ `tncserver` ต้องมีค่าที่ต่างกัน

สิ่งอ้างอิงที่เกี่ยวข้อง:

"คำสั่ง pmconf" ในหน้า 40

การอิมพอร์ตใบรับรอง Trusted Network Connect

ศึกษาขั้นตอนในการอิมพอร์ตใบรับรอง และการส่งข้อมูลใน เครือข่ายอย่างปลอดภัย

| การสื่อสาร Trusted Network Connect (TNC) daemons บน ช่องทางที่เข้ารหัสไว้ที่เปิดใช้งานโดยใช้โปรโตคอล Transport
| Layer Security (TLS) หรือ Secure Sockets Layer (SSL)daemon นี้ทำให้แน่ใจว่า ข้อมูลและคำสั่งที่อยู่บนเครือข่าย จะได้รับ
| การรับรอง และปลอดภัย แต่ละระบบจะมีคีย์และใบรับรองของตัวเอง ที่สร้างขึ้นเมื่อรันคำสั่งเริ่มต้นสำหรับ คอมโพเนนต์
| กระบวนการนี้จะโปร่งใสต่อผู้ดูแลระบบ และต้องการ ความเกี่ยวข้องที่น้อยลงจากผู้ดูแลระบบ เมื่อไคลเอ็นต์ถูกตรวจสอบ
| ในครั้งแรก ใบรับรองของไคลเอ็นต์จะถูกอิมพอร์ตไปยังฐานข้อมูล ของเซิร์ฟเวอร์ ใบรับรองจะถูกทำเครื่องหมายเป็นไม่ไว้วาง
| ใจในตอนเริ่มแรก และ ผู้ดูแลระบบจะใช้คำสั่ง **psconf** เพื่อ ดู และทำเครื่องหมายใบรับรองเป็นไว้วางใจโดยการป้อนคำสั่ง
| ต่อไปนี้:

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

| หากผู้ดูแลระบบต้องการใช้คีย์ และใบรับรองที่แตกต่าง คำสั่ง **psconf** จะมีคุณลักษณะเพื่อ อิมพอร์ตคีย์และใบรับรอง

| เพื่ออิมพอร์ตใบรับรองจากเซิร์ฟเวอร์ให้ป้อน คำสั่งต่อไปนี้:

```
| psconf import  -S -k <key filename> -f <filename>
```

| เพื่ออิมพอร์ตใบรับรองจากไคลเอ็นต์ให้ป้อน คำสั่งต่อไปนี้:

```
| psconf import -C -k <key filename> -f <filename>
```

สิ่งอ้างอิงที่เกี่ยวข้อง:

"คำสั่ง psconf" ในหน้า 44

การสร้างรายงานของเซิร์ฟเวอร์ TNC

เซิร์ฟเวอร์ Trusted Network Connect (TNC) สนับสนุนทั้ง รูปแบบค่าที่คั่นด้วยเครื่องหมายคอมม่า (CSV) และรูปแบบเอาต์พุตข้อความ สำหรับ Common Vulnerabilities And Exposures (CVE) IBM Security Advisory, นโยบายเซิร์ฟเวอร์ TNC , โปรแกรมแก้ไขที่ปลอดภัย ของไคลเอ็นต์ TNC และรายงานเซอร์วิสแพ็คที่ลงทะเบียนไว้ และโปแกรมแก้ไขปัญหา ระหว่างเวอร์ชัน

รายงาน CVE จะแสดงจุดอ่อนและ ช่องโหว่ที่พบทั่วไปสำหรับเซอร์วิสแพ็คที่ลงทะเบียนไว้ เพื่อแสดง ผลลัพธ์ของรายงานนี้ ให้ป้อนคำสั่งต่อไปนี้:

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

รายงาน IBM Security Advisory จะแสดงช่องโหว่ด้านความปลอดภัยที่รู้จักบน ซอฟต์แวร์ IBM ที่ติดตั้งไว้ เพื่อแสดง ผลลัพธ์ของรายงานนี้ ให้ป้อนคำสั่งต่อไปนี้:

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

รายงานของนโยบายเซิร์ฟเวอร์ TNC จะแสดงนโยบาย ด้านความปลอดภัยที่จะใช้บังคับบนเซิร์ฟเวอร์ TNC เพื่อแสดง ผลลัพธ์ของรายงานนี้ ให้ป้อนคำสั่งต่อไปนี้:

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

รายงานการแก้ไขของไคลเอ็นต์ TNC จะแสดงโปรแกรมแก้ไขปัญหา ระหว่างเวอร์ชันที่ขาดหายไป และที่ติดตั้งไว้สำหรับไคลเอ็นต์ TNC เพื่อแสดง ผลลัพธ์ของรายงานนี้ ให้ป้อนคำสั่งต่อไปนี้:

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

คุณยังสามารถรันรายงานที่สร้างรายการ เซอร์วิสแพ็คที่ลงทะเบียนไว้ และรายงานการวิเคราะห์โปรแกรมที่ได้รับอนุญาต ที่เกี่ยวข้อง (APARs) และโปรแกรมแก้ไขปัญหาระหว่างเวอร์ชัน เพื่อแสดง ผลลัพธ์ของรายงานนี้ ให้ป้อนคำสั่งต่อไปนี้:

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

สิ่งอ้างอิงที่เกี่ยวข้อง:

"คำสั่ง psconf" ในหน้า 44

การแก้ไขปัญหาการจัดการ Trusted Network Connect และ Patch

ศึกษาสาเหตุที่เป็นไปได้สำหรับความล้มเหลว และขั้นตอนเพื่อ แก้ไขปัญหาระบบการจัดการ TNC และแพตช์

เพื่อแก้ไขปัญหา TNC และระบบการจัดการแพตช์ ให้ตรวจสอบ การตั้งค่าคอนฟิกูเรชันที่แสดงในตารางต่อไปนี้

ตารางที่ 3. การแก้ไขปัญหาการตั้งค่าคอนฟิกูเรชัน ระบบการจัดการ TNC และ Patch

ปัญหา	วิธีแก้ไข
เซิร์ฟเวอร์ TNC ไม่สตาร์ท หรือตอบสนอง	ดำเนินการขั้นตอนต่อไปนี้: 1. ตรวจสอบว่า daemon ของเซิร์ฟเวอร์ TNC รันอยู่หรือไม่โดยการป้อนคำสั่ง: `ps -eaf | grep tnccsd` 2. หากไม่ถูกรันอยู่ ให้ลบไฟล์ `/var/tnc/.tncsock` 3. รีสตาร์ทเซิร์ฟเวอร์ หากไม่สามารถแก้ไขปัญหา ให้ตรวจสอบไฟล์คอนฟิกูเรชัน `/etc/tnccs.conf` สำหรับรายการ `component = SERVER` บนเซิร์ฟเวอร์ TNC
เซิร์ฟเวอร์การจัดการแพตช์ TNC ไม่สตาร์ท หรือตอบสนอง	• ตรวจสอบว่า daemon ของเซิร์ฟเวอร์การจัดการแพตช์ TNC รันอยู่โดยการป้อนคำสั่งต่อไปนี้หรือไม่: `ps -eaf | grep tncpmd` • ตรวจสอบไฟล์คอนฟิกูเรชัน `/etc/tnccs.conf` สำหรับรายการ `component = TNCPM` บนเซิร์ฟเวอร์การจัดการ แพตช์ TNC
ไคลเอ็นต์ TNC ไม่สตาร์ทหรือตอบสนอง	• ตรวจสอบว่า daemon ของไคลเอ็นต์ TNC รันอยู่โดยการป้อน คำสั่งต่อไปนี้: `ps -eaf | grep tnccsd` • ตรวจสอบไฟล์คอนฟิกูเรชัน `/etc/tnccs.conf` สำหรับรายการ `component = CLIENT` บนไคลเอ็นต์ TNC
ตัวอ้างอิง TNC IP ไม่ได้รันบน Virtual I/O Server (VIOS)	• ตรวจสอบว่า daemon ตัวอ้างอิง IP ของ TNC รันอยู่หรือไม่โดยการป้อนคำสั่งต่อไปนี้: `ps -eaf | grep tnccsd` • ตรวจสอบไฟล์คอนฟิกูเรชัน `/etc/tnccs.conf` สำหรับรายการ `component = IPREF` บน VIOS
ไม่สามารถกำหนดค่าคอนฟิกระบบได้ทั้งเซิร์ฟเวอร์ และไคลเอ็นต์ TNC	ไคลเอ็นต์และเซิร์ฟเวอร์ TNC ไม่สามารถรันพร้อมกันได้ บนระบบเดียวกัน
Daemons รันอยู่แต่ไม่มี การตรวจสอบ	เปิดใช้ข้อความล็อกสำหรับ daemons ตั้งค่า ล็อก `level=info` ในไฟล์ `/etc/tnccs.conf` คุณสามารถวิเคราะห์ข้อความล็อก

คำสั่ง PowerSC Standard Edition

PowerSC Standard Edition จะมีคำสั่งที่ทำให้สามารถสื่อสารกับคอมโพเนนต์ Trusted Firewall และคอมโพเนนต์ Trusted Network Connect โดยใช้ บรรทัดคำสั่ง

คำสั่ง chvfilt

วัตถุประสงค์

เปลี่ยนแปลง ค่าสำหรับกฎตัวกรองการข้าม LAN เสมือนที่มีอยู่

ไวยากรณ์

chvfilt [-v <4|6>] -n fid [-a <D|P>] [-z <svlan>] [-Z <dvlan>] [-s <s_addr>] [-d <d_addr>] [-o <src_port_op>] [-p <src_port>] [-O <dst_port_op>] [-P <dst_port>] [-c <protocol>]

คำอธิบาย

คำสั่ง **chvfilt** จะถูกใช้เพื่อเปลี่ยนแปลงนิยาม กฎตัวกรองการข้าม LAN เสมือนในตารางกฎตัวกรอง

แฟล็ก

`-a` ระบุการดำเนินการ ค่าที่ถูกมีดังนี้:

- D (ปฏิเสธ): บล็อกทราฟฟิก
- P (อนุญาต): อนุญาตทราฟฟิก

`-c` ระบุโปรโตคอลที่แตกต่างให้กับกฎตัวกรองที่มี ค่าที่ถูกต้องมีดังนี้:

- udp
- icmp
- icmpv6
- tcp
- อื่นๆ

`-d` ระบุแอดเดรสปลายทางในรูปแบบ IPv4 หรือ IPv6

`-m` ระบุมาส์กแอดเดรสต้นทาง

`-M` ระบุมาร์กแอดเดรสปลายทาง

`-n` ระบุ ID ตัวกรองของกฎตัวกรองที่ควรถูกแก้ไข

`-o` ระบุพอร์ตต้นทาง หรือการดำเนินการประเภท Internet Control Message Protocol (ICMP) ค่าที่ถูกต้องมีดังนี้:

- lt
- gt
- eq
- อื่นๆ

`-O` ระบุพอร์ตปลายทางหรือการดำเนินการโค้ด ICMP ค่าที่ถูกต้อง มีดังนี้:

- lt
- gt
- eq
- อื่นๆ

`-p` ระบุพอร์ตต้นทาง หรือประเภท ICMP

`-P` ระบุพอร์ตปลายทางหรือโค้ด ICMP

`-s` ระบุแอดเดรสต้นทางในรูปแบบ v4 หรือ v6

-v ระบุเวอร์ชัน IP ของตารางกฎตัวกรอง ค่าที่ถูกต้อง คือ 4 และ 6

-z ระบุ ID ของ LAN เสมือนของโลจิคัลพาร์ติชันต้นทาง

-Z ระบุ ID ของ LAN เสมือนของโลจิคัลพาร์ติชันปลายทาง

สถานะของการออก

คำสั่งนี้จะส่งคืนค่าการออกดังต่อไปนี้:

0 เสร็จสมบูรณ์

>0 เกิดข้อผิดพลาด

ตัวอย่าง

1. เพื่อเปลี่ยนกฎตัวกรองที่ถูกต้องที่มีอยู่ในเคอร์เนล ให้พิมพ์ คำสั่งดังนี้:

   ```
   chvfilt -n 1 -v4 -a P -z 100 -Z 300 -o eq -p 23 -O lt -P 345 -c tcp
   ```

2. เมื่อกฎตัวกรอง (n=2) ไม่มีอยู่ในเคอร์เนล เอาท์พุท จะเป็นดังนี้:

   ```
   chvfilt -n 2 -v4 -a P -z 100 -Z 300 -o eq -p 23 -O lt -P 345 -c tcp
   ```

   ระบบจะแสดงเอาท์พุทดังนี้:

   ```
   ioctl(QUERY_FILTER) failed no filter rule err=2
   Cannot Change the filter rule
   ```

คำสั่ง genvfilt

วัตถุประสงค์

เพิ่ม กฎตัวกรองสำหรับการข้าม LAN เสมือน (VLAN) ระหว่างโลจิคัล พาร์ติชันบนเซิร์ฟเวอร์ IBM Power Systems เดียวกัน

ไวยากรณ์

genvfilt −v <**4**|**6**> **−a** <**D**|**P**> **−z** <**svlan**> **−Z** <**dvlan**> [**−s** <**s_addr**>] [**−d** <**d_addr**>] [**−o** <**src_port_op**>] [**−p** <**src_port**>] [**−O** <**dst_port_op**>] [**−P** <**dst_port**>] [**−c** <**protocol**>]

คำอธิบาย

คำสั่ง **genvfilt** จะเพิ่มกฎตัวกรองสำหรับ การข้าม Virtual LAN (VLAN) ระหว่างโลจิคัลพาร์ติชัน (LPARs) บน เซิร์ฟเวอร์ IBM Power Systems เดียวกัน

แฟล็ก

-a ระบุการดำเนินการ ค่าที่ถูกต้องมีดังนี้:

- D (ปฏิเสธ): บล็อกทราฟฟิก
- P (อนุญาต): อนุญาตทราฟฟิก

-c ระบุโปรโตคอลที่แตกต่างให้กับกฎตัวกรองที่มี ค่าที่ถูกต้องมีดังนี้:

- udp

- icmp
- icmpv6
- tcp
- อื่นๆ

`-d` ระบุแอดเดรสปลายทางในรูปแบบ v4 หรือ v6

`-m` ระบุมาส์กแอดเดรสต้นทาง

`-M` ระบุมาส์กแอดเดรสปลายทาง

`-o` ระบุพอร์ตต้นทาง หรือการดำเนินการประเภท Internet Control Message Protocol (ICMP) ค่าที่ถูกต้องมีดังนี้:

- lt
- gt
- eq
- อื่นๆ

`-O` ระบุพอร์ตปลายทางหรือการดำเนินการโค้ด ICMP ค่าที่ถูกต้อง มีดังนี้:

- lt
- gt
- eq
- อื่นๆ

`-p` ระบุพอร์ตต้นทาง หรือประเภท ICMP

`-P` ระบุพอร์ตปลายทางหรือโค้ด ICMP

`-s` ระบุแอดเดรสต้นทางในรูปแบบ IPv4 หรือ IPv6

`-v` ระบุเวอร์ชัน IP ของตารางกฎตัวกรอง ค่าที่ถูกต้อง คือ 4 และ 6

`-z` ระบุ ID ของ LAN เสมือนของ LPAR ต้นทาง ID ของ LAN เสมือนต้องอยู่ในช่วง 1 – 4096

`-Z` ระบุ ID ของ LAN เสมือนของ LPAR ปลายทาง ID ของ LAN เสมือนต้องอยู่ในช่วง 1 – 4096

สถานะของการออก

คำสั่งนี้จะส่งคืนค่าการออกดังต่อไปนี้:

`0` เสร็จสมบูรณ์

`>0` เกิดข้อผิดพลาด

ตัวอย่าง

1. เพื่อเพิ่มกฎตัวกรองในการอนุญาตให้ข้อมูล TCP จาก ID ของ VLAN ต้นทาง ที่เท่ากับ 100 ไปยัง ID ของ VLAN ปลายทางที่เท่ากับ 200 บนพอร์ตที่ระบุ ให้พิมพ์ คำสั่งดังนี้:

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

สิ่งอ้างอิงที่เกี่ยวข้อง:

"คำสั่ง mkvfilt"

"คำสั่ง vlantfw" ในหน้า 51

คำสั่ง lsvfilt

วัตถุประสงค์

แสดง กฎตัวกรองการข้าม LAN เสมือนจากตารางตัวกรอง

ไวยากรณ์

lsvfilt [**-a**]

คำอธิบาย

คำสั่ง **lsvfilt** จะถูกใช้เพื่อแสดงกฎตัวกรอง การข้าม LAN เสมือน และสถานะของกฎ

แฟล็ก

`-a` แสดงเฉพาะกฎตัวกรองที่ใช้งานอยู่

สถานะการออก

คำสั่งนี้จะส่งคืนค่าการออกดังต่อไปนี้:

`0` เสร็จสมบูรณ์

`>0` เกิดข้อผิดพลาด

ตัวอย่าง

1. เพื่อแสดงกฎตัวกรองที่ใช้งานอยู่ทั้งหมดในเคอร์เนล ให้พิมพ์คำสั่ง ต่อไปนี้:

```
lsvfilt -a
```

หลักการที่เกี่ยวข้อง:

"การปิดใช้งานกฎ" ในหน้า 18

คุณสามารถปิดใช้งานกฎที่เปิดใช้การกำหนดเส้นทางข้าม VLAN ในคุณลักษณะ Trusted Firewall

คำสั่ง mkvfilt

วัตถุประสงค์

เปิดใช้งาน กฎตัวกรองการข้าม LAN เสมือนที่กำหนดด้วยคำสั่ง **genvfilt**

ไวยากรณ์

mkvfilt -u

คำอธิบาย

คำสั่ง **mkvfilt** จะเรียกใช้กฎตัวกรองการข้าม LAN เสมือนที่กำหนดด้วยคำสั่ง **genvfilt**

แฟล็ก

`-u` เปิดใช้งานกฎตัวกรองในตารางกฎตัวกรอง

สถานะการออก

คำสั่งนี้จะส่งคืนค่าการออกดังต่อไปนี้:

`0` เสร็จสมบูรณ์

`>0` เกิดข้อผิดพลาด

ตัวอย่าง

1. เพื่อเปิดใช้กฎตัวกรองในเคอร์เนล ให้พิมพ์คำสั่ง ต่อไปนี้:

```
mkvfilt -u
```

สิ่งอ้างอิงที่เกี่ยวข้อง:

"คำสั่ง genvfilt" ในหน้า 37

คำสั่ง pmconf

วัตถุประสงค์

รายงานและจัดการเซิร์ฟเวอร์การจัดการ แพตช์การเชื่อมต่อเครือข่ายที่ไว้วางใจได้ (TNCPM) โดยการลงทะเบียน Technology Levels และเซิร์ฟเวอร์ TNC สำหรับโปรแกรมแก้ไขล่าสุด และการสร้างรายงานเกี่ยวกับ สถานะ TNCPM

หมายเหตุ: เซิร์ฟเวอร์ TNCPM ต้องรันบน AIX เวอร์ชัน 7.1 ที่มี 7100-02 Technology Level เท่านั้นเพื่อทำให้สามารถดาวน์โหลดเมตาดาต้าเซอร์วิสแพ็ค

ไวยากรณ์

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

pmconf rmtncpm

pmconf start

pmconf stop

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

pmconf add -l *TL_list*

pmconf add -p *<SP List>* [**-U** *<user-defined SP path>*]

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

| **pmconf add -y** *<advisory file>* **-v** *<signature file>* **-e** *<ifix tar file>*

pmconf delete -l *TL_list*

pmconf delete -p *<SP List>*

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

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 *cert_filename* **-k** *key_filename*

pmconf export -f *filename*

pmconf modify -i *< download interval>*

pmconf modify -P *<download path>*

pmconf modify -g *<yes or no to accept all licenses>*

pmconf modify -t *<APAR type list>*

| **pmconf modify -x** *<ifix interval>*

| **pmconf modify -K** *<ifix key>*

pmconf delete -l *<TL list>*

pmconf restart

pmconf status

pmconf log loglevel = info | error | none

pmconf chtncpm attribute = *value*

คำอธิบาย

ฟังก์ชันของคำสั่ง **pmconf** มีดังนี้:

การจัดการที่เก็บโปรแกรมแก้ไข

ลงทะเบียน หรือยกเลิกการลงทะเบียน Technology Levels ยกเลิกการลงทะเบียนเซิร์ฟเวอร์ TNC TNCPM จะสร้างที่เก็บโปรแกรมแก้ไขสำหรับแต่ละ Technology Level ที่มี โปรแกรมแก้ไขล่าสุด ข้อมูล **lslpp** (ตัวอย่างเช่น ข้อมูล เกี่ยวกับชุดไฟล์ที่ติดตั้ง หรือการอัพเดตชุดไฟล์) และโปรแกรมแก้ไขที่ปลอดภัย สำหรับ Technology Level นั้น

การสร้างรายงาน

สร้างรายงานเกี่ยวกับสถานะของ TNCPM

การดำเนินการต่อไปนี้สามารถทำโดย ใช้คำสั่ง **pmconf**:

รายการ	คำอธิบาย
add	ลงทะเบียน Technology Level ใหม่โดยใช้ TNCPM
chtncpm	เปลี่ยนแปลงแอ็ตทริบิวต์ในไฟล์ tnccs.conf คำสั่ง **start** ที่ชัดเจนเป็นสิ่งจำเป็นเพื่อให้การเปลี่ยนแปลง มีผลในเซิร์ฟเวอร์ TNCPM
delete	ยกเลิกการลงทะเบียน Technology Level โดยใช้ TNCPM
history	แสดงประวัติการอัพเดต และการดาวน์โหลด
list	แสดงข้อมูลเกี่ยวกับ TNCPM
log	ตั้งค่าระดับการบันทึกสำหรับคอมโพเนนต์ TNC
mktncpm	สร้างเซิร์ฟเวอร์ TNCPM
modify	แก้ไขแอ็ตทริบิวต์ tncpm.conf
rmtncpm	ลบเซิร์ฟเวอร์ TNCPM
start	สตาร์ทเซิร์ฟเวอร์ TNCPM
stop	หยุดเซิร์ฟเวอร์ TNCPM

แฟล็ก

รายการ	คำอธิบาย
-A	ยอมรับข้อตกลงการใช้ซอฟต์แวร์ทั้งหมดเมื่อดำเนินการอัพเดต ไคลเอ็นต์
-a <advisory file>	ระบุไฟล์แอดไวเซอร์ที่สอดคล้อง กับพารามิเตอร์ `ifix` หากไม่มีไฟล์แอดไวเซอร์ ถูกระบุไว้ พารามิเตอร์ `ifix` จะไม่ถูกมองเป็นแอดเดรส Common Vulnerabilities and Exposures (CVE) ของโปรแกรมแก้ไขปัญหา ระหว่างเวอร์ชัน
-e <ifix file>	ระบุโปรแกรมแก้ไขปัญหาระหว่างเวอร์ชันที่ถูกเพิ่มไปยัง TNCPM
-i *download_interval*	ระบุช่วงเวลาที่ TNCPM ตรวจสอบเพื่อหา เซอร์วิสแพ็คใหม่สำหรับระดับเทคโนโลยีที่ลงทะเบียนไว้ ช่วงเวลา จะเป็นค่าเลขจำนวนเต็มที่แสดงเป็นนาที หรือในรูปแบบต่อไปนี้: **d** (จำนวนวัน): **h** (ชั่วโมง): **m** (นาที)
-K <ifix key>	ระบุคีย์พับลิกของ IBM AIX Product Security Incident Response Tool (PSIRT) ที่ใช้เพื่อพิสูจน์ตัวตนแอดไวเซอร์ และโปรแกรมแก้ไขปัญหาระหว่างเวอร์ชันที่ดาวน์โหลด คีย์พับลิกนี้สามารถดาวน์โหลดได้จาก เซิร์ฟเวอร์คีย์พับลิก PGP โดยใช้ ID **0x28BFAA12**
-p *SP_list*	ระบุรายการเซอร์วิสแพ็คที่จะดาวน์โหลด รายการคือรายการที่คั่นด้วยเครื่องหมายคอมม่าในรูปแบบ REL00-TL-SP (ตัวอย่างเช่น `6100-01-04` แสดงถึงเซอร์วิสแพ็ค 04 สำหรับระดับเทคโนโลยี 01 และเวอร์ชัน 6.1) เมื่อคุณใช้แฟล็ก -U จะระบุเพียงหนึ่ง SP เท่านั้น
-t *APAR_type_list*	ระบุชนิด APAR ที่ TNCPM สนับสนุน สำหรับรายการเซิร์ฟเวอร์ TNC และการอัพเดตไคลเอ็นต์ APARs ที่ปลอดภัยจะได้รับการสนับสนุน ตลอดเวลา APAR_type_list คือรายการที่คั่นด้วยเครื่องหมายคอมม่าของชนิด ต่อไปนี้: HIPER, FileNet® Process Engine, Enhancement
-P *fix_repository_path*	ระบุไดเร็กทอรีที่ดาวน์โหลดสำหรับที่เก็บ โปรแกรมแก้ไขที่จะถูกดาวน์โหลดโดย TNCPM ไดเร็กทอรีดีฟอลต์ คือ **/var/tnc/tncpm/fix_repository**
-U *user_defined_fix_repository*	ระบุพาธไปยังที่เก็บโปรแกรมแก้ไขที่ผู้ใช้กำหนด ระบุรีลีส ระดับเทคโนโลยี และเซอร์วิสแพ็คที่ เชื่อมโยงกับที่เก็บโปรแกรมแก้ไขที่ถูกใช้สำหรับการตรวจสอบ และการอัพเดตไคลเอ็นต์
-s	สร้างรายงานของเซอร์วิสแพ็คที่ลงทะเบียนไว้
-l *SP*	สร้างรายงานของข้อมูล **lslpp** สำหรับเซอร์วิสแพ็ค *SP* จะอยู่ในรูปแบบ REL00-TL-SP (ตัวอย่าง เช่น `6100-01-04` ซึ่งแสดงถึงเซอร์วิสแพ็ค 04 สำหรับระดับเทคโนโลยี 01 และเวอร์ชัน 6.1)
-u	สร้างรายงานของประวัติการอัพเดตไคลเอ็นต์
-d	สร้างรายงานของประวัติการดาวน์โหลด เซอร์วิสแพ็ค
-C	สร้างรายงานสำหรับใบรับรองเซิร์ฟเวอร์

รายการ	คำอธิบาย
-a *SP*	สร้างรายงานของข้อมูลรายงานการวิเคราะห์โปรแกรม ที่ได้รับอนุญาต (APAR) ที่ปลอดภัยสำหรับเซอร์วิสแพ็ค *SP* อยู่ในรูปแบบ REL00-TL-SP (ตัวอย่างเช่น 6100-01-04 ซึ่งแสดงถึงเซอร์วิสแพ็ค 04 สำหรับระดับเทคโนโลยี 01 และเวอร์ชัน 6.1)
-f *filename*	ระบุชื่อไฟล์ใบรับรอง
-k *key_filename*	ระบุไฟล์ที่ใบรับรอง ต้องอ่านในกรณีของการอิมพอร์ต

-c	แสดงแอ็ตทริบิวต์ผู้ใช้ในเร็กคอร์ดที่คั่นด้วยเครื่องหมายโคลอน ดังต่อไปนี้:
	`# name: attribute1: attribute2: ...`
	`policy: value1: value2: ...`

-v *<signature file>*	ระบุไฟล์ Signature สำหรับแอดไวเซอร์ที่มีช่องโหว่ของ IBM AIX
-y *<advisory file>*	ระบุไฟล์แอดไวเซอร์ที่มีช่องโหว่ของ IBM AIX
-q	ยกเลิกข้อมูลส่วนหัว
-x *<ifix interval>*	ระบุช่วงเวลาในหน่วยนาทีเพื่อตรวจสอบ และดาวน์โหลดโปรแกรมแก้ไขปัญหาระหว่างเวอร์ชันใหม่ หากค่านี้ถูกตั้งค่าเป็น 0 การแจ้งเตือน และการดาวน์โหลด โปรแกรมแก้ไขปัญหาระหว่างเวอร์ชันจะถูกปิดใช้งาน ช่วงเวลาดีฟอลต์ คือทุกๆ 24 ชั่วโมง

สถานะการออก

คำสั่งนี้จะส่งคืน ค่าการออกดังต่อไปนี้:

รายการ	คำอธิบาย
0	คำสั่งถูกรันสำเร็จ และทำการเปลี่ยนแปลง ที่ร้องขอทั้งหมด
>0	เกิดข้อผิดพลาด ข้อความแสดงข้อผิดพลาดที่พิมพ์ จะมีรายละเอียดเพิ่มเติมเกี่ยวกับชนิดของความล้มเหลว

ตัวอย่าง

1. เพื่อเริ่มต้น TNCPM ให้ป้อนคำสั่งต่อไปนี้:

   ```
   pmconf init -f 10080 -l 5300-11,6100-00
   ```

2. เพื่อสร้าง TNCPM daemon ให้ป้อนคำสั่งต่อไปนี้:

   ```
   mktncpm pmport=55777 tncserver=11.11.11.11:77555
   ```

3. เพื่อสตาร์ทเซิร์ฟเวอร์ ให้ป้อนคำสั่งต่อไปนี้:

   ```
   pmconf start
   ```

4. เพื่อหยุดเซิร์ฟเวอร์ ให้ป้อนคำสั่งต่อไปนี้:

   ```
   pmconf stop
   ```

5. เพื่อลงทะเบียนระดับเทคโนโลยีใหม่โดยใช้ TNCPM ให้ป้อนคำสั่ง ต่อไปนี้:

   ```
   pmconf add -l 6100-01
   ```

6. เพื่อยกเลิกการลงทะเบียนระดับเทคโนโลยีจาก TNCPM ให้ป้อนคำสั่ง ต่อไปนี้:

   ```
   pmconf delete -l 6100-01
   ```

7. เพื่อยกเลิกการลงทะเบียนเซิร์ฟเวอร์ TNC ที่มี IP แอดเดรสเท่ากับ 11.11.11.11 จาก TNCPM ให้ป้อนคำสั่งต่อไปนี้:

   ```
   pmconf delete -t 11.11.11.11
   ```

8. เพื่อลงทะเบียนเวอร์ชันที่ใหม่กว่าของเซอร์วิสแพ็คก่อนหน้าใน TNCPM ให้ป้อนคำสั่งต่อไปนี้:

   ```
   pmconf add -s 6100-01-04
   ```

9. เพื่อยกเลิกการลงทะเบียนเซอร์วิสแพ็คก่อนหน้าจาก TNCPM ให้ป้อนคำสั่ง ต่อไปนี้:

   ```
   pmconf delete -s 6100-01-04
   ```

10. เพื่อสร้างรายงานของที่เก็บโปรแกรมแก้ไขสำหรับแต่ละระดับเทคโนโลยี ที่ลงทะเบียน ให้ป้อนคำสั่งต่อไปนี้:

    ```
    pmconf list -s
    ```

11. เพื่อสร้างรายงานของข้อมูลระดับเทคโนโลยีที่ลงทะเบียนไว้ **lslpp** ให้ป้อนคำสั่งต่อไปนี้:

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

12. เพื่อสร้างรายงานจากประวัติการอัพเดต ให้ป้อนคำสั่ง ต่อไปนี้:

```
pmconf hist -u
```

13. เพื่อสร้างรายงานจากประวัติการดาวน์โหลด ให้ป้อนคำสั่ง ต่อไปนี้:

```
pmconf hist -d
```

14. เพื่อสร้างรายงานของใบรับรองเซิร์ฟเวอร์ ให้ป้อนคำสั่ง ต่อไปนี้:

```
pmconf list -C
```

15. เพื่อสร้างรายงานของข้อมูล APAR ที่ปลอดภัยของเซอร์วิสแพ็ค ให้ป้อนคำสั่งต่อไปนี้:

```
pmconf list -a 6100-01-02
```

16. เพื่ออิมพอร์ตใบรับรองเซิร์ฟเวอร์ ให้ป้อนคำสั่งต่อไปนี้:

```
pmconf import -f /tmp/server.txt -k /tmp/server-cert-key.txt
```

17. เพื่อเอ็กซ์พอร์ตใบรับรองเซิร์ฟเวอร์ ให้ป้อนคำสั่งต่อไปนี้:

```
pmconf export -f /tmp/server.txt
```

คำสั่ง psconf

วัตถุประสงค์

รายงานและจัดการเซิร์ฟเวอร์ Trusted Network Connect (TNC) , ไคลเอ็นต์ TNC, TNC IP Referrer (IPRef) และ Service Update Management Assistant (SUMA) ซึ่งจะจัดการ การตั้งค่าไฟล์ และนโยบายการจัดการแพตช์ตามบูรณภาพของอุปกรณ์ปลายทาง (เซิร์ฟเวอร์ และ ไคลเอ็นต์) ขณะที่ หรือหลังจากการเชื่อมต่อเครือข่ายเพื่อปกป้องเครือข่าย จากการคุกคามและการโจมตี

ไวยากรณ์

การดำเนินการของเซิร์ฟเวอร์ TNC:

psconf mkserver [**tncport=**<*port*>] **pmserver=**<*host*:*port*> [tsserver=<host>] [**recheck_interval=**<*time_in_minutes*> | **d** (days) : **h** (hours) : **m** (minutes)] [**dbpath** = <*user-defined directory*>]

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

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

psconf chserver attribute = *value*

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

psconf add { **-G** <*ipgroupname*> **ip=**[**±**]<*host1, host2...*> | { **-A**<*apargrp*> [**aparlist=**[**±**]*apar1, apar2...* | { **-V** <*ifixgrp*> [*ifixlist*=[+|-]*ifix1*,*ifix2...*]}

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

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

| **psconf add -I ip=** [±]<*host1, host2...*>

| **psconf delete** { **-F** <*FSPolicyname*> | **-G** <*ipgroupname*> | **-P** <*policyname*> | **-A** <*apargrp*> | **-V** <*ifixgrp*> }

| **psconf delete -H -i** <*host* | **ALL**> **-D** <*yyyy-mm-dd*>

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

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

| **psconf verify -i** <*host*> | **-G** <*ipgroup*>

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

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

| **psconf import -C -i** <*host*> **-f** <*filename*> | **-d** <*import database filename*>

| **psconf** { **import -k** <*key_filename*> | **export**} **-S -f** <*filename*>

| **psconf list** { **-S** | **-G** < *ipgroupname* | **ALL** > | **-F** < *FSPolicyname* | **ALL** > | **-P** < *policyname* | **ALL** > | **-r** < *buildinfo* | **ALL** > |
| **-I -i** < *ip* | **ALL** > | **-A** < *apargrp* | **ALL** > | **-V** <*ifixgrp*> } [**-c**] [**-q**]

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

| **psconf export -d** <*path to export directory*>

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

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

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

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

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

| การดำเนินการของไคลเอ็นต์ TNC:

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

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

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

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

| **psconf chclient** attribute = *value*

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

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

| **psconf import** { **-S** | **-C -k** <*key_filename*> } **-f** <*filename*>

| TNC IPRef operations:

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

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

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

| **psconf chipref** attribute = *value*

| **psconf** { **import -k** <*key_filename*> | **export** } **-R -f** <*filename*>

| **psconf list -R**

คำอธิบาย

เทคโนโลยี TNC คือสถาปัตยกรรม ที่ใช้มาตรฐานแบบเปิดสำหรับการพิสูจน์ตัวตนอุปกรณ์ปลายทาง, การวัดค่า บูรณภาพของแพล็ตฟอร์ม และการบูรณภาพระบบการรักษาความปลอดภัย สถาปัตยกรรม TNC จะตรวจสอบอุปกรณ์ปลายทาง (เซิร์ฟเวอร์และไคลเอ็นต์ของเครือข่าย) สำหรับความสอดคล้องกับ นโยบายการรักษาความปลอดภัยก่อนที่จะอนุญาตให้สามารถใช้ได้ในเครือข่ายที่มีการป้องกัน TNC IPRef จะแจ้งเตือนเซิร์ฟเวอร์ TNC เกี่ยวกับ IPs ใหม่ที่ตรวจพบ บนเซิร์ฟเวอร์ I/O เสมือน (VIOS)

SUMA จะช่วยย้ายผู้ดูแลระบบ ออกจากงานการเรียกข้อมูลการอัพเดตการบำรุงรักษาด้วยตัวเองจาก เว็บ ซึ่งจะมีอ็อพชันที่ยืดหยุ่นที่ช่วยให้ผู้ดูแลระบบ สามารถตั้งค่าอินเตอร์เฟสในการดาวน์โหลดโปรแกรมแก้ไขโดยอัตโนมัติจากเว็บไซต์ ที่กระจายโปรแกรมแก้ไขไปยังระบบ

คำสั่ง **psconf** จะจัดการ ไคลเอ็นต์ และเซิร์ฟเวอร์เครือข่ายโดยการเพิ่มหรือลบนโยบายการรักษาความปลอดภัย, การตรวจสอบว่าเป็นไคลเอ็นต์ที่ไว้วางใจได้ หรือไม่ไว้วางใจ การสร้างรายงาน และ การอัพเดตเซิร์ฟเวอร์และไคลเอ็นต์

สามารถดำเนินการต่อไปนี้ โดยใช้คำสั่ง **psconf** :

รายการ	คำอธิบาย
add	เพิ่มนโยบาย ไคลเอ็นต์ หรือข้อมูลอีเมล บนเซิร์ฟเวอร์ TNC
apargrp	ระบุชื่อกลุ่ม APAR เป็นส่วนหนึ่งของ นโยบายการตั้งค่าไฟล์ที่ใช้สำหรับการตรวจสอบไคลเอ็นต์ TNC
aparlist	ระบุรายการ APARs ที่เป็นส่วนหนึ่งของ กลุ่ม APAR
certadd	ทำเครื่องหมายใบรับรองเป็นไว้วางใจได้ หรือไม่ไว้วางใจ
certdel	ลบข้อมูลไคลเอ็นต์
chclient	เปลี่ยนแปลงแอ็ตทริบิวต์ในไฟล์ `tnccs.conf` คำสั่ง **start** ที่ชัดเจนเป็นสิ่งจำเป็นเพื่อให้การเปลี่ยนแปลง มีผลในไคลเอ็นต์ TNC ไวยากรณ์ attribute=value จะเหมือนกับไวยากรณ์ของ **mkclient**
chipref	เปลี่ยนแปลงแอ็ตทริบิวต์ในไฟล์ `tnccs.conf` คำสั่ง **start** ที่ชัดเจนเป็นสิ่งจำเป็น เพื่อให้การเปลี่ยนแปลงมีผลใน IPRef ไวยากรณ์ attribute=value จะเหมือนกันกับไวยากรณ์ของ **mkipref**
chserver	เปลี่ยนแปลงแอ็ตทริบิวต์ในไฟล์ `tnccs.conf` คำสั่ง **start** ที่ชัดเจนเป็นสิ่งจำเป็น เพื่อให้การเปลี่ยนแปลงมีผลในเซิร์ฟเวอร์ TNC ไวยากรณ์ attribute=value จะเหมือนกับไวยากรณ์ของ **mkserver** **หมายเหตุ:** แอ็ตทริบิวต์ **dbpath** ไม่สามารถเปลี่ยนแปลงโดยใช้คำสั่ง **chserver** ซึ่งสามารถ ตั้งค่าได้ขณะรัน **mkserver**
dbpath	ระบุตำแหน่งฐานข้อมูล TNC ค่าดีฟอลต์ คือ `/var/tnc`
delete	ลบนโยบายหรือข้อมูลไคลเอ็นต์
export	เอ็กซ์พอร์ตใบรับรองไคลเอ็นต์หรือเซิร์ฟเวอร์ หรือ ฐานข้อมูลบนเซิร์ฟเวอร์ TNC
fspolicy	ระบุนโยบายการตั้งค่าไฟล์ของรีลีส, ระดับเทคโนโลยี และเซอร์วิสแพ็คที่ใช้สำหรับการตรวจสอบ ไคลเอ็นต์ TNC
import	อิมพอร์ตใบรับรองบนไคลเอ็นต์ หรือเซิร์ฟเวอร์ หรือ ฐานข้อมูลบนเซิร์ฟเวอร์ TNC
ipgroup	ระบุกลุ่ม Internet Protocol (IP) ที่ มีหลาย IP แอดเดรสของไคลเอ็นต์ หรือชื่อโฮสต์
list	แสดงข้อมูลเกี่ยวกับเซิร์ฟเวอร์ TNC ไคลเอ็นต์ TNC หรือ SUMA
log	ตั้งค่าระดับการบันทึกสำหรับคอมโพเนนต์ TNC
mkclient	กำหนดค่าคอนฟิกไคลเอ็นต์ TNC
mkipref	กำหนดค่าคอนฟิก TNC IPRef
mkserver	กำหนดค่าคอนฟิกเซิร์ฟเวอร์TNC
pmport	ระบุหมายเลขพอร์ตที่ซึ่ง **pmserver** คอยฟัง ค่าดีฟอลต์คือ 38240
pmserver	ระบุชื่อโฮสต์หรือ IP แอดเดรสของคำสั่ง **suma** ที่ดาวน์โหลดเซอร์วิสแพ็คล่าสุด และโปรแกรมแกรมแก้ไข ที่ปลอดภัยที่มีอยู่ในเว็บไซต์ IBM® ECC และเว็บไซต์ IBM Fix Central
recheck_interval	ระบุช่วงเวลาในหน่วยนาที หรือรูปแบบ d (วัน) : h (ชั่วโมง) : m (นาที) สำหรับเซิร์ฟเวอร์ TNC เพื่อตรวจสอบ ไคลเอ็นต์ TNC **หมายเหตุ:** ค่าของ **recheck_interval=0** หมายความว่าตัวกำหนดเวลาไม่ได้เริ่มต้นการตรวจสอบไคลเอ็นต์ ที่ช่วงเวลาปกติ และไคลเอ็นต์ที่ลงทะเบียนไว้จะถูกตรวจสอบโดยอัตโนมัติ ขณะเริ่มต้นทำงาน ในกรณีเช่นนี้ สามารถตรวจสอบไคลเอ็นต์ด้วยตัวเอง
report	สร้างรายงานที่มีส่วนขยายไฟล์ .txt หรือ .csv
restart	รีสตาร์ทไคลเอ็นต์ TNC เซิร์ฟเวอร์ TNC หรือ TNC IPRef
rmclient	ยกเลิกการกำหนดคอนฟิกไคลเอ็นต์ TNC
rmipref	ยกเลิกการกำหนดค่าคอนฟิก TNC IPRef
rmserver	ยกเลิกการกำหนดค่าคอนฟิกเซิร์ฟเวอร์ TNC
start	สตาร์ทไคลเอ็นต์ TNC , เซิร์ฟเวอร์ TNC หรือ TNC IPRef
สถานะ	แสดงสถานะของการกำหนดค่าคอนฟิก TNC
stop	หยุดไคลเอ็นต์ TNC , เซิร์ฟเวอร์ TNC หรือ TNC IPRef
tncport	ระบุหมายเลขพอร์ตที่ซึ่งเซิร์ฟเวอร์ TNC ใช้ฟัง ค่าดีฟอลต์คือ 42830
tncserver	ระบุเซิร์ฟเวอร์ TNC ที่ตรวจสอบหรืออัพเดต ไคลเอ็นต์ TNC
tssserver	ระบุ IP หรือชื่อโฮสต์ของเซิร์ฟเวอร์ Trusted Surveyor
update	ติดตั้งแพตช์บนไคลเอ็นต์
verify	เริ่มต้นการตรวจสอบด้วยตัวเองของไคลเอ็นต์

แฟล็ก

รายการ	คำอธิบาย
-A <advisoryName>	ระบุชื่อแอดไวเซอร์สำหรับรายงาน
-B <buildinfo>	ระบุข้อมูลบิลด์เพื่อจัดเตรียม รายงานแพตช์

-c	แสดงแอ็ตทริบิวต์ผู้ใช้ในเร็กคอร์ด ที่คั่นด้วยเครื่องหมายโคลอนดังนี้:
	`# name: attribute1: attribute2: ...`
	`policy: value1: value2: ...`

-C	ระบุว่าการดำเนินการมีไว้สำหรับคอมโพเนนต์ของไคลเอ็นต์
-d *database file location/dir path of database*	ระบุตำแหน่งพาธไฟล์สำหรับอิมพอร์ต ของฐานข้อมูล/ระบุตำแหน่งพาธไดเร็กทอรีสำหรับเอ็กซ์พอร์ตของ ฐานข้อมูล
-D *yyyy-mm-dd*	ระบุวันที่สำหรับรายการไคลเอ็นต์เฉพาะ ในประวัติล็อก โดยที่ *yyyy* คือปี *mm* คือ เดือน และ *dd* คือวันที่
-e *emailid* **ipgroup=**[**±**]*g1, g2...*	ระบุ ID อีเมลที่ตามด้วยรายชื่อกลุ่ม ที่คั่นด้วยเครื่องหมายคอมม่า
-E | FAIL | COMPLIANT | ALL |	ระบุเหตุการณ์ที่อีเมลต้อง ถูกส่งไปยัง id อีเมลที่กำหนดค่าคอนฟิกไว้ FAIL– Mails จะถูกส่งเมื่อ สถานะการตรวจสอบของไคลเอ็นต์คือ FAILED COMPLIANT– Mails จะถูกส่งเมื่อสถานะการตรวจสอบของไคลเอ็นต์คือ COMPLAINT ALL – Mails จะถูกส่งสำหรับสถานะทั้งหมดของการตรวจสอบไคลเอ็นต์
-f *filename*	ระบุไฟล์ที่ใบรับรอง ต้องอ่านในกรณีของการอิมพอร์ต หรือระบุตำแหน่ง ที่ใบรับรองต้องถูกเขียนทับในกรณีของการเอ็กซ์พอร์ต
-F *fspolicy buildinfo*	ระบุชื่อนโยบายของระบบไฟล์ ตามด้วย ข้อมูลบิลด์ ข้อมูลบิลด์สามารถอยู่ใน รูปแบบต่อไปนี้: `6100-04-01` โดย `6100` หมายถึงเวอร์ชัน 6.1, `04` คือ ระดับการบำรุงรักษา และ `01` คือเซอร์วิสแพ็ค
-G *ipgroupname* **ip=**[**±**]*ip1, ip2...*	ระบชื่อกลุ่ม IP ตามด้วยรายการ IP ที่คั่นด้วยเครื่องหมายคอมม่า
-H	แสดงการบันทึกประวัติ
-i *host*	ระบุ IP แอดเดรส หรือชื่อโฮสต์
-I ip=[**±**]*ip1, ip2...* | [±] host1,host2...	ระบุ IP/ชื่อโฮสต์ที่ต้องละเว้น ระหว่างการตรวจสอบ
-k *filename*	ระบุไฟล์ที่คีย์ใบรับรอง ต้องอ่านในกรณีของการอิมพอร์ต
-p	แสดงตัวอย่างการอัพเดตไคลเอ็นต์ TNC
-P <policyName>	ระบุชื่อนโยบายเพื่อจัดเตรียมรายงานนโยบาย ของไคลเอ็นต์
-q	ยกเลิกข้อมูลส่วนหัว
-r *buildinfo*	สร้างรายงานตามข้อมูลบิลด์ ข้อมูลบิดล์สามารถอยู่ในรูปแบบต่อไปนี้: `6100-04-01` โดย `6100` หมายถึงเวอร์ชัน 6.1, `04` คือ ระดับการบำรุงรักษา และ `01` คือเซอร์วิสแพ็ค
-R	ระบุว่าการดำเนินการมีไว้สำหรับคอมโพเนนต์ IPRef
-s COMPLIANT | IGNORE | FAILED | ALL	แสดงไคลเอ็นต์ตามสถานะดังนี้: **COMPLIANT** แสดงไคลเอ็นต์ที่ทำงานอยู่ **IGNORE** แสดงไคลเอ็นต์ที่ถูกยกเว้นจาการตรวจสอบใดๆ **FAILED** แสดงไคลเอ็นต์ที่มีการตรวจสอบที่ล้มเหลวตาม นโยบายที่กำหนดค่าคอนฟิกไว้ **ALL** แสดงไคลเอ็นต์ทั้งหมดโดยไม่คำนึงถึงสถานะ
-S <host>	ระบุชื่อโฮสต์เพื่อจัดเตรียมรายงานการแก้ไข ที่ปลอดภัยของไคลเอ็นต์
-t TRUSTED | UNTRUSTED	ทำเครื่องหมายไคลเอ็นต์ที่ระบุเป็นไว้วางใจได้หรือไม่ไว้วางใจ **หมายเหตุ:** เฉพาะผู้ดูแลระบบเท่านั้นที่สามารถตรวจสอบเซิร์ฟเวอร์หรือไคลเอ็นต์ว่าเป็นไว้วางใจได้ หรือไม่ไว้วางใจ
-T	ระบุว่าไคลเอ็นต์สามารถยอมรับคำขอ จากเซิร์ฟเวอร์ TS ใดๆ ที่มีใบรับรองที่ถูกต้อง
-u	ถอนการติดตั้งโปรแกรมแก้ไขปัญหาระหว่างเวอร์ชันที่ติดตั้งไว้ บนไคลเอ็นต์ TNC
-v	ระบุรายการโปรแกรมแก้ไขปัญหาระหว่างเวอร์ชันที่คั่นด้วยเครื่องคอมม่า
-V	ระบุชื่อกลุ่มโปรแกรมแก้ไขปัญหาระหว่างเวอร์ชัน

สถานะการออก

คำสั่งนี้จะส่งคืน ค่าการออกดังต่อไปนี้:

รายการ	คำอธิบาย
0	คำสั่งถูกรันสำเร็จ และทำการเปลี่ยนแปลง ที่ร้องขอทั้งหมด
>0	เกิดข้อผิดพลาด ข้อความแสดงข้อผิดพลาดที่พิมพ์ จะมีรายละเอียดเพิ่มเติมเกี่ยวกับชนิดของความล้มเหลว

ตัวอย่าง

1. เพื่อสตาร์ทเซิร์ฟเวอร์ TNC ให้ป้อนคำสั่งต่อไปนี้:

   ```
   psconf start server
   ```

2. เพื่อเพิ่มนโยบายระบบไฟล์ที่ชื่อ 71D_latest สำหรับ บิลด์ 7100-04-02 ให้ป้อนคำสั่งต่อไปนี้:

   ```
   psconf add -F 71D_latest 7100-04-02
   ```

3. เพื่อลบนโยบายระบบไฟล์ที่ชื่อ 71D_old, ให้ป้อนคำสั่งต่อไปนี้:

   ```
   psconf delete -F 71D_old
   ```

4. เพื่อตรวจสอบว่าไคลเอ็นต์ที่มี IP แอดเดรสเท่ากับ 11.11.11.11 เป็น **ไว้วางใจได้** ให้ป้อนคำสั่งต่อไปนี้:

   ```
   psconf certadd -i 11.11.11.11 -t TRUSTED
   ```

5. เพื่อลบไคลเอ็นต์ที่มี IP แอดเดรสเท่ากับ 11.11.11.11 จากเซิร์ฟเวอร์ ให้ป้อนคำสั่งต่อไปนี้:

   ```
   psconf certdel -i 11.11.11.11
   ```

6. เพื่อตรวจสอบข้อมูลไคลเอ็นต์ที่มี IP แอดเดรสเท่ากับ 11.11.11.11 ให้ป้อนคำสั่งต่อไปนี้:

   ```
   psconf verify -i 11.11.11.11
   ```

7. เพื่อแสดงข้อมูลไคลเอ็นต์ที่มี IP แอดเดรสเท่ากับ 11.11.11.11 ให้ป้อนคำสั่งต่อไปนี้:

   ```
   psconf list -i 11.11.11.11
   ```

8. สร้างรายงานสำหรับไคลเอ็นต์ที่อยู่ในสถานะ **COMPLAINT** ให้ป้อนคำสั่งต่อไปนี้:

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

9. เพื่อสร้างรายงานสำหรับบิลด์ 7100-04-02 ให้ป้อนคำสั่งต่อไปนี้:

   ```
   psconf list -r 7100-04-02
   ```

10. เพื่อแสดงประวัติการเชื่อมต่อของไคลเอ็นต์ที่มี IP แอดเดรส เท่ากับ 11.11.11.11 ให้ป้อนคำสั่งต่อไปนี้:

    ```
    psconf list -H -i 11.11.11.11
    ```

11. เพื่อลบรายการไคลเอ็นต์ที่มี IP แอดเดรสเท่ากับ 11.11.11.11 จากประวัติบันทึกที่เก่ากว่า หรือเท่ากับ 1 กุมภาพันธ์ 2009 ให้ป้อนคำสั่งต่อไปนี้:

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

12. เพื่ออิมพอร์ตใบรับรองไคลเอ็นต์ของไคลเอ็นต์ที่มี IP แอดเดรส เท่ากับ 11.11.11.11 จากเซิร์ฟเวอร์ ให้ป้อนคำสั่งต่อไปนี้:

    ```
    psconf import -C -i 11.11.11.11 -f /tmp/client.txt
    ```

13. เพื่อเอ็กซ์พอร์ตใบรับรองเซิร์ฟเวอร์จากไคลเอ็นต์ ให้ป้อนคำสั่ง ต่อไปนี้:

    ```
    psconf export -S -f /tmp/server.txt
    ```

14. เพื่ออัพเดตไคลเอ็นต์ที่มี IP แอดเดรสเท่ากับ 11.11.11.11 เป็นระดับที่เหมาะสมจากเซิร์ฟเวอร์ ให้ป้อนคำสั่งต่อไปนี้:

    ```
    psconf update -i 11.11.11.11
    ```

15. เพื่อแสดงสถานะของไคลเอ็นต์ ให้ป้อนคำสั่งต่อไปนี้:

    ```
    psconf status
    ```

16. เพื่อแสดงใบรับรองของไคลเอ็นต์ ให้ป้อนคำสั่งต่อไปนี้:

    ```
    psconf list -C
    ```

17. สตาร์ทไคลเอ็นต์ ให้ป้อนคำสั่งต่อไปนี้:

    ```
    psconf start client
    ```

ความปลอดภัย

การพิจารณาถึงผู้ใช้ RBAC และผู้ใช้ Trusted AIX :

คำสั่งนี้ สามารถดำเนินการที่ได้รับสิทธิ์ เฉพาะผู้ใช้ที่มีสิทธิ์ที่สามารถรันการดำเนินการ ที่ได้รับสิทธิ์ สำหรับข้อมูลเพิ่มเติมเกี่ยวกับสิทธิ์ และการอนุญาต โปรดดู Privileged Command Database in Security สำหรับรายการสิทธิ์ และการอนุญาตที่เกี่ยวข้องกับคำสั่งนี้ โปรดดูที่คำสั่ง **lssecattr** หรือคำสั่งย่อย **getcmdattr**

คำสั่ง rmvfilt

วัตถุประสงค์

ลบ กฎตัวกรองการข้าม LAN เสมือนจากตารางตัวกรอง

ไวยากรณ์

rmvfilt −n [**fid**|**all**>]

คำอธิบาย

คำสั่ง **rmvfilt** จะถูกใช้เพื่อลบกฎตัวกรอง การข้าม LAN เสมือนออกจากตารางตัวกรอง

แฟล็ก

`-n` ระบุ ID ของกฎตัวกรองที่จะถูกลบ อ็อพชัน `all` จะถูกใช้เพื่อลบกฎตัวกรอง

สถานะการออก

คำสั่งนี้จะส่งคืนค่าการออกดังต่อไปนี้:

`0` เสร็จสมบูรณ์

`>0` เกิดข้อผิดพลาด

ตัวอย่าง

1. เพื่อลบกฎตัวกรองทั้งหมดหรือปิดใช้งานกฎตัวกรองทั้งหมด ในเคอร์เนล ให้พิมพ์คำสั่งต่อไปนี้:

   ```
   rmvfilt -n all
   ```

หลักการที่เกี่ยวข้อง:

"การปิดใช้งานกฎ" ในหน้า 18
คุณสามารถปิดใช้งานกฎที่เปิดใช้การกำหนดเส้นทางข้าม VLAN ในคุณลักษณะ Trusted Firewall

คำสั่ง vlantfw

วัตถุประสงค์

แสดงหรือล้างข้อมูลการแม็พ IP และ Media Access Control (MAC) และควบคุมฟังก์ชันการบันทึก

ไวยากรณ์

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

คำอธิบาย

คำสั่ง **vlantfw** จะแสดงหรือ ล้างไคลเอ็นต์การแม็พ IP และ MAC และยังมีความสามารถ ในการสตาร์ท หรือหยุดแฟซิลิตี้การบันทึกของ Trusted Firewall

แฟล็ก

`-d` แสดงข้อมูลการแม็พ IP ทั้งหมด

`-D` แสดงข้อมูลการเชื่อมต่อที่รวบรวมไว้

`-E` แสดงข้อมูลการเชื่อมต่อระหว่างโลจิคัลพาร์ติชัน (LPARs) บนคอมเพล็กซ์ตัวประมวลผลกลางที่แตกต่างกัน

`-f` ลบข้อมูลการแม็พ IP ทั้งหมด

`-F` ล้างแคชข้อมูลการเชื่อมต่อ

`-G` แสดงกฎตัวกรองที่สามารถกำหนดค่าคอฟนิกเพื่อกำหนดเส้นทาง ทราฟฟิกภายในด้วย Trusted Firewall

`-I` แสดงข้อมูลการเชื่อมต่อระหว่าง LPARs ที่เชื่อมโยงกับ VLAN IDs ที่ต่างกัน แต่แบ่งใช้คอมเพล็กซ์ตัวประมวลผลกลางเดียวกัน

`-l` สตาร์ทแฟลซิลิตี้การบันทึกล็อก Trusted Firewall

`-L` หยุดแฟซลิตี้การบันทึกล็อก Trusted Firewall และเปลี่ยนเส้นทาง เนื้อหาไฟล์การติดตามไปยังไฟล์ `/home/padmin/svm/svm.log`

`-m` เปิดใช้การมอนิเตอร์ Trusted Firewall

`-M` ปิดใช้งานการมอนิเตอร์ Trusted Firewall

`-q` เคียวรีสถานะเครื่องเสมือนที่ปลอดภัย

`-s` สตาร์ท Trusted Firewall

`-t` หยุด Trusted Firewall

พารามิเตอร์

-N *integer*
แสดงกฎตัวกรองที่สอดคล้องกับเลขจำนวนเต็ม ที่ระบุไว้

สถานะการออก

คำสั่งนี้จะส่งคืนค่าการออกดังต่อไปนี้:

0 เสร็จสมบูรณ์

>0 เกิดข้อผิดพลาด

ตัวอย่าง

1. เพื่อแสดงการแม็พ IP ทั้งหมด ให้พิมพ์คำสั่งต่อไปนี้:

   ```
   vlantfw -d
   ```

2. เพื่อลบการแม็พ IP ทั้งหมด ให้พิมพ์คำสั่งต่อไปนี้:

   ```
   vlantfw -f
   ```

3. เพื่อสตาร์ทฟังก์ชันการบันทึกล็อก Trusted Firewall ให้พิมพ์คำสั่งต่อไปนี้:

   ```
   vlantfw -l
   ```

4. เพื่อตรวจสอบสถานะของเครื่องเสมือนที่ปลอดภัย ให้พิมพ์คำสั่ง ต่อไปนี้:

   ```
   vlantfw -q
   ```

5. เพื่อสตาร์ท Trusted Firewall ให้พิมพ์คำสั่งต่อไปนี้:

   ```
   vlantfw -s
   ```

6. เพื่อหยุด Trusted Firewall ให้พิมพ์คำสั่งต่อไปนี้:

   ```
   vlantfw -t
   ```

7. เพื่อแสดงกฎที่สอดคล้องกันที่สามารถ ใช้เพื่อสร้างกฎตัวกรองที่กำหนดเส้นทางทราฟฟิกภายในคอมเพล็กซ์ตัวประมวลผลกลาง ให้พิมพ์คำสั่งต่อไปนี้:

   ```
   vlantfw -G
   ```

สิ่งอ้างอิงที่เกี่ยวข้อง:

"คำสั่ง genvfilt" ในหน้า 37

คำประกาศ

ข้อมูลนี้จัดทำขึ้นสำหรับผลิตภัณฑ์และการบริการที่นำเสนอในสหรัฐอเมริกา

IBM อาจไม่นำเสนอผลิตภัณฑ์ การบริการ หรือคุณลักษณะที่อธิบายในเอกสารนี้ในประเทศอื่นๆ โปรดปรึกษาตัวแทน IBM ในท้องถิ่นของคุณสำหรับข้อมูลเกี่ยวกับผลิตภัณฑ์และการบริการที่มีอยู่ในพื้นที่ของคุณในปัจจุบัน การอ้างอิงใดๆ ถึงผลิตภัณฑ์ โปรแกรม หรือการบริการของ IBM ไม่ได้มีวัตถุประสงค์ที่จะระบุหรือตีความว่าสามารถใช้ได้เฉพาะผลิตภัณฑ์ โปรแกรม หรือการบริการของ IBM เพียงอย่างเดียวเท่านั้น ผลิตภัณฑ์ โปรแกรม หรือการบริการใดๆ ที่สามารถทำงานได้เท่าเทียมกัน และไม่ละเมิดสิทธิทรัพย์สินทางปัญญาของ IBM สามารถนำมาใช้แทนได้ อย่างไรก็ตาม ถือเป็นความรับผิดชอบของผู้ใช้ในการประเมิน และตรวจสอบการดำเนินงานของผลิตภัณฑ์ โปรแกรม หรือการบริการที่ไม่ใช่ของ IBM

IBM อาจมีสิทธิบัตรหรืออยู่ระหว่างการขอสิทธิบัตรที่ครอบคลุมหัวข้อที่อธิบายในเอกสารนี้ การนำเสนอเอกสารนี้ไม่ได้เป็นการมอบใบอนุญาตในสิทธิบัตรดังกล่าวให้แก่คุณ คุณสามารถส่งคำถามเกี่ยวกับใบอนุญาตเป็นลายลักษณ์อักษรไปที่:

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

หากมีคำถามเกี่ยวกับข้อมูลชุดอักขระไบต์คู่ (DBCS) โปรดติดต่อแผยกทรัพย์สินทางปัญญาของ IBM ในประเทศของคุณ หรือส่งคำถามเป็นลายลักษณ์อักษรไปที่ :

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

ย่อหน้าต่อไปนี้ไม่ได้ใช้กับสหราชอาณาจักรหรือประเทศอื่นใดที่ข้อกำหนดดังกล่าวไม่สอดคล้องกับกฎหมายท้องถิ่น: บริษัทธุรกิจระหว่างประเทศนำเสนอสิ่งพิมพ์นี้ "ตามสภาพ" โดยไม่มีการรับประกันใดๆ ไม่ว่าจะเป็นทางตรงหรือทางอ้อม รวมถึงแต่ไม่จำกัดเฉพาะการรับประกันทางอ้อมถึงการไม่ละเมิดสิทธิ การขายได้ หรือความเหมาะสมสำหรับวัตถุประสงค์เฉพาะ เนื่องจากรัฐบางรัฐไม่อนุญาตให้ปฏิเสธการรับประกันทางตรงหรือทางอ้อมในธุรกรรมบางอย่าง ดังนั้น ข้อความนี้จึงอาจจะไม่ใช้กับคุณ

ข้อมูลนี้อาจมีความไม่ถูกต้องด้านเทคนิคหรือข้อผิดพลาดจากการพิมพ์ มีการดำเนินการเปลี่ยนแปลงข้อมูลในเอกสารนี้เป็นครั้งคราว การเปลี่ยนแปลงเหล่านี้จะรวมอยู่ในสิ่งพิมพ์เอดิชันใหม่ IBM อาจปรับปรุงและ/หรือเปลี่ยนแปลงในผลิตภัณฑ์และ/หรือโปรแกรมที่อธิบายไว้ในสิ่งพิมพ์นี้ได้ตลอดเวลาโดยไม่ต้องแจ้งให้ทราบ

การอ้างอิงใด ๆ ในข้อมูลเกี่ยวกับเว็บไซต์ที่ไม่ใช่ของ IBM ถูกนำเสนอเพื่อความสะดวกเท่านั้น และไม่อนุญาตให้กระทำการใด ๆ บนเว็บไซต์ เอกสารประกอบที่เว็บไซต์ดังกล่าวไม่ได้เป็นส่วนประกอบของเอกสารประกอบสำหรับIBM ผลิตภัณฑ์นี้และการใช้เว็บไซต์ดังกล่าวถือเป็นความเสี่ยงของคุณเอง

IBM อาจใช้หรือแจกจ่ายข้อมูลใดๆ ที่คุณให้ในรูปแบบต่างๆ ซึ่ง IBM เชื่อว่ามีความเหมาะสมได้โดยไม่เกิดข้อผูกมัดใดๆ กับคุณ

ผู้รับใบอนุญาตของโปรแกรมนี้ที่ต้องได้รับข้อมูลเกี่ยวกับโปรแกรมเพื่อเปิดใช้งาน: (i) การแลกเปลี่ยนข้อมูลระหว่างโปรแกรมที่สร้างขึ้นอย่างอิสระและโปรแกรมอื่นๆ (รวมถึงโปรแกรมนี้) และ (ii) การใช้ข้อมูลที่มีการแลกเปลี่ยนร่วมกัน ควรติดต่อ:

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

ข้อมูลดังกล่าวอาจพร้อมใช้งานภายใต้ระยะเวลาและเงื่อนไขที่เหมาะสม โดยมีการชำระค่าธรรมเนียมในบางกรณี

โปรแกรมที่ได้รับอนุญาตซึ่งอธิบายไว้ในเอกสารนี้และเอกสารประกอบที่ได้รับอนุญาตทั้งหมดที่มีอยู่มีการนำเสนอโดย IBM ภายใต้ระยะเวลา IBM ข้อตกลงกับลูกค้า IBM ข้อตกลงเกี่ยวกับใบอนุญาตโปรแกรมระหว่างประเทศของ หรือข้อตกลงที่เท่าเทียมใดๆระหว่างเรา

ข้อมูลประสิทธิภาพการทำงานใดๆ ที่มีอยู่ในเอกสารนี้กำหนดขึ้นในสภาพแวดล้อมที่มีการควบคุม ด้วยเหตุนี้ ผลลัพธ์ที่ได้ในสภาพแวดล้อมการดำเนินงานอื่นๆ จึงอาจแตกต่างกันไปอย่างมาก การวัดบางอย่างอาจดำเนินการบนระบบที่อยู่ระหว่างการพัฒนา และไม่มีการรับประกันว่าการวัดดังกล่าวจะเหมือนกันบนระบบต่างๆ ที่มีอยู่โดยทั่วไป ยิ่งไปกว่านั้น การวัดบางอย่างอาจเป็นค่าการประเมินโดยวิธีการประมาณค่านอกช่วง ผลลัพธ์จริงอาจแตกต่างไป ผู้ใช้เอกสารนี้ควรตรวจสอบข้อมูลที่เหมาะสมสำหรับสภาพแวดล้อมเฉพาะของตน

ข้อมูลเกี่ยวกับผลิตภัณฑ์ที่ไม่ใช่ของ IBM ได้มาจากซัพพลายเออร์ของผลิตภัณฑ์เหล่านั้น คำประกาศที่เผยแพร่ หรือแหล่งข้อมูลที่พร้อมใช้งานสำหรับสาธารณะอื่นๆ IBM ไม่ได้ทดสอบผลิตภัณฑ์ดังกล่าว และไม่สามารถยืนยันความถูกต้องของประสิทธิภาพ ความเข้ากันได้ หรือการเรียกร้องอื่นใดที่เกี่ยวข้องกับผลิตภัณฑ์ที่ไม่ใช่ของ IBM หากมีคำถามเกี่ยวกับความสามารถของผลิตภัณฑ์ที่ไม่ใช่ของ IBM ควรสอบถามกับผู้จัดจำหน่ายของผลิตภัณฑ์ดังกล่าว

ข้อความทั้งหมดเกี่ยวกับแนวทางในอนาคตของ IBM หรือความตั้งใจสามารถเปลี่ยนหรือถอดถอนได้โดยไม่ต้องแจ้งให้ทราบ หรือแสดงเป้าหมายและวัตถุประสงค์เท่านั้น

ราคาที่แสดงทั้งหมดของ IBM เป็นราคาเสนอขายปลีกของ IBM ในปัจจุบันและอาจเปลี่ยนแปลงโดยไม่ต้องแจ้งให้ทราบ ผลลัพธ์จริงอาจแตกต่างไป

ข้อมูลนี้สำหรับวัตถุประสงค์การวางแผนเท่านั้น ข้อมูลนี้อาจมีการเปลี่ยนแปลงได้ก่อนที่ผลิตภัณฑ์ดังกล่าวใช้ประโยชน์ได้

ข้อมูลนี้มีตัวอย่างของข้อมูลและรายงานที่ใช้ในการดำเนินธุรกิจประจำวัน เพื่อแสดงข้อมูลให้สมบูรณ์ที่สุดเท่าที่จะเป็นไปได้ ตัวอย่างจึงมีชื่อของแต่ละบุคคล บริษัท ยี่ห้อ และผลิตภัณฑ์ต่างๆ ชื่อทุกชื่อเหล่านี้เป็นชื่อที่แต่งขึ้น และการเหมือนกันกับชื่อและที่อยู่ที่องค์กรธุรกิจจริงใช้งานถือเป็นเรื่องบังเอิญอย่างแท้จริง

ใบอนุญาตลิขสิทธิ์:

ข้อมูลนี้ประกอบด้วยโปรแกรมแอ็พพลิเคชันตัวอย่างในภาษาต้นฉบับ ซึ่งสาธิตเทคนิคการเขียนโปรแกรมบนแพล็ตฟอร์มการดำเนินงานต่างๆ คุณสามารถคัดลอก ดัดแปลง และแจกจ่ายโปรแกรมตัวอย่างเหล่านี้ในรูปแบบต่างๆ ได้โดยไม่ต้องชำระเงินให้แก่ IBM เพื่อใช้สำหรับการพัฒนา การใช้งาน การตลาด หรือการแจกจ่ายโปรแกรมแอ็พพลิเคชันที่สอดคล้องกับอินเตอร์เฟสโปรแกรมแอ็พพลิเคชันของแพล็ตฟอร์มการดำเนินงานที่เขียนโปรแกรมตัวอย่าง ตัวอย่างเหล่านี้ยังไม่ได้ผ่านการทดสอบในทุกสภาพ ดังนั้น IBM จึงไม่สามารถรับประกันหรือแจ้งถึงความน่าเชื่อถือ การให้บริการได้ หรือฟังก์ชันของโปรแกรมเหล่านี้ได้ โปรแกรมตัวอย่างถูกนำเสนอ "ตามสภาพ" โดยไม่มีการรับประกันใดๆ IBM จะไม่รับผิดชอบต่อความเสียหายใดๆซึ่งเกิดจากใช้โปรแกรมตัวอย่าง

สำเนาแต่ละฉบับหรือส่วนใดๆ ของโปรแกรมตัวอย่างเหล่านี้หรืองานที่ต่อเนื่องใดๆ ต้องมีคำประกาศลิขสิทธิ์ดังนี้:

© (ชื่อบริษัทของคุณ) (ปี) ส่วนต่างๆ ของรหัสนี้ได้มาจากโปรแกรมตัวอย่างของ IBM Corp. © Copyright IBM Corp. © ลิขสิทธิ์ IBM Corp. _ป้อนปี_

หากคุณกำลังดูสำเนาชั่วคราวข้อมูลนี้ ภาพถ่ายและภาพประกอบสีอาจไม่ปรากฏ

สิ่งที่ต้องพิจารณาเกี่ยวกับนโยบายความเป็นส่วนตัว

ผลิตภัณฑ์ซอฟต์แวร์ของ IBM รวมถึงโซลูชันบริการระบบซอฟแวร์ ("ข้อเสนอซอฟต์แวร์") อาจใช้คุกกี้หรือเทคโนโลยีอื่นเพื่อรวบรวมข้อมูลการใช้งานผลิตภัณฑ์ เพื่อช่วยในการปรับปรุงประสบการณ์การใช้งานของผู้ใช้ขั้นปลาย เพื่อปรับแต่งการโต้ตอบกับ ผู้ใช้ขั้นปลาย หรือเพื่อวัตถุประสงค์อื่นๆ ในหลายๆ กรณี จะไม่มีการรวบรวม ข้อมูลอัตลักษณ์ส่วนบุคคลโดย ข้อเสนอซอฟต์แวร์ ซึ่งข้อเสนอซอฟต์แวร์บางอย่าง สามารถช่วยให้คุณรวบรวมข้อมูลอัตลักษณ์ ส่วนบุคคลได้ ถ้าข้อเสนอซอฟต์แวร์นี้ใช้คุกกี้ เพื่อรวบรวมข้อมูลอัตลักษณ์, ระบุข้อมูล เกี่ยวกับการใช้คุกกี้ของข้อเสนอนี้ถูกกำหนดไว้ด้านล่าง

ข้อเสนอซอฟต์แวร์นี้ไม่ใช้คุกกี้ หรือเทคโนโลยีอื่นเพื่อรวบรวมข้อมูลอัตลักษณ์ส่วนบุคคล

ถ้าคอนฟิกูเรชันถูกปรับใช้สำหรับ ข้อเสนอกนี้จัดเตรียมให้คุณในฐานะลูกค้าสามารถรวบรวม ข้อมูลอัตลักษณ์ส่วนบุคคลจากผู้ใช้ขั้นปลายผ่านทางคุกกี้ และเทคโนโลยีอื่น คุณควรปรึกษากับที่ปรึกษาด้านกฎหมายเกี่ยวกับ ที่ใช้บังคับในการรวบรวมข้อมูล รวมถึงข้อกำหนดต่างๆ เพื่อการแจ้งเตือนและการยินยอม

สำหรับข้อมูลเพิ่มเติมเกี่ยวกับการใช้ เทคโนโลยีต่างๆ รวมถึงคุกกี้ สำหรับวัตถุประสงค์เหล่านี้ โปรดดู นโยบายความเป็นส่วนตัวของ IBM ที่ http://www.ibm.com/privacy และ คำชี้แจงสิทธิส่วนบุคคลออนไลน์ของ IBM ที่ส่วน http://www.ibm.com/privacy/details "Cookies, Web Beacons and Other Technologies" และ "IBM Software Products and Software-as-a-Service Privacy Statement" ที่ http://www.ibm.com/software/info/product-privacy

เครื่องหมายการค้า

IBM, ตราสัญลักษณ์ IBM , และ ibm.com เป็นเครื่องหมายการค้าหรือเครื่องหมายการค้าที่จดทะเบียนของ International Business Machines Corp. ซึ่งจดทะเบียนในหลายเขตอำนาจศาลทั่วโลก ชื่อผลิตภัณฑ์และการบริการอื่นอาจเป็นเครื่องหมายการค้าของ IBM หรือบริษัทอื่น รายการปัจจุบันของเครื่องหมายการค้า IBM มีอยู่บนเว็บไซต์ที่ ข้อมูลลิขสิทธิ์และเครื่องหมายการค้า ที่ www.ibm.com/legal/copytrade.shtml

Linux เป็นเครื่องหมายการค้าจดทะเบียนของ Linus Torvalds ในสหรัฐอเมริกา ประเทศอื่นๆ หรือทั้งสองกรณี

Java และเครื่องหมายการค้าและตราสัญลักษณ์ที่สร้างขึ้นจาก Java ทั้งหมดเป็นเครื่องหมายการค้าที่จดทะเบียนของ Oracle และ/หรือ บริษัทในเครือ

ดัชนี

A

P

S

T

ก

ข

ค

ซ

ต

น

ป

ภ

ม

ร

ล

ส

อ

พิมพ์ในสหรัฐอเมริกา