IBM PowerSC

Standard Edition

เวอร์ชัน 1.1.4

# PowerSC Standard Edition

IBM PowerSC

Standard Edition

เวอร์ชัน 1.1.4

# PowerSC Standard Edition

**หมายเหตุ**

ก่อนที่คุณจะใช้ข้อมูลนี้และผลิตภัณฑ์ที่สนับสนุน โปรดอ่านข้อมูลใน “คำประกาศ” ในหน้า 191

เอดิชันนี้ใช้กับ IBM PowerSC Standard Edition เวอร์ชัน 1.1.4 และกับ รีลีสและโมดิฟิเคชันต่อมาทั้งหมดจนกว่าจะมีการระบุเป็นอย่างอื่นในเอดิชันใหม่

# สารบัญ

# เกี่ยวกับเอกสารนี้

เอกสารนี้จะมีผู้ดูแลระบบที่มีข้อมูลที่สมบูรณ์ เกี่ยวกับไฟล์ ระบบ และการรักษาความปลอดภัยเครือข่าย

## การไฮไลต์

ระเบียบการไฮไลต์ที่ใช้ในเอกสารนี้มีดังต่อไปนี้:

| | |
|---|---|
| **ตัวหนา** | ระบุคำสั่ง รูทีนย่อย คีย์เวิร์ด ไฟล์ โครงสร้าง ไดเร็กทอรี และไอเท็มอื่นๆ ที่มีชื่อถูกกำหนดไว้ล่วงหน้าโดยระบบ รวมทั้งระบุอ็อบเจ็กต์กราฟิก เช่น ปุ่ม เลเบล และไอคอนที่ผู้ใช้เลือก |
| *ตัวเอน* | ระบุพารามิเตอร์ที่ชื่อแท้จริง หรือค่าจะถูกกำหนดโดยผู้ใช้ |
| ไมโนสเปซ | ระบุตัวอย่างค่าข้อมูลที่ระบุ ตัวอย่างข้อความที่คล้ายกับที่คุณจะเห็นเมื่อถูกแสดง ตัวอย่าง ของส่วนของโค้ดโปรแกรมที่คล้ายกับที่คุณอาจเขียนในฐานะที่เป็นโปรแกรมเมอร์ ข้อความจากระบบ หรือข้อมูลที่คุณควรพิมพ์ |

## การคำนึงถึงขนาดตัวพิมพ์ใน AIX®

ทุกสิ่งในระบบปฏิบัติการ AIX เป็นแบบตรงตาม ตัวพิมพ์ ซึ่งหมายความว่ามีการแยกแยะความแตกต่างระหว่างตัวอักษรพิมพ์ใหญ่ และพิมพ์เล็ก ตัวอย่างเช่น คุณสามารถใช้คำสั่ง **ls** เพื่อ แสดงรายชื่อไฟล์ หากคุณพิมพ์ `LS` ระบบจะตอบกลับ คำสั่งนั้นว่า `not found` ในลักษณะคล้ายกัน `FILEA`, `FiLea` และ `filea` คือชื่อไฟล์สามชื่อที่แตกต่างกัน แม้ว่า ไฟล์เหล่านั้นอยู่ในไดเร็กทอรีเดียวกัน เพื่อหลีกเลี่ยงการเกิดการดำเนินการ แอ็คชันที่ไม่ต้องการ ให้แน่ใจว่าคุณใช้ขนาดตัวพิมพ์ที่ถูกต้องเสมอ

## ISO 9000

ระบบรับรองคุณภาพที่ลงทะเบียน ISO 9000 ใช้ในการพัฒนาและการผลิตผลิตภัณฑ์นี้

# สิ่งใหม่ใน PowerSC Standard Edition 1.1.4

อ่านเกี่ยวกับข้อมูลใหม่ หรือที่เปลี่ยนแปลงอย่างมากสำหรับคอลเล็กชันหัวข้อ PowerSC™ Standard Edition เวอร์ชัน 1.1.4

ในไฟล์ PDF นี้ คุณอาจเห็นแถบ การแก้ไข (|) ในขอบด้านซ้ายที่ระบุข้อมูลใหม่ และข้อมูลที่เปลี่ยนแปลง

## ธันวาคม 2015

- เมข้อมูลเกี่ยวกับโปรไฟล์ความเข้ากันได้ในหัวข้อต่อไปนี้:
  - "ความเชื่อถือได้กับ North American Electric Reliability Corporation" ในหน้า 116
  - "มาตรฐาน Payment Card Industry - Data Security Standard" ในหน้า 93
  - "ความเข้ากันได้ STIG ของกระทรวงกลาโหม" ในหน้า 10
  - "ความเข้ากันได้กับ Sarbanes-Oxley Act และ COBIT" ในหน้า 110
  - "Health Insurance Portability and Accountability Act (HIPAA)" ในหน้า 110
- เพิ่มข้อมูลเกี่ยวกับฟังก์ชัน Real Time Compliance ในหัวข้อ "PowerSC Real Time Compliance" ในหน้า 129
- เพิ่มการดำเนินการ **clientData** และ **default_policy** และแฟล็ก **-l** และ **-g** ในคำสั่ง **psconf**
- อัเดตแฟล็ก **-a, -c, -l** และ **-n** ในคำสั่ง **pscxpert**
- อัพเดตแฟล็ก **-i** และ **-x** ในคำสั่ง **pmconf**

# PowerSC Standard Edition Release Notes เวอร์ชัน 1.1.4

รีลีสโน้ตมีข้อมูลเกี่ยวกับการเปลี่ยนไปเป็น PowerSC Standard Edition เวอร์ชัน 1.1.4 ที่ระบุไว้หลังจากที่เอกสารนี้สมบูรณ์แล้ว

## การเปลี่ยนแปลงชุดไฟล์ PowerSC Standard Edition

PowerSC Express Edition ไม่สามารถซื้อได้จาก IBM® อีกต่อไป PowerSC Standard Edition 1.1.4 หรือใหม่กว่า ประกอบด้วยฟังก์ชัน และคุณลักษณะต่อไปนี้ที่มีให้ก่อนหน้านี้ใน PowerSC Express Edition:

- ความเข้ากันได้ STIG ของกระทรวงกลาโหม
- ความเข้ากันได้กับ Sarbanes-Oxley Act และ COBIT
- ความเข้ากันได้กับ Health Insurance Portability and Accountability Act (HIPAA)
- Real Time Compliance

ตารางต่อไปนี้แสดงชื่อของชุดไฟล์ PowerSC Express Edition ที่ถูกรวมเข้าในชุดไฟล์ PowerSC Standard Edition เวอร์ชัน 1.1.4 หรือใหม่กว่า:

*ตารางที่ 1. ชุดไฟล์ PowerSC Standard Edition 1.1.4 หรือใหม่กว่า*

| PowerSC Express Editionfileset | PowerSC Standard Editionfileset |
|---|---|
| powerscExp.rtc | powerscStd.rtc |
| powerscExp.msg.<LANG> | powerscStd.msg.<LANG> |
| powerscExp.license | powerscStd.license |
| powerscExp.ice | powerscStd.ice |

## อ่านข้อมูลนี้ก่อนการติดตั้ง PowerSC Standard Edition

เมื่อต้องการดูเวอร์ชันล่าสุดของ Release Notes ดูที่ Release Notes ออนไลน์ใน IBM Knowledge Center (http://www.ibm.com/support/knowledgecenter/SSTQK9_1.1.4/com.ibm.powersc114.se/powersc_se_rn.htm)

PowerSC Standard Edition เป็น ไลเซนส์โปรแกรม และไม่รวมอยู่ในระบบปฏิบัติการ AIX

**หมายเหตุ:** ซอฟต์แร์นี้อาจมีข้อผิดพลาดที่อาจส่งผลให้เกิดผลกระทบเชิงธุรกิจ ที่รุนแรง ติดตั้ง โปรแกรมแก้ไขที่มีล่าสุดก่อนใช้ซอฟต์แวร์นี้

## การติดตั้ง การโอนย้าย การอัพเกรด และข้อมูล คอนฟิกูเรชัน

สำหรับข้อมูลเกี่ยวกับการติดตั้ง PowerSC Standard Edition ดูที่ การติดตั้ง PowerSC Standard Edition เวอร์ชัน 1.1.4

สำหรับข้อมูลเกี่ยวกับฮาร์ดแวร์และเวอร์ชันของระบบปฏิบัติการ AIX ที่ใช้ได้สำหรับ PowerSC Standard Edition ดูที่ แนวคิด PowerSC Standard Edition 1.1.4

## ข้อกำหนด ชุดไฟล์เพิ่มเติมสำหรับการรัน Trusted Network Connect

เมื่อต้องการรัน Trusted Network Connect คุณต้องติดตั้งชุดไฟล์ `powerscStd.tnc_commands` ที่พร้อมใช้งานบนดีวีดี IBM PowerSC Standard Edition ของคุณ ติดตั้งชุดไฟล์บนระบบ AIX ของคุณโดยใช้คำสั่ง **installp** ชุดไฟล์นี้มีฟังก์ชันของคำสั่ง **psconf** และ **pmconf**

**หมายเหตุ:** ถ้าคุณกำลังใช้ฟังก์ชัน IP Referrer ของ Trusted Network Connect คุณยังต้อง ติดตั้งชุดไฟล์ `powerscStd.tnc_commands` บนระบบ VIOS ของคุณ

## การเปลี่ยนแปลงคำสั่ง

คำสั่งต่อไปนี้เปลี่ยนแปลง:

- ใน IBM AIX 6 ที่มีเทคโนโลยีระดับ 8 หรือใหม่กว่า คุณสามารถใช้ คำสั่ง **tncconsole** เพื่อรายงานและจัดการเซิร์ฟเวอร์ trusted network connect (TNC), ไคลเอ็นต์ TNC, TNC IP Referrer (IPRef) และ Service Update Management Assistant (SUMA) อย่างไรก็ตาม คำสั่ง **tncconsole** มีฟังก์ชันจำกัด เมื่อต้องการใช้ฟังก์ชันเต็ม ของคำสั่ง **tncconsole** คุณต้องติดตั้ง PowerSC Standard Edition ใน PowerSC Standard Edition ชื่อของคำสั่ง **tncconsole** ถูกเปลี่ยนเป็นคำสั่ง **psconf**
- แฟล็ก **-o** ถูกลบออกจากคำสั่ง **pscxpert**

# แนวคิด PowerSC Standard Edition 1.1.4

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 2. คอมโพเนนต์ PowerSC Standard Edition , คำอธิบาย , การสนับสนุนของระบบปฏิบัติการ และการสนับสนุนทางฮาร์ดแวร์*

| คอมโพเนนต์ | คำอธิบาย | ระบบปฏิบัติการที่สนับสนุน | ฮาร์ดแวร์ที่สนับสนุน |
|---|---|---|---|
| Security and Compliance Automation | การตั้งค่าโดยอัตโนมัติ, การมอนิเตอร์ และการตรวจสอบ คอนฟิกูเรชันของการรักษาความปลอดภัย และการปฏิบัติตามข้อบังคับสำหรับมาตรฐานต่อไปนี้:<br>• Payment Card Industry Data Security Standard (PCI DSS)<br>• มาตรฐาน Sarbanes-Oxley Act และ COBIT (SOX/COBIT)<br>• U.S. Department of Defense (DoD) STIG<br>• Health Insurance Portability and Accountability Act (HIPAA) | • AIX 5.3<br>• AIX 6.1<br>• AIX 7.1 | • POWER5<br>• POWER6®<br>• POWER7®<br>• POWER8 |
| Trusted Boot | วัดค่าอิมเมจการบูต, ระบบปฏิบัติการ และ แอ็พพลิเคชัน และยืนยันความไว้วางใจโดยการใช้เทคโนโลยี Virtual Trusted Platform Module (TPM) | • AIX 6 ที่มี 6100-07 หรือใหม่กว่า<br>• AIX 7 ที่มี 7100-01 หรือใหม่กว่า | POWER7 เฟิร์มแวร์ eFW7.4 หรือใหม่กว่า |
| Trusted Firewall | ประหยัดเวลา และทรัพยากรโดยการเปิดใช้การกำหนดเส้นทาง โดยตรงระหว่าง Virtual LANs (VLANs) ที่ระบุที่ถูกควบคุม โดย Virtual I/O Server เดียวกัน | • AIX 6.1<br>• AIX 7.1<br>• VIOS เวอร์ชัน 2.2.1.4 หรือใหม่กว่า | • POWER6<br>• POWER7<br>• POWER8<br>• Virtual I/O Server เวอร์ชัน 6.1S หรือใหม่กว่า |

*ตารางที่ 2. คอมโพเนนต์ PowerSC Standard Edition , คำอธิบาย , การสนับสนุนของระบบปฏิบัติการ และการสนับสนุนทางฮาร์ดแวร์ (ต่อ)*

| คอมโพเนนต์ | คำอธิบาย | ระบบปฏิบัติการที่สนับสนุน | ฮาร์ดแวร์ที่สนับสนุน |
|---|---|---|---|
| Trusted Logging | ล็อกของ AIX ในปัจจุบันจะอยู่บน Virtual I/O Server (VIOS) ในแบบเรียลไทม์ คุณลักษณะนี้จะมีการบันทึกแบบ Tamper Proof และมีการจัดการและการแบ็กอัพล็อกที่สะดวก | • AIX 5.3<br>• AIX 6.1<br>• AIX 7.1 | • POWER5<br>• POWER6<br>• POWER7<br>• POWER8 |
| การจัดการ Trusted Network Connect และแพตช์ | ตรวจสอบว่าระบบ AIX ทั้งหมดในสภาพแวดล้อมเสมือนจะอยู่ที่ซอฟต์แวร์ ที่ระบุ และระดับแพตช์ และมีเครื่องมือการจัดการเพื่อให้แน่ใจว่า ระบบ AIX ทั้งหมดจะอยู่ที่ระดับซอฟต์แวร์ ที่ระบุ มีการแจ้งเตือนหากมีการเพิ่มระบบเสมือนระดับล่าง ไปยังเครือข่าย หรือหากแพ็กทช์การรักษาความปลอดภัยที่ส่งออกมามีผลกระทบ กับระบบ | • AIX 5.3<br>• AIX 6.1<br>• AIX 7.1<br><br>ไคลเอ็นต์ Trusted Network Connect ต้องการ หนึ่งในคอมโพเนนต์ต่อไปนี้:<br>• AIX 6.1 ที่มี 6100-06 หรือ ใหม่กว่า<br>• ระบบคอนโซล AIX เวอร์ชัน 7.1 Service Update Management Assistant (SUMA) ภายในสภาพแวดล้อม SUMA สำหรับการจัดการแพตช์ | • POWER5<br>• POWER6<br>• POWER7<br>• POWER8 |

# การติดตั้ง PowerSC Standard Edition 1.1.4

คุณต้องติดตั้ง fileset สำหรับแต่ละฟังก์ชันเฉพาะของ PowerSC Standard Edition

filesets ต่อไปนี้จะสามารถใช้ได้สำหรับ PowerSC Standard Edition:

- `powerscStd.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`: ติดตั้งบน AIX เวอร์ชัน 6.1 ที่มีระดับเทคโนโลยี 6100-06 หรือใหม่กว่า หรือบน AIX เวอร์ชัน 7.1 หรือใหม่กว่า ระบบคอนโซล, Service Update Management Assistant (SUMA) ภายในสภาวะแวดล้อม SUMA สำหรับการจัดการแพตช์
- `powerscStd.svm`: ติดตั้งบนระบบ AIX ที่อาจเป็นประโยชน์จากการเรียกใช้ คุณลักษณะของ PowerSC Standard Edition
- `powerscStd.rtc`: ติดตั้งบนระบบ AIX ที่ต้องการคุณลักษณะ Real Time Compliance ของ PowerSC Standard Edition

คุณสามารถติดตั้ง PowerSC Standard Edition โดยใช้หนึ่งใน อินเตอร์เฟสต่อไปนี้:

- 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

ซอฟต์แวร์ไลเซนส์ สามารถดูได้ใน CLI โดยใช้คำสั่งต่อไปนี้:

```
% 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 1.1.4" ในหน้า 5
ภาพรวมนี้ของ PowerSC Standard Edition จะอธิบาย คุณลักษณะ คอมโพเนนต์ และการสนับสนุนทางฮาร์ดแวร์ที่เกี่ยวข้องกับคุณลักษณะ PowerSC Standard Edition

"การติดตั้ง Trusted Boot" ในหน้า 133
มีการกำหนดค่าคอนฟิกทางฮาร์ดแวร์และซอฟต์แวร์บางอย่าง ที่จำเป็นในการติดตั้ง Trusted Boot

"การติดตั้ง Trusted Network Connect" ในหน้า 155
การติดตั้งคอมโพเนนต์ของ Trusted Network Connect (TNC) ต้องการให้คุณดำเนินการบางขั้นตอน

**งานที่เกี่ยวข้อง:**

"การติดตั้ง Trusted Firewall" ในหน้า 141
การติดตั้ง PowerSC Trusted Firewall จะคล้ายกับการติดตั้งคุณลักษณะ PowerSC อื่นๆ

"การติดตั้ง Trusted Logging" ในหน้า 150
คุณสามารถติดตั้งคุณลักษณะ PowerSC Trusted Logging โดยใช้อินเตอร์เฟสบรรทัดคำสั่ง หรือเครื่องมือ SMIT

# ความปลอดภัยและความเข้ากันได้อัตโนมัติ

AIX Profile Manager จัดการโปรไฟล์ที่กำหนดล่วงหน้าสำหรับความปลอดภัยและความเข้ากันได้ PowerSC Real Time Compliance จะมอนิเตอร์ ระบบ AIX ที่เปิดใช้อย่างต่อเนื่อง เพื่อให้แน่ใจว่ามีการกำหนดค่าคอนฟิกอย่างปลอดภัย และต่อเนื่อง

โปรไฟล์ XML ทำให้การกำหนดคอนฟิกระบบ AIX ที่แนะนำของ IBM สอดคล้องกับ Payment Card Data Security Standard, Sarbanes-Oxley Act, หรือ U.S. Department of Defense UNIX Security Technical Implementation Guide และ Health Insurance Portability and Accountability Act (HIPAA) โดยอัตโนมัติ องค์กรที่เป็นไปตามมาตรฐาน การรักษาความปลอดภัยต้องใช้การตั้งค่าการรักษาความปลอดภัยระบบที่กำหนดไว้ล่วงหน้า

AIX Profile Manager จะทำงานเป็นปลั๊กอิน IBM Systems Director ที่ช่วยให้ง่ายต่อการปรับใช้การตั้งค่าการรักษาความปลอดภัย การมอนิเตอร์ การตั้งค่าการรักษาความปลอดภัย และการตั้งค่าการรักษาความปลอดภัยการตรวจสอบสำหรับทั้งระบบปฏิบัติการ AIX และระบบ Virtual I/O Server (VIOS) เมื่อต้องการใช้คุณลักษณะความเข้ากันได้ของการรักษาความปลอดภัย แอ็พพลิเคชัน PowerSC ต้องถูกติดตั้งบนระบบที่ถูกจัดการ AIX ที่เป็นไปตามมาตรฐาน ความเข้ากันได้ คุณลักษณะ Security and Compliance Automation ถูกรวมใน PowerSC Standard Edition

แพ็กเกจการติดตั้ง PowerSC Standard Edition, 5765-PSE ต้องติดตั้งบนระบบที่ถูกจัดการ AIX แพ็กเกจการติดตั้งจะติดตั้งชุดไฟล์ `powerscStd.ice` ที่ สามารถใช้บนระบบโดยใช้ AIX Profile Manager หรือ คำสั่ง **pscxpert** PowerSC ที่มีมาตรฐาน IBM Compliance Expert Express (ICEE) จะถูกเปิดใช้เพื่อจัดการและปรับปรุงโปรไฟล์ XML โปรไฟล์ XML ถูกจัดการโดย AIX Profile Manager

**หมายเหตุ:** ติดตั้งแอ็พพลิเคชันทั้งหมดบนระบบก่อนที่คุณจะใช้โปรไฟล์ ความปลอดภัย

## แนวคิดของความปลอดภัยและความเข้ากันได้อัตโนมัติ

คุณลักษณะการรักษาความปลอดภัย PowerSC และความเข้ากันได้เป็นวิธีการอัตโนมัติในการกำหนดคอนฟิกและตรวจสอบระบบ AIX ตาม U.S. Department of Defense (DoD) Security Technical Implementation Guide (STIG), Payment Card Industry (PCI) data security standard (DSS), Sarbanes-Oxley act, COBIT compliance (SOX/COBIT) และ Health Insurance Portability and Accountability Act (HIPAA)

PowerSC ช่วยให้การกำหนดคอนฟิก และติดตามระบบโดยอัตโนมัติ ต้องเข้ากันได้กับมาตรฐานความปลอดภัยข้อมูล (DSS) Payment Cad Industy (PCI) เวอร์ชัน 1.2, 2.0 หรือ 3.0 ดังนั้น คุณลักษณะการรักษาความปลอดภัยและความเข้ากันได้กับ PowerSC เป็นเมธอดความถูกต้อง และความเข้ากันได้ของการทำให้ การกำหนดคอนฟิกการรักษาความปลอดภัยอัตโนมัติที่ใช้เพื่อให้ตรงตามข้อกำหนดความเข้ากันได้ด้าน IT ของ DoD UNIX STIG, PCI DSS, Sarbanes-Oxley act, COBIT compliance (SOX/COBIT) และ Health Insurance Portability and Accountability Act (HIPAA)

**หมายเหตุ:** การอัพเดตการรักษาความปลอดภัย และความเข้ากันได้ PowerSC ของโปรไฟล์ xml ที่มีอยู่ ที่ใช้โดยเอดิชัน IBM Compliance Expert express (ICEE) คุณสามารถใช้โปรไฟล์ PowerSC Standard Edition XML ด้วยคำสั่ง **pscxpert** คล้ายกับ ICEE

โปรไฟล์ความเข้ากันได้ที่กำหนดคอนฟิกล่วงหน้าถูกจัดส่งพร้อม PowerSC Standard Edition ช่วยลดเวิร์กโหลดของการควบคุมดูแลสำหรับการตีความเอกสารคู่มือความเข้ากันได้ และการอิมพลีเมนต์มาตรฐานพารามิเตอร์ของคอนฟิกูเรชันระบบที่ระบุ เทคโนโลยีนี้ช่วยลดค่าใช้จ่ายในการกำหนดคอนฟิกความเข้ากันได้ และการตรวจสอบโดยกระบวนการอัตโนมัติ IBMPowerSC Standard Edition ถูกออกแบบมาเพื่อช่วยจัดการข้อกำหนดระบบที่สัมพันธ์กับความเข้ากันได้ มาตรฐานอย่างมีประสิทธิภาพ ที่สามารถลด ค่าใช้จ่ายและเพิ่มความเข้ากันได้

## ความเข้ากันได้ STIG ของกระทรวงกลาโหม

กระทรวงกลาโหมของประเทศสหรัฐอเมริกา (DoD) ต้องการระบบคอมพิวเตอร์ ที่มีความปลอดภัยสูง ระดับการรักษาความปลอดภัย และคุณภาพนี้กำหนดโดย DoD เป็นไปตามคุณภาพและลูกค้าตาม AIX บนเซิร์ฟเวอร์ Power Systems™

ระบบปฏิบัติการแบบปลอดภัย เช่น AIX ต้องถูกกำหนดคอนฟิกอย่างถูกต้องเพื่อให้เป็นไปตาม เป้าหมายการรักษาความปลอดภัยที่ระบุ DoD จดจำ ความต้องการคอนฟิกูเรชันความปลอดภัยของระบบปฏิบัติการทั้งหมดในคำสั่ง 8500.1 คำสั่งนี้สร้างนโยบายและกำหนดความรับผิดชอบต่อ Defense Information Security Agency (DISA) ของสหรัฐเพื่อจัดเตรียมคำแนะนำ ในการคอนฟิกูเรชันความปลอดภัย

DISA ได้พัฒนาหลักการและแนวทางใน UNIX Security Technical Implementation Guide (STIG) ที่จัดให้มีสภาวะแวดล้อมที่ตรงตามหรือ สูงกว่าข้อกำหนดด้านความปลอดภัยของระบบ DoD ซึ่งดำเนินการ ที่ระดับ Mission Assurance Category (MAC) II ที่สำคัญ โดยที่มีข้อมูลที่สำคัญ DoD ของสหรัฐเข้มงวดในเรื่องของข้อกำหนดด้านความปลอดภัยของ IT และมีรายละเอียดของค่าติดตั้งคอนฟิกูเรชันที่จำเป็น เพื่อมั่นใจว่า ระบบทำงานด้วยความปลอดภัย คุณสามารถ ยกระดับคำแนะนำของผู้เชี่ยวชาญที่จำเป็น PowerSC Standard Edition ช่วยให้ กระบวนการกำหนดคอนฟิกค่าติดตั้งอัตโนมัติตามที่กำหนดโดย DoD

**หมายเหตุ:** ไฟล์สคริปต์แบบกำหนดเองทั้งหมดซึ่งได้จัดให้มี เพื่อเก็บรักษาความเข้ากันได้กับ DoD ในไดเร็กทอรี `/etc/security/pscexpert/dodv2`

PowerSC Standard Edition สนับสนุน ข้อกำหนดของเวอร์ชัน 1 รีลีส 2 ของ AIX DoD STIG ข้อสรุปของข้อกำหนดและวิธีการตรวจสอบให้เกิดความมั่นใจว่า มีความสอดคล้องกันจะอยู่ในตารางต่อไปนี้

*ตารางที่ 3. ข้อกำหนดทั่วไปของ DoD*

| ID จุดตรวจสอบของ Department of Defense STIG | หมวดหมู่ของกฎ STIG | รายละเอียด | ตำแหน่งของสคริปต์ที่นิยามแอ็คชัน และผลลัพธ์ของแอ็คชันที่เปิดใช้งานความเข้ากันได้ |
|---|---|---|---|
| AIX00020 | 2 | ซอฟต์แวร์ AIX Trusted Computing Base จำเป็นต้องถูกติดตั้งไว้ | **ตำแหน่ง** `/etc/security/pscexpert/dodv2/trust`<br>**แอ็คชันความเข้ากันได้**<br>ตรวจสอบให้แน่ใจว่า ระบบตรงกับข้อกำหนดที่ระบุไว้ |
| AIX00040 | 2 | คำสั่ง **securetcpip** ต้องถูกนำมาใช้ | **ตำแหน่ง** `/etc/security/pscexpert/dodv2/dodsecuretcpip`<br>**แอ็คชันความเข้ากันได้**<br>ตรวจสอบให้แน่ใจว่า ระบบตรงกับข้อกำหนดที่ระบุไว้ |

*ตารางที่ 3. ข้อกำหนดทั่วไปของ DoD (ต่อ)*

| ID จุดตรวจสอบของ Department of Defense STIG | หมวดหมู่ของกฎ STIG | รายละเอียด | ตำแหน่งของสคริปต์ที่นิยามแอ็คชัน และผลลัพธ์ของแอ็คชันที่เปิดใช้งานความเข้ากันได้ |
|---|---|---|---|
| AIX00060 | 2 | ระบบต้องถูกตรวจสอบทุกสัปดาห์สำหรับไฟล์ `setuid` ที่ไม่ได้รับสิทธิ์ และโมดิฟิเคชันที่ไม่ได้รับสิทธิ์เพื่อให้สิทธิ์กับไฟล์ `setuid` | **ตำแหน่ง** `/etc/security/pscexpert/dodv2/trust`<br>**แอ็คชันความเข้ากันได้** ตรวจสอบทุกสัปดาห์เพื่อระบุความเปลี่ยนแปลงกับไฟล์ ที่ระบุไว้ |
| AIX00080 | 1 | แอ็ตทริบิวต์ `SYSTEM` ต้องไม่ถูกตั้งค่าเป็น *none* สำหรับแอคเคาต์ใดๆ | **ตำแหน่ง** `/etc/security/pscexpert/dodv2/SYSattr`<br>**แอ็คชันความเข้ากันได้** ตรวจสอบให้แน่ใจว่า แอ็ตทริบิวต์ที่ระบุถูกตั้งที่ไม่ใช่ *none*<br>**หมายเหตุ:** ค่าติดตั้งนี้ไม่ได้ถูกเปลี่ยนโดยอัตโนมัติเมื่อรีเซ็ตนโยบายเป็น นโยบายดีฟอลต์ของ AIX โดยใช้ไฟล์ `DoDv2_to_AIXDefault.xml` คุณต้องเปลี่ยนค่าติดตั้งนี้แบบแมนวล |
| AIX00200 | 2 | ระบบต้องไม่อนุญาตให้บอร์ดคาสก์โดยตรง เพื่อย้ายผ่านเกตเวย์ | **ตำแหน่ง** `/etc/security/pscexpert/dodv2/ntwkoptsdod`<br>**แอ็คชันความเข้ากันได้** ตั้งค่าอ็อพชันเครือข่าย `direct_broadcast` ไปเป็น *0* |
| AIX00210 | 2 | ระบบต้องจัดเตรียมการป้องกันการจู่โจมจาก Internet Control Message Protocol (ICMP) บนการเชื่อมต่อ TCP | **ตำแหน่ง** `/etc/security/pscexpert/dodv2/ntwkoptsdod`<br>**แอ็คชันความเข้ากันได้** ตั้งค่าอ็อพชันเครือข่าย `tcp_icmpsecure` เป็น *1* |
| AIX00220 | 2 | ระบบต้องจัดเตรียมการป้องกันสำหรับสแต็ก TCP กับการรีเซ็ตการเชื่อมต่อ ซิงโครไนซ์ (SYN) และการติดไวรัส ของข้อมูล | **ตำแหน่ง** `/etc/security/pscexpert/dodv2/ntwkoptsdod`<br>**แอ็คชันความเข้ากันได้** ตรวจสอบให้แน่ใจว่า ค่าสำหรับอ็อพชัน `tcp_tcpsecure` ถูกตั้งค่าเป็น *7* |
| AIX00230 | 2 | ระบบต้องจัดเตรียมการป้องกันการจู่โจมการทำแฟรกเมนต์ IP | **ตำแหน่ง** `/etc/security/pscexpert/dodv2/ntwkoptsdod`<br>**แอ็คชันความเข้ากันได้** ตั้งค่าอ็อพชันเครือข่าย `ip_nfrag` เป็น *200* |

*ตารางที่ 3. ข้อกำหนดทั่วไปของ DoD (ต่อ)*

| ID จุดตรวจสอบของ Department of Defense STIG | หมวดหมู่ของกฎ STIG | รายละเอียด | ตำแหน่งของสคริปต์ที่นิยามแอ็คชัน และผลลัพธ์ของแอ็คชันที่เปิดใช้งานความเข้ากันได้ |
|---|---|---|---|
| AIX00300 | 1,2,3 | ระบบไม่ต้องการให้เซอร์วิส bootp แอ็คทีฟ | **ตำแหน่ง** `/etc/security/pscexpert/dodv2/inetdservices`<br>**แอ็คชันความเข้ากันได้**<br>ปิดใช้งานเซอร์วิสที่ระบุ |
| AIX00310 | 2 | ไฟล์ `/etc/ftpaccess.ctl` ต้องมีอยู่ | **ตำแหน่ง** `/etc/security/pscexpert/dodv2/dodv2loginherald`<br>**แอ็คชันความเข้ากันได้**<br>ตรวจสอบให้แน่ใจว่า ไฟล์มีอยู่จริง |
| GEN000020 | 2 | ระบบต้องมีการพิสูจน์ตัวตน เมื่อเริ่มต้นโหมดผู้ใช้เดี่ยว | **ตำแหน่ง** `/etc/security/pscexpert/dodv2/rootpasswd_home`<br>**แอ็คชันความเข้ากันได้**<br>ตรวจสอบให้แน่ใจว่า แอคเคาต์สำหรับพาร์ติชันที่สามารถบูตได้มีรหัสผ่านอยู่ในไฟล์ `/etc/security/passwd`<br>**หมายเหตุ:** ค่าติดตั้งนี้ไม่ได้ถูกเปลี่ยนโดยอัตโนมัติเมื่อรีเซ็ตนโยบายเป็น นโยบายดีฟอลต์ของ AIX โดยใช้ไฟล์ `DoDv2_to_AIXDefault.xml` คุณต้องเปลี่ยนค่าติดตั้งนี้แบบแมนวล |
| GEN000100 | 1 | ระบบปฏิบัติการต้องสนับสนุน รีลีส | **ตำแหน่ง** `/etc/security/pscexpert/dodv2/dodv2cat1`<br>**แอ็คชันความเข้ากันได้**<br>แสดงผลลัพธ์ของการทดสอบกฎที่ระบุเฉพาะ |
| GEN000120 | 2 | แพตช์และอัพเดตความปลอดภัยของระบบปัจจุบันโดยส่วนใหญ่ ต้องถูกติดตั้งไว้ | **ตำแหน่ง** `/usr/sbin/instfix -i`<br>`/etc/security/pscexpert/dodv2/dodv2cat1`<br>**แอ็คชันความเข้ากันได้**<br>กำหนดคอนฟิกนี้โดยใช้คุณลักษณะ Trusted Network Connect |

*ตารางที่ 3. ข้อกำหนดทั่วไปของ DoD (ต่อ)*

| ID จุดตรวจสอบของ Department of Defense STIG | หมวดหมู่ของกฎ STIG | รายละเอียด | ตำแหน่งของสคริปต์ที่นิยามแอ็คชัน และผลลัพธ์ของแอ็คชันที่เปิดใช้งานความเข้ากันได้ |
|---|---|---|---|
| GEN000140 | 2 | ระบบต้องถูกตรวจสอบทุกสัปดาห์สำหรับไฟล์ setuid ที่ไม่ได้รับสิทธิ์ และโมดิฟิเคชันที่ไม่ได้รับสิทธิ์เพื่อให้สิทธิ์กับไฟล์ setuid | **ตำแหน่ง** /etc/security/pscexpert/dodv2/trust<br>**แอ็คชันความเข้ากันได้** ตรวจสอบทุกสัปดาห์เพื่อระบุความเปลี่ยนแปลงกับไฟล์ที่ระบุไว้ |
| GEN000220 | 2 | ระบบต้องถูกตรวจสอบทุกสัปดาห์สำหรับไฟล์ setuid ที่ไม่ได้รับสิทธิ์ และโมดิฟิเคชันที่ไม่ได้รับสิทธิ์เพื่อให้สิทธิ์กับไฟล์ setuid | **ตำแหน่ง** /etc/security/pscexpert/dodv2/trust<br>**แอ็คชันความเข้ากันได้** ตรวจสอบทุกสัปดาห์เพื่อระบุความเปลี่ยนแปลงกับไฟล์ที่ระบุไว้ |
| GEN000240 | 2 | นาฬิกาของระบบต้องถูกซิงโครไนซ์กับแหล่งข้อมูลเวลา Department of Defense (DoD) ที่ได้รับสิทธิ์ | **ตำแหน่ง** /etc/security/pscexpert/dodv2/dodv2cmntrows<br>**แอ็คชันความเข้ากันได้** ตรวจสอบให้แน่ใจว่า เวลาของระบบสอดคล้องกัน |
| GEN000241 | 2 | นาฬิกาของระบบต้องถูกซิงโครไนซ์อย่างต่อเนื่อง หรืออย่างน้อยทุกวัน | **ตำแหน่ง** /etc/security/pscexpert/dodv2/dodv2cmntrows<br>**แอ็คชันความเข้ากันได้** ตรวจสอบให้แน่ใจว่า เวลาของระบบสอดคล้องกัน |
| GEN000242 | 2 | ระบบต้องใช้แหล่งข้อมูลเวลาอย่างน้อยสองแหล่ง สำหรับการซิงโครไนซ์นาฬิกา | **ตำแหน่ง** /etc/security/pscexpert/dodv2/dodv2netrules<br>**แอ็คชันความเข้ากันได้** ตรวจสอบให้แน่ใจว่ามีแหล่งข้อมูลเวลามากกว่าหนึ่งแหล่งที่ต้องถูกใช้สำหรับการซิงโครไนซ์นาฬิกา |
| GEN000280 | 2 | การล็อกอินโดยตรงไปยังชนิดของแอคเคาต์ต่อไปนี้ไม่ได้รับอนุญาต:<br>• แอ็พพลิเคชัน<br>• ค่าดีฟอลต์<br>• แบ่งใช้<br>• ยูทิลิตี | **ตำแหน่ง** /etc/security/pscexpert/dodv2/lockacc_rlogin<br>**แอ็คชันความเข้ากันได้** จัดเตรียมการล็อกอินโดยตรงไปยังแอคเคาต์ที่ระบุเฉพาะ |

*ตารางที่ 3. ข้อกำหนดทั่วไปของ DoD (ต่อ)*

| ID จุดตรวจสอบของ Department of Defense STIG | หมวดหมู่ของกฎ STIG | รายละเอียด | ตำแหน่งของสคริปต์ที่นิยามแอ็คชัน และผลลัพธ์ของแอ็คชันที่เปิดใช้งานความเข้ากันได้ |
|---|---|---|---|
| GEN000290 | 2 | ระบบต้องไม่มีแอคเคาต์ที่ไม่จำเป็น | **ตำแหน่ง** `/etc/security/pscexpert/dodv2/lockacc_rlogin`<br>**แอ็คชันความเข้ากันได้**<br>ตรวจสอบให้แน่ใจว่าไม่มีแอคเคาต์ที่ไม่ได้ใช้งาน |
| GEN000300 (เกี่ยวข้องกับ GEN000320, GEN000380, GEN000880) | 2 | แอคเคาต์ทั้งหมดบนระบบต้องเป็นผู้ใช้หรือชื่อแอคเคาต์ที่ไม่ซ้ำกัน และรหัสผ่านผู้ใช้หรือรหัสผ่านแอคเคาต์ที่ไม่ซ้ำกัน | **ตำแหน่ง** `/etc/security/pscexpert/dodv2/grpusrpass_chk`<br>**แอ็คชันความเข้ากันได้**<br>ตรวจสอบให้แน่ใจว่าแอคเคาต์ทั้งหมดตรงกับข้อกำหนดที่ระบุไว้เฉพาะ<br>**หมายเหตุ:** ค่าติดตั้งนี้ไม่ได้ถูกเปลี่ยนโดยอัตโนมัติเมื่อรีเซ็ตนโยบายเป็น นโยบายดีฟอลต์ของ AIX โดยใช้ไฟล์ `DoDv2_to_AIXDefault.xml` คุณต้องเปลี่ยนค่าติดตั้งนี้แบบแมนวล |
| GEN000320 (เกี่ยวข้องกับ GEN000300, GEN000380, GEN000880) | 2 | แอคเคาต์ทั้งหมดบนระบบต้องเป็นผู้ใช้หรือชื่อแอคเคาต์ที่ไม่ซ้ำกัน และรหัสผ่านผู้ใช้หรือรหัสผ่านแอคเคาต์ที่ไม่ซ้ำกัน | **ตำแหน่ง** `/etc/security/pscexpert/dodv2/grpusrpass_chk`<br>**แอ็คชันความเข้ากันได้**<br>ตรวจสอบให้แน่ใจว่าแอคเคาต์ทั้งหมดตรงกับข้อกำหนดที่ระบุไว้เฉพาะ<br>**หมายเหตุ:** ค่าติดตั้งนี้ไม่ได้ถูกเปลี่ยนโดยอัตโนมัติเมื่อรีเซ็ตนโยบายเป็น นโยบายดีฟอลต์ของ AIX โดยใช้ไฟล์ `DoDv2_to_AIXDefault.xml` คุณต้องเปลี่ยนค่าติดตั้งนี้แบบแมนวล |
| GEN000340 | 2 | User IDs (UIDs) และ Group IDs (GIDs) ที่ถูกสงวนไว้สำหรับแอคเคาต์ระบบต้องไม่ถูกกำหนดให้กับแอคเคาต์ที่ไม่ใช่แอคเคาต์ของระบบ หรือกลุ่มที่ไม่ใช่กลุ่มของระบบ | **ตำแหน่ง** `/etc/security/pscexpert/dodv2/account`<br>**แอ็คชันความเข้ากันได้**<br>ค่าติดตั้งถูกเปิดใช้งานโดยอัตโนมัติเพื่อบังคับใช้กฎนี้ |

*ตารางที่ 3. ข้อกำหนดทั่วไปของ DoD (ต่อ)*

| ID จุดตรวจสอบของ Department of Defense STIG | หมวดหมู่ของกฎ STIG | รายละเอียด | ตำแหน่งของสคริปต์ที่นิยามแอ็คชัน และผลลัพธ์ของแอ็คชันที่เปิดใช้งานความเข้ากันได้ |
|---|---|---|---|
| GEN000360 | 2 | UIDs และ GIDs ที่ถูกสงวนไว้สำหรับแอคเคาต์ของระบบ ต้องไม่ถูกกำหนดให้กับแอคเคาต์ที่ไม่ใช่แอคเคาต์ของระบบหรือกลุ่มที่ไม่ใช่ กลุ่มของระบบ | **ตำแหน่ง** `/etc/security/pscexpert/dodv2/account`<br>**แอ็คชันความเข้ากันได้** ค่าติดตั้งนี้เปิดใช้งานโดยอัตโนมัติเพื่อบังคับใช้กฎนี้ |
| GEN000380 (เกี่ยวข้องกับ GEN000300, GEN000320, GEN000880) | 2 | แอคเคาต์ทั้งหมดบนระบบต้องเป็นผู้ใช้หรือชื่อแอคเคาต์ที่ไม่ซ้ำกัน และรหัสผ่านผู้ใช้หรือรหัสผ่านแอคเคาต์ที่ไม่ซ้ำกัน | **ตำแหน่ง** `/etc/security/pscexpert/dodv2/grpusrpass_chk`<br>**แอ็คชันความเข้ากันได้** ตรวจสอบให้แน่ใจว่าแอคเคาต์ทั้งหมดตรงกับข้อกำหนดที่ระบุไว้เฉพาะ |
| GEN000400 | 2 | แบนเนอร์ล็อกอิน Department of Defense (DoD) ต้องถูกแสดงในทันทีก่อนหรือเป็นส่วนหนึ่งของพร้อมต์ล็อกอิน คอนโซล | **ตำแหน่ง** `/etc/security/pscexpert/dodv2/dodv2loginherald`<br>**แอ็คชันความเข้ากันได้** แสดงแบนเนอร์ที่ต้องการ |
| GEN000402 | 2 | แบนเนอร์ล็อกอิน DoD ต้องถูกแสดงในทันที ก่อน หรือเป็นส่วนหนึ่งของพร้อมต์ล็อกอินสภาวะแวดล้อมเดสก์ท็อปแบบกราฟิก | **ตำแหน่ง** `/etc/security/pscexpert/dodv2/dodv2loginherald`<br>**แอ็คชันความเข้ากันได้** แบนเนอร์ล็อกอินถูกตั้งค่าเป็นแบนเนอร์ Department of Defense |
| GEN000410 | 2 | เซอร์วิส File Transfer Protocol over SSL (FTPS) หรือ File Transfer Protocol (FTP) บนระบบต้องถูกต้องค่าด้วยแบนเนอร์ล็อกอิน DoD | **ตำแหน่ง** `/etc/security/pscexpert/dodv2/dodv2loginherald`<br>**แอ็คชันความเข้ากันได้** แสดงแบนเนอร์เมื่อคุณใช้ FTP |
| GEN000440 | 2 | ความพยายามในการล็อกอินหรือล็อกเอาต์ที่สำเร็จหรือไม่สำเร็จ ต้องถูกบันทึก | **ตำแหน่ง** `/etc/security/pscexpert/dodv2/loginout`<br>**แอ็คชันความเข้ากันได้** เปิดใช้งานการล็อกที่จำเป็น |
| GEN000452 | 2 | ระบบต้องแสดงวันที่และเวลาล็อกอินแอคเคาต์ล่าสุดที่เป็นผลสำเร็จ ในแต่ละครั้งที่ล็อกอิน | **ตำแหน่ง** `/etc/security/pscexpert/dodv2/sshDoDconfig`<br>**แอ็คชันความเข้ากันได้** แสดงข้อมูลที่จำเป็น |

*ตารางที่ 3. ข้อกำหนดทั่วไปของ DoD (ต่อ)*

| ID จุดตรวจสอบของ Department of Defense STIG | หมวดหมู่ของกฎ STIG | รายละเอียด | ตำแหน่งของสคริปต์ที่นิยามแอ็คชัน และผลลัพธ์ของแอ็คชันที่เปิดใช้งานความเข้ากันได้ |
|---|---|---|---|
| GEN000460 | 2 | กฎนี้ปิดใช้งานแอคเคาต์หลังจากพยายามล็อกออนด้วยความล้มเหลวติดต่อกัน 3 ครั้ง | **ตำแหน่ง** `/etc/security/pscexpert/dodv2/chusrattrdod`<br>**แอ็คชันความเข้ากันได้** ตั้งค่าข้อจำกัดของความพยายามในการล็อกอินตามค่าที่ระบุไว้ |
| GEN000480 | 2 | กฎนี้ตั้งค่าเวลาหน่วงของการล็อกอินไว้ 4 วินาที | **ตำแหน่ง** `/etc/security/pscexpert/dodv2/chdefstanzadod`<br>**แอ็คชันความเข้ากันได้** ตั้งค่าเวลาหน่วงของการล็อกอินไว้เป็นค่าต้องการ |
| GEN000540 | 2 | ค่านี้ทำให้มั่นใจได้ว่า การกำหนดค่าของไฟล์คอนฟิกูเรชันสำหรับ รหัสผ่านโกลบอลของระบบเป็นไปตามข้อกำหนดเกี่ยวกับรหัสผ่าน | **ตำแหน่ง** `/etc/security/pscexpert/dodv2/chusrattrdod`<br>**แอ็คชันความเข้ากันได้** ตั้งค่ารหัสผ่านที่ต้องการ |
| GEN000560 | 1 | แอคเคาต์ทั้งหมดบนระบบต้องมี รหัสผ่านที่ถูกต้อง | **ตำแหน่ง** `/etc/security/pscexpert/dodv2/grpusrpass_chk`<br>**แอ็คชันความเข้ากันได้** ตรวจสอบให้แน่ใจว่า แอคเคาต์มีรหัสผ่าน |
| GEN000580 | 2 | กฎนี้ทำให้มั่นใจได้ว่า รหัสผ่านทั้งหมดมีอักขระ อย่างน้อยที่สุด 14 ตัวอักษร | **ตำแหน่ง** `/etc/security/pscexpert/dodv2/chusrattrdod`<br>**แอ็คชันความเข้ากันได้** ตั้งค่าความยาวรหัสผ่านต่ำสุดเป็น 14 ตัวอักษร |
| GEN000585 | 2 | ระบบต้องใช้ Federal Information Processing Standards (FIPS) 140-2 ที่ได้รับการอนุมัติในส่วนของอัลกอริทึมการแฮชของการเข้ารหัส สำหรับการสร้างการแฮชรหัสผ่านแอคเคาต์ | **ตำแหน่ง** `/etc/security/pscexpert/dodv2/fipspasswd`<br>**แอ็คชันความเข้ากันได้** ตรวจสอบให้แน่ใจว่า การแฮชรหัสผ่านใช้อัลกอริทึมการแฮชที่ได้รับอนุญาต |

*ตารางที่ 3. ข้อกำหนดทั่วไปของ DoD (ต่อ)*

| ID จุดตรวจสอบของ Department of Defense STIG | หมวดหมู่ของกฎ STIG | รายละเอียด | ตำแหน่งของสคริปต์ที่นิยามแอ็คชัน และผลลัพธ์ของแอ็คชันที่เปิดใช้งานความเข้ากันได้ |
|---|---|---|---|
| GEN000590 | 2 | ระบบต้องใช้ FIPS 140-2 ที่ได้รับการอนุมัติ ในส่วนของอัลกอริทึมการแฮชของการเข้ารหัสสำหรับการสร้างการแฮชรหัสผ่านแอคเคาต์ | **ตำแหน่ง** `/etc/security/pscexpert/dodv2/fipspasswd`<br>**แอ็คชันความเข้ากันได้** ตรวจสอบให้แน่ใจว่า การแฮชรหัสผ่านใช้อัลกอริทึมการแฮชที่ได้รับอนุญาต |
| GEN000595 | 2 | ใช้ FIPS 140-2 ที่ได้รับการอนุมัติในส่วนของ อัลกอริทึมการแฮชของการเข้ารหัสผ่านเมื่อสร้างการแฮชรหัสผ่านที่ถูกเก็บไว้บนระบบ | **ตำแหน่ง** `/etc/security/pscexpert/dodv2/fipspasswd`<br>**แอ็คชันความเข้ากันได้** ตรวจสอบให้แน่ใจว่า การแฮชรหัสผ่านใช้อัลกอริทึมการแฮชที่ได้รับอนุญาต |
| GEN000640 | 2 | กฎนี้ต้องการอักขระที่ไม่ใช่ตัวอักษรอย่างน้อยหนึ่งตัว ในรหัสผ่าน | **ตำแหน่ง** `/etc/security/pscexpert/dodv2/chusrattrdod`<br>**แอ็คชันความเข้ากันได้** ตั้งค่าจำนวนต่ำสุดของอักขระที่ไม่ใช่ตัวอักษรในรหัสผ่าน เป็น 1 |
| GEN000680 | 2 | กฎนี้ทำให้มั่นใจว่า รหัสผ่านไม่มีอักขระที่ซ้ำกันต่อเนื่อง มากกว่าสามตัวอักษร | **ตำแหน่ง** `/etc/security/pscexpert/dodv2/chusrattrdod`<br>**แอ็คชันความเข้ากันได้** ตั้งค่าจำนวนต่ำสุดของอักขระที่ซ้ำกันในรหัสผ่าน เป็น 3 |
| GEN000700 | 2 | ค่านี้ทำให้มั่นใจได้ว่า การกำหนดค่าของไฟล์คอนฟิกูเรชันสำหรับ รหัสผ่านโกลบอลของระบบเป็นไปตามข้อกำหนดเกี่ยวกับรหัสผ่าน | **ตำแหน่ง** `/etc/security/pscexpert/dodv2/chusrattrdod`<br>**แอ็คชันความเข้ากันได้** ตรวจสอบให้แน่ใจว่า ไฟล์คอนฟิกูเรชันรหัสผ่านตรงกับข้อกำหนด |
| GEN000740 | 2 | รหัสผ่านแอคเคาต์การประมวลผลแบบไม่โต้ตอบและเป็นแบบอัตโนมัติทั้งหมด ต้องถูกล็อก (GEN000280) การล็อกอินโดยตรงต้องไม่ได้รับอนุญาตให้แบ่งใช้ หรือทำเป็นค่าดีฟอลต์ หรือเป็นแอ็พพลิเคชัน หรือแอคเคาต์ยูทิลิตีใดๆ (GEN002640) แอคเคาต์ของระบบดีฟอลต์ต้องถูกปิดใช้งานหรือถูกลบทิ้ง | **ตำแหน่ง** `/etc/security/pscexpert/dodv2/loginout`<br>`/etc/security/pscexpert/dodv2/lockacc_rlogin`<br>**แอ็คชันความเข้ากันได้** ค่าติดตั้งนี้ถูกเปิดใช้งานแบบอัตโนมัติ |

*ตารางที่ 3. ข้อกำหนดทั่วไปของ DoD (ต่อ)*

| ID จุดตรวจสอบของ Department of Defense STIG | หมวดหมู่ของกฎ STIG | รายละเอียด | ตำแหน่งของสคริปต์ที่นิยามแอ็คชัน และผลลัพธ์ของแอ็คชันที่เปิดใช้งานความเข้ากันได้ |
|---|---|---|---|
| GEN000740 | 2 | รหัสผ่านแอคเคาต์การประมวลผลแบบไม่โต้ตอบและเป็นแบบอัตโนมัติทั้งหมด ต้องถูกเปลี่ยนอย่างน้อยหนึ่งครั้งต่อปีหรือต้องถูกล็อก | **ตำแหน่ง** `/etc/security/pscexpert/dodv2/lockacc_rlogin`<br>**แอ็คชันความเข้ากันได้**<br>ตรวจสอบให้แน่ใจว่า รหัสผ่านที่ระบุไว้ถูกเปลี่ยนทุกปีหรือถูกล็อก |
| GEN000750 | 2 | กฎนี้ต้องการรหัสผ่านใหม่เพื่อให้มีอักขระอย่างน้อย 4 ตัวอักษรที่ไม่ได้อยู่ในรหัสผ่านเก่า | **ตำแหน่ง** `/etc/security/pscexpert/dodv2/chusrattrdod`<br>**แอ็คชันความเข้ากันได้**<br>ตั้งค่าจำนวนต่ำสุดของอักขระใหม่ที่ต้องการในรหัสผ่านใหม่ ให้มีค่า 4 |
| GEN000760 | 2 | แอคเคาต์ต้องถูกล็อกหลังจากที่ไม่ได้ใช้งาน 35 วัน | **ตำแหน่ง** `/etc/security/pscexpert/dodv2/disableacctdod`<br>**แอ็คชันความเข้ากันได้**<br>ล็อกแอคเคาต์หลังจากที่ไม่ได้ใช้งาน 35 วัน |
| GEN000790 | 2 | ระบบต้องปกป้องการใช้คำในพจนานุกรม สำหรับรหัสผ่าน | **ตำแหน่ง** `/etc/security/pscexpert/dodv2/chuserstanzadod`<br>**แอ็คชันความเข้ากันได้**<br>ตรวจสอบให้แน่ใจว่า รหัสผ่านดีฟอลต์ที่ตั้งค่าไว้แข็งแรง |
| GEN000800 | 2 | กฎนี้ทำให้มั่นใจได้ว่า รหัสผ่านห้าอันดับสุดท้าย ไม่ได้ถูกนำมาใช้ใหม่ | **ตำแหน่ง** `/etc/security/pscexpert/dodv2/chusrattrdod`<br>**แอ็คชันความเข้ากันได้**<br>ตรวจสอบให้มั่นใจว่า รหัสผ่านใหม่ไม่ใช่รหัสผ่านที่ตรงกับรหัสผ่าน 5 อันดับสุดท้าย |
| GEN000880 (เกี่ยวข้องกับ GEN000300, GEN000320, GEN000380) | 2 | แอคเคาต์ทั้งหมดบนระบบต้องเป็นผู้ใช้หรือชื่อแอคเคาต์ที่ไม่ซ้ำกัน และรหัสผ่านผู้ใช้หรือรหัสผ่านแอคเคาต์ที่ไม่ซ้ำกัน | **ตำแหน่ง** `/etc/security/pscexpert/dodv2/grpusrpass_chk`<br>**แอ็คชันความเข้ากันได้**<br>ตรวจสอบให้แน่ใจว่า แอคเคาต์ทั้งหมดตรงกับข้อกำหนดที่ระบุไว้ |

*ตารางที่ 3. ข้อกำหนดทั่วไปของ DoD (ต่อ)*

| ID จุดตรวจสอบของ Department of Defense STIG | หมวดหมู่ของกฎ STIG | รายละเอียด | ตำแหน่งของสคริปต์ที่นิยามแอ็คชัน และผลลัพธ์ของแอ็คชันที่เปิดใช้งานความเข้ากันได้ |
|---|---|---|---|
| GEN000900 | 3 | โฮมไดเร็กทอรีของผู้ใช้ root ต้องไม่เป็นไดเร็กทอรี roote (/) | **ตำแหน่ง** `/etc/security/pscexpert/dodv2/rootpasswd_home`<br>**แอ็คชันความเข้ากันได้**<br>ตรวจสอบให้แน่ใจว่า ระบบตรงกับข้อกำหนดที่ระบุไว้<br>**หมายเหตุ:** ค่าติดตั้งนี้ไม่ได้ถูกเปลี่ยนโดยอัตโนมัติเมื่อรีเซ็ตนโยบายเป็น นโยบายดีฟอลต์ของ AIX โดยใช้ไฟล์ `DoDv2_to_AIXDefault.xml` คุณต้องเปลี่ยนค่าติดตั้งนี้แบบแมนวล |
| GEN000940 | 2 | พาธการค้นหาที่สามารถเรียกทำงานได้ของแอคเคาต์ root ต้องเป็นค่าดีฟอลต์ของผู้จำหน่าย และต้องมีพาธสัมพันธ์เท่านั้น | **ตำแหน่ง** `/etc/security/pscexpert/dodv2/fixpathvars`<br>**แอ็คชันความเข้ากันได้**<br>ตรวจสอบให้แน่ใจว่า ระบบตรงกับข้อกำหนด ที่ระบุไว้<br>**หมายเหตุ:** ค่าติดตั้งนี้ไม่ได้ถูกเปลี่ยนโดยอัตโนมัติเมื่อรีเซ็ตนโยบายเป็น นโยบายดีฟอลต์ของ AIX โดยใช้ไฟล์ `DoDv2_to_AIXDefault.xml` คุณต้องเปลี่ยนค่าติดตั้งนี้แบบแมนวล |
| GEN000945 | 2 | พาธการค้นหาไลบรารีของแอคเคาต์ root ต้องเป็นค่าดีฟอลต์ของระบบ และต้องมีเฉพาะพาธสัมบูรณ์เท่านั้น | **ตำแหน่ง** `/etc/security/pscexpert/dodv2/fixpathvars`<br>**แอ็คชันความเข้ากันได้**<br>ตรวจสอบให้แน่ใจว่า ระบบตรงกับข้อกำหนด ที่ระบุไว้<br>**หมายเหตุ:** ค่าติดตั้งนี้ไม่ได้ถูกเปลี่ยนโดยอัตโนมัติเมื่อรีเซ็ตนโยบายเป็น นโยบายดีฟอลต์ของ AIX โดยใช้ไฟล์ `DoDv2_to_AIXDefault.xml` คุณต้องเปลี่ยนค่าติดตั้งนี้แบบแมนวล |

*ตารางที่ 3. ข้อกำหนดทั่วไปของ DoD (ต่อ)*

| ID จุดตรวจสอบของ Department of Defense STIG | หมวดหมู่ของกฎ STIG | รายละเอียด | ตำแหน่งของสคริปต์ที่นิยามแอ็คชัน และผลลัพธ์ของแอ็คชันที่เปิดใช้งานความเข้ากันได้ |
|---|---|---|---|
| GEN000950 | 2 | รายชื่อแอคเคาต์ root ของไลบรารีที่โหลดไว้ล่วงหน้า ต้องว่าง | **ตำแหน่ง** `/etc/security/pscexpert/dodv2/fixpathvars`<br>**แอ็คชันความเข้ากันได้**<br>ตรวจสอบให้แน่ใจว่า ระบบตรงกับข้อกำหนด ที่ระบุไว้<br>**หมายเหตุ:** ค่าติดตั้งนี้ไม่ได้ถูกเปลี่ยนโดยอัตโนมัติเมื่อรีเซ็ตนโยบายเป็น นโยบายดีฟอลต์ของ AIX โดยใช้ไฟล์ `DoDv2_to_AIXDefault.xml` คุณต้องเปลี่ยนค่าติดตั้งนี้แบบแมนวล |
| GEN000960 (เกี่ยวข้องกับ GEN003000, GEN003020, GEN003160, GEN003360, GEN003380) | 2 | แอคเคาต์ root ต้องมีไดเร็กทอรีที่สามารถเขียนได้ ในพาธการค้นหาที่สามารถเรียกทำงานได้ | **ตำแหน่ง** `/etc/security/pscexpert/dodv2/rmwwpaths`<br>**แอ็คชันความเข้ากันได้**<br>ตรวจสอบให้แน่ใจว่า ระบบตรงกับข้อกำหนด ที่ระบุไว้<br>**หมายเหตุ:** ค่าติดตั้งนี้ไม่ได้ถูกเปลี่ยนโดยอัตโนมัติเมื่อรีเซ็ตนโยบายเป็น นโยบายดีฟอลต์ของ AIX โดยใช้ไฟล์ `DoDv2_to_AIXDefault.xml` คุณต้องเปลี่ยนค่าติดตั้งนี้แบบแมนวล |
| GEN000980 | 2 | ระบบต้องปกป้องแอคเคาต์ root จากการล็อกอินโดยตรง ยกเว้นจากคอนโซลของระบบ | **ตำแหน่ง** `/etc/security/pscexpert/dodv2/chuserstanzadod`<br>**แอ็คชันความเข้ากันได้**<br>ตรวจสอบให้แน่ใจว่า ระบบตรงกับข้อกำหนดที่ระบุไว้ |
| GEN001000 | 2 | คอนโซลแบบรีโมตต้องถูกปิดใช้งานหรือได้รับการปกป้อง จากการเข้าถึงที่ไม่ได้รับอนุญาต | **ตำแหน่ง** `/etc/security/pscexpert/dodv2/remoteconsole`<br>**แอ็คชันความเข้ากันได้**<br>ตรจสอบให้แน่ใจว่า คอนโซลที่ระบุไว้ถูกปิดใช้งาน |
| GEN001020 | 2 | แอคเคาต์ root ต้องไม่ถูกใช้สำหรับ การล็อกอินโดยตรง | **ตำแหน่ง** `/etc/security/pscexpert/dodv2/sshDoDconfig`<br>**แอ็คชันความเข้ากันได้**<br>ปิดใช้งานแอคเคาต์ root จากการล็อกอินโดยตรง |

*ตารางที่ 3. ข้อกำหนดทั่วไปของ DoD (ต่อ)*

| ID จุดตรวจสอบของ Department of Defense STIG | หมวดหมู่ของกฎ STIG | รายละเอียด | ตำแหน่งของสคริปต์ที่นิยามแอ็คชัน และผลลัพธ์ของแอ็คชันที่เปิดใช้งานความเข้ากันได้ |
|---|---|---|---|
| GEN001060 | 2 | ระบบต้องมีความพยายามในการล็อกที่เป็นผลสำเร็จหรือไม่สำเร็จ เพื่อเข้าถึงแอคเคาต์ root | **ตำแหน่ง** `/etc/security/pscexpert/dodv2/loginout`<br>**แอ็คชันความเข้ากันได้** ตรวจสอบให้แน่ใจว่า ระบบตรงกับข้อกำหนดที่ระบุไว้ |
| GEN001100 | 1 | รหัสผ่าน root ต้องไม่ส่งผ่านเครือข่าย ในรูปของข้อความ | **ตำแหน่ง** `/etc/security/pscexpert/dodv2/chuserstanzadod`<br>**แอ็คชันความเข้ากันได้** ตรวจสอบให้แน่ใจว่า ระบบตรงกับข้อกำหนดที่ระบุไว้ |
| GEN001120 | 2 | ระบบต้องไม่อนุญาตให้ใช้ล็อกอิน root โดยใช้โปรโตคอล SSH | **ตำแหน่ง** `/etc/security/pscexpert/dodv2/sshDoDconfig`<br>**แอ็คชันความเข้ากันได้** ปิดใช้งานล็อกอิน root สำหรับ SSH |
| GEN001440 | 3 | ผู้ใช้แบบโต้ตอบทั้งหมดต้องถูกกำหนดโฮมไดเร็กทอรี ไว้ในไฟล์ `/etc/passwd` | **ตำแหน่ง** `/etc/security/pscexpert/dodv2/grpusrpass_chk`<br>**แอ็คชันความเข้ากันได้** ตรวจสอบให้แน่ใจว่า ผู้ใช้แบบโต้ตอบทั้งหมดมีไดเร็กทอรีที่ระบุเฉพาะ |
| GEN001475 | 2 | ไฟล์ `/etc/group` ต้องไม่มีการแฮชรหัสผ่านแบบกลุ่มใดๆ | **ตำแหน่ง** `/etc/security/pscexpert/dodv2/passwdhash`<br>**แอ็คชันความเข้ากันได้** ตรวจสอบให้แน่ใจว่า ไม่มีการแฮชรหัสผ่านแบบกลุ่มใน ไฟล์ที่ระบุเฉพาะ<br>**หมายเหตุ:** ค่าติดตั้งนี้ไม่ได้ถูกเปลี่ยนโดยอัตโนมัติเมื่อรีเซ็ตนโยบายเป็น นโยบายดีฟอลต์ของ AIX โดยใช้ไฟล์ `DoDv2_to_AIXDefault.xml` คุณต้องเปลี่ยนค่าติดตั้งนี้แบบแมนวล |

*ตารางที่ 3. ข้อกำหนดทั่วไปของ DoD (ต่อ)*

| ID จุดตรวจสอบของ Department of Defense STIG | หมวดหมู่ของกฎ STIG | รายละเอียด | ตำแหน่งของสคริปต์ที่นิยามแอ็คชัน และผลลัพธ์ของแอ็คชันที่เปิดใช้งานความเข้ากันได้ |
|---|---|---|---|
| GEN001600 | 2 | การรันพาธการค้นหาที่สามารถเรียกทำงานได้ของสคริปต์แบบควบคุม ต้องมีพาธสัมบูรณ์เท่านั้น | **ตำแหน่ง** `/etc/security/pscexpert/dodv2/fixpathvars`<br>**แอ็คชันความเข้ากันได้**<br>ตรวจสอบให้แน่ใจว่า ระบบตรงกับข้อกำหนด ที่ระบุไว้<br>**หมายเหตุ:** ค่าติดตั้งนี้ไม่ได้ถูกเปลี่ยนโดยอัตโนมัติเมื่อรีเซ็ตนโยบายเป็น นโยบายดีฟอลต์ของ AIX โดยใช้ไฟล์ `DoDv2_to_AIXDefault.xml` คุณต้องเปลี่ยนค่าติดตั้งนี้แบบแมนวล |
| GEN001605 | 2 | การรันพาธการค้นหาไลบรารีของสคริปต์แบบควบคุม ต้องมีพาธสัมบูรณ์เท่านั้น | **ตำแหน่ง** `/etc/security/pscexpert/dodv2/fixpathvars`<br>**แอ็คชันความเข้ากันได้**<br>ตรวจสอบให้แน่ใจว่า ระบบตรงกับข้อกำหนด ที่ระบุไว้<br>**หมายเหตุ:** ค่าติดตั้งนี้ไม่ได้ถูกเปลี่ยนโดยอัตโนมัติเมื่อรีเซ็ตนโยบายเป็น นโยบายดีฟอลต์ของ AIX โดยใช้ไฟล์ `DoDv2_to_AIXDefault.xml` คุณต้องเปลี่ยนค่าติดตั้งนี้แบบแมนวล |
| GEN001610 | 2 | การไลบรารีที่โหลดล่วงหน้าของสคริปต์แบบควบคุม ต้องมีพาธสัมบูรณ์เท่านั้น | **ตำแหน่ง** `/etc/security/pscexpert/dodv2/fixpathvars`<br>**แอ็คชันความเข้ากันได้**<br>ตรวจสอบให้แน่ใจว่า ระบบตรงกับข้อกำหนด ที่ระบุไว้<br>**หมายเหตุ:** ค่าติดตั้งนี้ไม่ได้ถูกเปลี่ยนโดยอัตโนมัติเมื่อรีเซ็ตนโยบายเป็น นโยบายดีฟอลต์ของ AIX โดยใช้ไฟล์ `DoDv2_to_AIXDefault.xml` คุณต้องเปลี่ยนค่าติดตั้งนี้แบบแมนวล |

*ตารางที่ 3. ข้อกำหนดทั่วไปของ DoD (ต่อ)*

| ID จุดตรวจสอบของ Department of Defense STIG | หมวดหมู่ของกฎ STIG | รายละเอียด | ตำแหน่งของสคริปต์ที่นิยามแอ็คชัน และผลลัพธ์ของแอ็คชันที่เปิดใช้งานความเข้ากันได้ |
|---|---|---|---|
| GEN001840 | 2 | พาธการค้นหาที่สามารถเรียกทำงานได้ของไฟล์เริ่มต้นทำงานแบบโกลบอล ต้องมีพาธสัมบูรณ์เท่านั้น | **ตำแหน่ง** `/etc/security/pscexpert/dodv2/fixpathvars`<br>**แอ็คชันความเข้ากันได้**<br>ตรวจสอบให้แน่ใจว่า ระบบตรงกับข้อกำหนด ที่ระบุไว้<br>**หมายเหตุ:** ค่าติดตั้งนี้ไม่ได้ถูกเปลี่ยนโดยอัตโนมัติเมื่อรีเซ็ตนโยบายเป็น นโยบายดีฟอลต์ของ AIX โดยใช้ไฟล์ `DoDv2_to_AIXDefault.xml` คุณต้องเปลี่ยนค่าติดตั้งนี้แบบแมนวล |
| GEN001845 | 2 | พาธการค้นหาไลบรารีของไฟล์เริ่มต้นทำงานแบบโกลบอล ต้องมีพาธสัมบูรณ์เท่านั้น | **ตำแหน่ง** `/etc/security/pscexpert/dodv2/fixpathvars`<br>**แอ็คชันความเข้ากันได้**<br>ตรวจสอบให้แน่ใจว่า ระบบตรงกับข้อกำหนด ที่ระบุไว้<br>**หมายเหตุ:** ค่าติดตั้งนี้ไม่ได้ถูกเปลี่ยนโดยอัตโนมัติเมื่อรีเซ็ตนโยบายเป็น นโยบายดีฟอลต์ของ AIX โดยใช้ไฟล์ `DoDv2_to_AIXDefault.xml` คุณต้องเปลี่ยนค่าติดตั้งนี้แบบแมนวล |
| GEN001850 | 2 | รายการไลบรารีที่โหลดล่วงหน้าของไฟล์เริ่มต้นทำงานแบบโกลบอลทั้งหมด ต้องมีพาธสัมบูรณ์เท่านั้น | **ตำแหน่ง** `/etc/security/pscexpert/dodv2/fixpathvars`<br>**แอ็คชันความเข้ากันได้**<br>ตรวจสอบให้แน่ใจว่า ระบบตรงกับข้อกำหนด ที่ระบุไว้<br>**หมายเหตุ:** ค่าติดตั้งนี้ไม่ได้ถูกเปลี่ยนโดยอัตโนมัติเมื่อรีเซ็ตนโยบายเป็น นโยบายดีฟอลต์ของ AIX โดยใช้ไฟล์ `DoDv2_to_AIXDefault.xml` คุณต้องเปลี่ยนค่าติดตั้งนี้แบบแมนวล |

*ตารางที่ 3. ข้อกำหนดทั่วไปของ DoD (ต่อ)*

| ID จุดตรวจสอบของ Department of Defense STIG | หมวดหมู่ของกฎ STIG | รายละเอียด | ตำแหน่งของสคริปต์ที่นิยามแอ็คชัน และผลลัพธ์ของแอ็คชันที่เปิดใช้งานความเข้ากันได้ |
|---|---|---|---|
| GEN001900 | 2 | พาธการค้นหาที่สามารถเรียกทำงานได้ของไฟล์การเริ่มต้นทำงานแบบโลคัลทั้งหมด ต้องมีพาธสัมบูรณ์เท่านั้น | **ตำแหน่ง** `/etc/security/pscexpert/dodv2/fixpathvars`<br>**แอ็คชันความเข้ากันได้**<br>ตรวจสอบให้แน่ใจว่า ระบบตรงกับข้อกำหนด ที่ระบุไว้<br>**หมายเหตุ:** ค่าติดตั้งนี้ไม่ได้ถูกเปลี่ยนโดยอัตโนมัติเมื่อรีเซ็ตนโยบายเป็น นโยบายดีฟอลต์ของ AIX โดยใช้ไฟล์ `DoDv2_to_AIXDefault.xml` คุณต้องเปลี่ยนค่าติดตั้งนี้แบบแมนวล |
| GEN001901 | 2 | พาธการค้นหาไลบรารีของไฟล์เริ่มต้นทำงานแบบโลคัลทั้งหมด มีพาธสัมบูรณ์เท่านั้น | **ตำแหน่ง** `/etc/security/pscexpert/dodv2/fixpathvars`<br>**แอ็คชันความเข้ากันได้**<br>ตรวจสอบให้แน่ใจว่า ระบบตรงกับข้อกำหนด ที่ระบุไว้<br>**หมายเหตุ:** ค่าติดตั้งนี้ไม่ได้ถูกเปลี่ยนโดยอัตโนมัติเมื่อรีเซ็ตนโยบายเป็น นโยบายดีฟอลต์ของ AIX โดยใช้ไฟล์ `DoDv2_to_AIXDefault.xml` คุณต้องเปลี่ยนค่าติดตั้งนี้แบบแมนวล |
| GEN001902 | 2 | รายการของไลบรารีที่โหลดล่วงหน้าของไฟล์การเริ่มต้นทำงานแบบโลคัลทั้งหมด ต้องมีพาธสัมบูรณ์เท่านั้น | **ตำแหน่ง** `/etc/security/pscexpert/dodv2/fixpathvars`<br>**แอ็คชันความเข้ากันได้**<br>ตรวจสอบให้แน่ใจว่า ระบบตรงกับข้อกำหนด ที่ระบุไว้<br>**หมายเหตุ:** ค่าติดตั้งนี้ไม่ได้ถูกเปลี่ยนโดยอัตโนมัติเมื่อรีเซ็ตนโยบายเป็น นโยบายดีฟอลต์ของ AIX โดยใช้ไฟล์ `DoDv2_to_AIXDefault.xml` คุณต้องเปลี่ยนค่าติดตั้งนี้แบบแมนวล |
| GEN001940 | 2 | ไฟล์การเริ่มต้นทำงานของผู้ใช้ต้องไม่รันโปรแกรมที่สามารถเขียน ได้ | **ตำแหน่ง** `/etc/security/pscexpert/dodv2/rmwwpaths`<br>**แอ็คชันความเข้ากันได้**<br>ตรวจสอบให้แน่ใจว่า ระบบตรงกับข้อกำหนดที่ระบุไว้ |

*ตารางที่ 3. ข้อกำหนดทั่วไปของ DoD (ต่อ)*

| ID จุดตรวจสอบของ Department of Defense STIG | หมวดหมู่ของกฎ STIG | รายละเอียด | ตำแหน่งของสคริปต์ที่นิยามแอ็คชัน และผลลัพธ์ของแอ็คชันที่เปิดใช้งานความเข้ากันได้ |
|---|---|---|---|
| GEN001980 | 2 | ไฟล์ .rhosts, .shosts, hosts.equiv, shosts.equiv, /etc/passwd, /etc/shadow หรือ /etc/group ต้องไม่มีเครื่องหมายบวก (+) ซึ่งไม่ได้นิยามรายการสำหรับ NIS+ netgroups | **ตำแหน่ง** /etc/security/pscexpert/dodv2/dodv2netrules<br>**แอ็คชันความเข้ากันได้**<br>ตรวจสอบให้แน่ใจว่า ไฟล์ที่ระบุไว้ตรงกับข้อกำหนดที่ระบุไว้ |
| GEN002000 | 2 | ต้องไม่มีไฟล์ .netrc บนระบบ | **ตำแหน่ง** /etc/security/pscexpert/dodv2/dodv2netrules<br>**แอ็คชันความเข้ากันได้**<br>ตรวจสอบให้มั่นใจว่า ไม่มีไฟล์ที่ระบุไว้บนระบบ<br>**หมายเหตุ:** ค่าติดตั้งนี้ไม่ได้ถูกเปลี่ยนโดยอัตโนมัติเมื่อรีเซ็ตนโยบายเป็น นโยบายดีฟอลต์ของ AIX โดยใช้ไฟล์ DoDv2_to_AIXDefault.xml คุณต้องเปลี่ยนค่าติดตั้งนี้แบบแมนวล |
| GEN002020 | 2 | ไฟล์ .rhosts, .shosts หรือ hosts.equiv ต้องมีคู่ของโฮสต์–ผู้ใช้ที่เชื่อถือได้ | **ตำแหน่ง** /etc/security/pscexpert/dodv2/dodv2netrules<br>**แอ็คชันความเข้ากันได้**<br>ตรวจสอบให้แน่ใจว่า ไฟล์ที่ระบุตรงกับข้อกำหนดนี้ |
| GEN002040 | 1 | กฎนี้ปิดใช้งานไฟล์ .rhosts, .shosts และ hosts.equiv หรือไฟล์ shosts.equiv | **ตำแหน่ง** /etc/security/pscexpert/dodv2/mvhostsfilesdod<br>**แอ็คชันความเข้ากันได้**<br>ปิดใช้งานไฟล์ที่ระบุไว้ |
| GEN002120 | 1,2 | กฎนี้ตรวจสอบและกำหนดคอนฟิกเชลล์ผู้ใช้ | **ตำแหน่ง** /etc/security/pscexpert/dodv2/usershells<br>**แอ็คชันความเข้ากันได้**<br>สร้างเชลล์ที่ต้องการ<br>**หมายเหตุ:** ค่าติดตั้งนี้ไม่ได้ถูกเปลี่ยนโดยอัตโนมัติเมื่อรีเซ็ตนโยบายเป็น นโยบายดีฟอลต์ของ AIX โดยใช้ไฟล์ DoDv2_to_AIXDefault.xml คุณต้องเปลี่ยนค่าติดตั้งนี้แบบแมนวล |

*ตารางที่ 3. ข้อกำหนดทั่วไปของ DoD (ต่อ)*

| ID จุดตรวจสอบของ Department of Defense STIG | หมวดหมู่ของกฎ STIG | รายละเอียด | ตำแหน่งของสคริปต์ที่นิยามแอ็คชัน และผลลัพธ์ของแอ็คชันที่เปิดใช้งานความเข้ากันได้ |
|---|---|---|---|
| GEN002140 | 1,2 | เชลล์ทั้งหมดที่อ้างถึงในรายการ `/etc/passwd` ต้องแสดงอยู่ในไฟล์ `/etc/shells` ยกเว้นว่า เชลล์ใดๆ ที่ระบุไว้เพื่อปกป้องการล็อกอิน | **ตำแหน่ง** `/etc/security/pscexpert/dodv2/usershells`<br>**แอ็คชันความเข้ากันได้**<br>ตรวจสอบให้แน่ใจว่า เชลล์แสดงอยู่ในไฟล์ที่ถูกต้อง<br>**หมายเหตุ:** ค่าติดตั้งนี้ไม่ได้ถูกเปลี่ยนโดยอัตโนมัติเมื่อรีเซ็ตนโยบายเป็น นโยบายดีฟอลต์ของ AIX โดยใช้ไฟล์ `DoDv2_to_AIXDefault.xml` คุณต้องเปลี่ยนค่าติดตั้งนี้แบบแมนวล |
| GEN002280 | 2 | ไฟล์และไดเร็กทอรีอุปกรณ์ต้องสามารถเขียนได้โดยผู้ใช้ ที่มีแอคเคาต์ระบบเท่านั้น หรือเป็นระบบที่ถูกกำหนดคอฟนิกไว้โดยผู้จำหน่าย | **ตำแหน่ง** `/etc/security/pscexpert/dodv2/wwdevfiles`<br>**แอ็คชันความเข้ากันได้**<br>แสดงไฟล์อุปกรณ์ ไดเร็กทอรี และไฟล์อื่นใดที่สามารถเขียนได้ บนระบบที่อยู่ในไดเร็กทอรีที่ไม่ใช่พับลิก |
| GEN002300 | 2 | ไฟล์อุปกรณ์ที่ใช้สำหรับการสำรองข้อมูล ต้องสามารถอ่านได้ สามารถเขียนได้ หรือทั้งสองอย่าง โดยผู้ใช้ root หรือผู้ใช้การสำรองข้อมูล เท่านั้น | **ตำแหน่ง** `/etc/security/pscexpert/dodv2/wwdevfiles`<br>**แอ็คชันความเข้ากันได้**<br>แสดงไฟล์อุปกรณ์ ไดเร็กทอรี และไฟล์อื่นใดที่สามารถเขียนได้ บนระบบที่อยู่ในไดเร็กทอรีที่ไม่ใช่พับลิก |
| GEN002400 | 2 | ระบบต้องถูกตรวจสอบทุกสัปดาห์สำหรับไฟล์ `setuid` ที่ไม่ได้รับสิทธิ์ และโมดิฟิเคชันที่ไม่ได้รับสิทธิ์เพื่อให้สิทธิ์กับไฟล์ `setuid` | **ตำแหน่ง** `/etc/security/pscexpert/dodv2/trust`<br>**แอ็คชันความเข้ากันได้**<br>ตรวจสอบทุกสัปดาห์เพื่อระบุความเปลี่ยนแปลงกับไฟล์ ที่ระบุไว้<br>**หมายเหตุ:** เปรียบเทียบล็อกที่ใหม่ที่สุดรายสัปดาห์สองไฟล์ที่สร้างขึ้นในไดเร็กทอรี `/var/security/pscexpert` เพื่อตรวจสอบว่า ไม่มีกิจกรรมใดๆ ที่ไม่ได้รับอนุญาต |

*ตารางที่ 3. ข้อกำหนดทั่วไปของ DoD (ต่อ)*

| ID จุดตรวจสอบของ Department of Defense STIG | หมวดหมู่ของกฎ STIG | รายละเอียด | ตำแหน่งของสคริปต์ที่นิยามแอ็คชัน และผลลัพธ์ของแอ็คชันที่เปิดใช้งานความเข้ากันได้ |
|---|---|---|---|
| GEN002420 | 2 | สื่อบันทึกที่สามารถลบได้ ระบบไฟล์แบบรีโมต และระบบไฟล์อื่น ที่ไม่มีไฟล์ `setuid` ที่อนุมัติ ต้องถูกเมาท์โดยใช้อ็อพชัน *nosuid* | **ตำแหน่ง** `/etc/security/pscexpert/dodv2/fsmntoptions`<br>**แอ็คชันความเข้ากันได้**<br>ตรวจสอบให้แน่ใจว่า ระบบไฟล์ที่เมาท์แบบรีโมตมีอ็อพชัน ที่ระบุเฉพาะ<br>**หมายเหตุ:** ค่าติดตั้งนี้ไม่ได้ถูกเปลี่ยนโดยอัตโนมัติเมื่อรีเซ็ตนโยบายเป็น นโยบายดีฟอลต์ของ AIX โดยใช้ไฟล์ `DoDv2_to_AIXDefault.xml` คุณต้องเปลี่ยนค่าติดตั้งนี้แบบแมนวล |
| GEN002430 | 2 | สื่อบันทึกที่สามารถถอดออกได้ ระบบไฟล์แบบรีโมต และระบบไฟล์อื่นๆ ที่ไม่มีไฟล์อุปกรณ์ที่อนุมัติแล้วต้องถูกเมาท์โดยใช้อ็อพชัน *nodev* | **ตำแหน่ง** `/etc/security/pscexpert/dodv2/fsmntoptions`<br>**แอ็คชันความเข้ากันได้**<br>ตรวจสอบให้แน่ใจว่า ระบบไฟล์ที่เมาท์แบบรีโมตมีอ็อพชัน ที่ระบุเฉพาะ<br>**หมายเหตุ:** ค่าติดตั้งนี้ไม่ได้ถูกเปลี่ยนโดยอัตโนมัติเมื่อรีเซ็ตนโยบายเป็น นโยบายดีฟอลต์ของ AIX โดยใช้ไฟล์ `DoDv2_to_AIXDefault.xml` คุณต้องเปลี่ยนค่าติดตั้งนี้แบบแมนวล |
| GEN002480 | 2 | ไดเร็กทอรีแบบพับลิกต้องเป็นไดเร็กทอรีที่สามารถเขียนได้ และไฟล์ที่สามารถเขียนได้ต้องวางอยู่ในไดเร็กทอรี แบบพับลิกเท่านั้น | **ตำแหน่ง** `/etc/security/pscexpert/dodv2/wwdevfiles`<br>`/etc/security/pscexpert/dodv2/fpmdodfiles`<br>**แอ็คชันความเข้ากันได้**<br>รายงานเมื่อไฟล์ที่สามารถเขียนได้ไม่ได้อยู่ในไดเร็กทอรีแบบพับลิก |
| GEN002640 | 2 | แอคเคาต์ระบบดีฟอลต์ต้องถูกปิดใช้งาน หรือถอนออกได้ | **ตำแหน่ง** `/etc/security/pscexpert/dodv2/lockacc_rlogin`<br>`/etc/security/pscexpert/dodv2/loginout`<br>**แอ็คชันความเข้ากันได้**<br>ปิดใช้งานแอคเคาต์ระบบดีฟอลต์ |

*ตารางที่ 3. ข้อกำหนดทั่วไปของ DoD (ต่อ)*

| ID จุดตรวจสอบของ Department of Defense STIG | หมวดหมู่ของกฎ STIG | รายละเอียด | ตำแหน่งของสคริปต์ที่นิยามแอ็คชัน และผลลัพธ์ของแอ็คชันที่เปิดใช้งานความเข้ากันได้ |
|---|---|---|---|
| GEN002660 | 2 | ระบบการตรวจสอบต้องเปิดใช้งาน | **ตำแหน่ง** `/etc/security/pscexpert/dodv2/dodaudit`<br>**แอ็คชันความเข้ากันได้**<br>เปิดใช้งานคำสั่ง `dodaudit` ซึ่งสามารถเปิดใช้งานระบบตรวจสอบ |
| GEN002720 | 2 | ระบบการตรวจสอบต้องถูกกำหนดคอนฟิกเพื่อตรวจสอบความพยายามที่ล้มเหลวในการเข้าถึง ไฟล์และโปรแกรม | **ตำแหน่ง** `/etc/security/pscexpert/dodv2/dodaudit`<br>**แอ็คชันความเข้ากันได้**<br>เปิดใช้งานการตรวจสอบระบบที่ระบุไว้โดยอัตโนมัติ |
| GEN002740 | 2 | ระบบการตรวจสอบต้องถูกกำหนดคอนฟิกเพื่อตรวจสอบการลบ ไฟล์ | **ตำแหน่ง** `/etc/security/pscexpert/dodv2/dodaudit`<br>**แอ็คชันความเข้ากันได้**<br>เปิดใช้งานการตรวจสอบระบบที่ระบุไว้โดยอัตโนมัติ |
| GEN002750 | 3 | ระบบการตรวจสอบต้องถูกกำหนดคอนฟิกเพื่อตรวจสอบ การสร้างแอคเคาต์ | **ตำแหน่ง** `/etc/security/pscexpert/dodv2/dodaudit`<br>**แอ็คชันความเข้ากันได้**<br>เปิดใช้งานการตรวจสอบระบบที่ระบุไว้โดยอัตโนมัติ |
| GEN002751 | 3 | ระบบการตรวจสอบต้องถูกกำหนดคอนฟิกเพื่อตรวจสอบ การปรับเปลี่ยนแอคเคาต์ | **ตำแหน่ง** `/etc/security/pscexpert/dodv2/dodaudit`<br>**แอ็คชันความเข้ากันได้**<br>เปิดใช้งานการตรวจสอบระบบที่ระบุไว้โดยอัตโนมัติ |
| GEN002752 | 3 | ระบบการตรวจสอบต้องถูกกำหนดคอนฟิกเพื่อตรวจสอบแอคเคาต์ ที่ถูกปิดใช้งาน | **ตำแหน่ง** `/etc/security/pscexpert/dodv2/dodaudit`<br>**แอ็คชันความเข้ากันได้**<br>เปิดใช้งานการตรวจสอบระบบที่ระบุไว้โดยอัตโนมัติ |

*ตารางที่ 3. ข้อกำหนดทั่วไปของ DoD (ต่อ)*

| ID จุดตรวจสอบของ Department of Defense STIG | หมวดหมู่ของกฎ STIG | รายละเอียด | ตำแหน่งของสคริปต์ที่นิยามแอ็คชัน และผลลัพธ์ของแอ็คชันที่เปิดใช้งานความเข้ากันได้ |
|---|---|---|---|
| GEN002753 | 3 | ระบบการตรวจสอบต้องถูกกำหนดคอนฟิกเพื่อตรวจสอบ การยกเลิกแอคเอาต์ | **ตำแหน่ง** `/etc/security/pscexpert/dodv2/dodaudit`<br>**แอ็คชันความเข้ากันได้** เปิดใช้งานการตรวจสอบระบบที่ระบุไว้โดยอัตโนมัติ |
| GEN002760 | 2 | ระบบการตรวจสอบต้องถูกกำหนดคอนฟิกเพื่อตรวจสอบแอ็คชัน การดูแลจัดการ สิทธิพิเศษ และความปลอดภัยทั้งหมด | **ตำแหน่ง** `/etc/security/pscexpert/dodv2/dodaudit`<br>**แอ็คชันความเข้ากันได้** เปิดใช้งานการตรวจสอบระบบที่ระบุไว้โดยอัตโนมัติ |
| GEN002800 | 2 | ระบบการตรวจสอบต้องถูกกำหนดคอนฟิกเพื่อตรวจสอบการเริ่มต้น ล็อกอิน ล็อกเอาต์ และเซสชัน | **ตำแหน่ง** `/etc/security/pscexpert/dodv2/dodaudit`<br>**แอ็คชันความเข้ากันได้** เปิดใช้งานการตรวจสอบระบบที่ระบุไว้โดยอัตโนมัติ |
| GEN002820 | 2 | ระบบการตรวจสอบต้องถูกกำหนดคอนฟิกเพื่อตรวจสอบ การปรับเปลี่ยนสิทธิการควบคุมการเข้าถึงอย่างรอบครอบ | **ตำแหน่ง** `/etc/security/pscexpert/dodv2/dodaudit`<br>**แอ็คชันความเข้ากันได้** เปิดใช้งานการตรวจสอบระบบที่ระบุไว้โดยอัตโนมัติ |
| GEN002825 | 2 | ระบบการตรวจสอบต้องถูกกำหนดคอนฟิกเพื่อตรวจสอบ การโหลดและยกเลิกการโหลดโมดูลเคอร์เนลแบบไดนามิก | **ตำแหน่ง** `/etc/security/pscexpert/dodv2/dodaudit`<br>**แอ็คชันความเข้ากันได้** เปิดใช้งานการตรวจสอบระบบที่ระบุไว้โดยอัตโนมัติ |
| GEN002860 | 2 | ล็อกการตรวจสอบต้องถูกเปลี่ยนรายวัน | **ตำแหน่ง** `/etc/security/pscexpert/dodv2/rotateauditdod`<br>**แอ็คชันความเข้ากันได้** ตรวจสอบให้มั่นใจว่า ล็อกการตรวจสอบถูกเปลี่ยน |

*ตารางที่ 3. ข้อกำหนดทั่วไปของ DoD (ต่อ)*

| ID จุดตรวจสอบของ Department of Defense STIG | หมวดหมู่ของกฎ STIG | รายละเอียด | ตำแหน่งของสคริปต์ที่นิยามแอ็คชัน และผลลัพธ์ของแอ็คชันที่เปิดใช้งานความเข้ากันได้ |
|---|---|---|---|
| GEN002960 | 2 | เข้าถึงยูทิลิตี cron ต้องถูกควบคุมโดยใช้ไฟล์ cron.allow หรือไฟล์ cron.deny หรือทั้งสอง | **ตำแหน่ง** /etc/security/pscexpert/dodv2/limitsysacc<br>**แอ็คชันความเข้ากันได้**<br>ตรวจสอบให้มั่นใจว่า ข้อจำกัดที่สอดคล้องกันถูกเปิดใช้งาน |
| GEN003000 (เกี่ยวข้องกับ GEN000960, GEN003020, GEN003160, GEN003360, GEN003380) | 2 | Cron ต้องไม่ได้รันโปรแกรมที่สามารถเขียนได้แบบกลุ่ม หรือโปรแกรมที่สามารถเขียนได้ทั่วไป | **ตำแหน่ง** /etc/security/pscexpert/dodv2/rmwwpaths<br>**แอ็คชันความเข้ากันได้**<br>ตรวจสอบให้มั่นใจว่า ข้อจำกัดที่สอดคล้องกันถูกเปิดใช้งาน<br>**หมายเหตุ:** ค่าติดตั้งนี้ไม่ได้ถูกเปลี่ยนโดยอัตโนมัติเมื่อรีเซ็ตนโยบายเป็น นโยบายดีฟอลต์ของ AIX โดยใช้ไฟล์ DoDv2_to_AIXDefault.xml คุณต้องเปลี่ยนค่าติดตั้งนี้แบบแมนวล |
| GEN003020 (เกี่ยวข้องกับ GEN000960, GEN003000, GEN003160, GEN003360, GEN003380) | 2 | Cron ต้องไม่รันโปรแกรม หรือ ส่วนขยาย ของไดเร็กทอรีที่สามารถเขียนได้ | **ตำแหน่ง** /etc/security/pscexpert/dodv2/rmwwpaths<br>**แอ็คชันความเข้ากันได้**<br>ถอนสิทธิที่สามารถเขียนได้จากไดเร็กทอรีโปรแกรม cron<br>**หมายเหตุ:** ค่าติดตั้งนี้ไม่ได้ถูกเปลี่ยนโดยอัตโนมัติเมื่อรีเซ็ตนโยบายเป็น นโยบายดีฟอลต์ของ AIX โดยใช้ไฟล์ DoDv2_to_AIXDefault.xml คุณต้องเปลี่ยนค่าติดตั้งนี้แบบแมนวล |
| GEN003060 | 2 | แอคเคาต์ระบบดีฟอลต์ (ยกเว้นสำหรับ root) ต้องไม่อยู่ในไฟล์ cron.allow หรือ ต้องถูกสอดแทรกในไฟล์ cron.deny หากไฟล์ cron.allow ไม่มีอยู่ | **ตำแหน่ง** cron.allow หรือ cron.deny<br>**แอ็คชันความเข้ากันได้**<br>ตรวจสอบให้แน่ใจว่า ระบบตรงกับข้อกำหนดที่ระบุไว้ |
| GEN003160 (เกี่ยวข้องกับ GEN000960, GEN003000, GEN003020, GEN003360, GEN003380) | 2 | การสร้างล็อก Cron ต้องรันอยู่ | **ตำแหน่ง** /etc/security/pscexpert/dodv2/rmwwpaths<br>**แอ็คชันความเข้ากันได้**<br>ตรวจสอบให้แน่ใจว่า ระบบตรงกับข้อกำหนดที่ระบุไว้ |

*ตารางที่ 3. ข้อกำหนดทั่วไปของ DoD (ต่อ)*

| ID จุดตรวจสอบของ Department of Defense STIG | หมวดหมู่ของกฎ STIG | รายละเอียด | ตำแหน่งของสคริปต์ที่นิยามแอ็คชัน และผลลัพธ์ของแอ็คชันที่เปิดใช้งานความเข้ากันได้ |
|---|---|---|---|
| GEN003280 | 2 | การเข้าถึงยูทิลิตี at ต้องถูกควบคุมโดยใช้ไฟล์ at.allow และ at.deny | **ตำแหน่ง** /etc/security/pscexpert/dodv2/chcronfilesdod<br>**แอ็คชันความเข้ากันได้**<br>ตรวจสอบให้แน่ใจว่า ระบบตรงกับข้อกำหนดที่ระบุไว้ |
| GEN003300 | 2 | ไฟล์ at.deny ต้องว่าง หากมีอยู่ | **ตำแหน่ง** /etc/security/pscexpert/dodv2/chcronfilesdod<br>**แอ็คชันความเข้ากันได้**<br>ตรวจสอบให้แน่ใจว่า ระบบตรงกับข้อกำหนดที่ระบุไว้ |
| GEN003320 | 2 | แอคเคาต์ระบบดีฟอลต์ที่ไม่ใช่ root ต้องไม่แสดงอยู่ในไฟล์ at.allow หรือต้อง สอดแทรกในไฟล์ at.deny หากไฟล์ at.allow ไม่มีอยู่ | **ตำแหน่ง** /etc/security/pscexpert/dodv2/chcronfilesdod<br>**แอ็คชันความเข้ากันได้**<br>ตรวจสอบให้แน่ใจว่า ระบบตรงกับข้อกำหนดที่ระบุไว้ |
| GEN003360 (เกี่ยวข้องกับ GEN000960, GEN003000, GEN003020, GEN003160, GEN003380) | 2 | at daemon ต้องไม่รันโปรแกรมที่สามารถเขียนได้แบบกลุ่มหรือแบบทั่วไป | **ตำแหน่ง** /etc/security/pscexpert/dodv2/rmwwpaths<br>**แอ็คชันความเข้ากันได้**<br>ตรวจสอบให้แน่ใจว่า ระบบตรงกับข้อกำหนด ที่ระบุไว้<br>**หมายเหตุ:** ค่าติดตั้งนี้ไม่ได้ถูกเปลี่ยนโดยอัตโนมัติเมื่อรีเซ็ตนโยบายเป็น นโยบายดีฟอลต์ของ AIX โดยใช้ไฟล์ DoDv2_to_AIXDefault.xml คุณต้องเปลี่ยนค่าติดตั้งนี้แบบแมนวล |
| GEN003380 (เกี่ยวข้องกับ GEN000960, GEN003000, GEN003020, GEN003160, GEN003360) | 2 | at daemon ต้องไม่รัน โปรแกรมใน หรือเป็นส่วนขยายของไดเร็กทอรีที่สามารถเขียนได้ทั่วไป | **ตำแหน่ง** /etc/security/pscexpert/dodv2/rmwwpaths<br>**แอ็คชันความเข้ากันได้**<br>ตรวจสอบให้แน่ใจว่า ระบบตรงกับข้อกำหนด ที่ระบุไว้<br>**หมายเหตุ:** ค่าติดตั้งนี้ไม่ได้ถูกเปลี่ยนโดยอัตโนมัติเมื่อรีเซ็ตนโยบายเป็น นโยบายดีฟอลต์ของ AIX โดยใช้ไฟล์ DoDv2_to_AIXDefault.xml คุณต้องเปลี่ยนค่าติดตั้งนี้แบบแมนวล |

*ตารางที่ 3. ข้อกำหนดทั่วไปของ DoD (ต่อ)*

| ID จุดตรวจสอบของ Department of Defense STIG | หมวดหมู่ของกฎ STIG | รายละเอียด | ตำแหน่งของสคริปต์ที่นิยามแอ็คชัน และผลลัพธ์ของแอ็คชันที่เปิดใช้งานความเข้ากันได้ |
|---|---|---|---|
| GEN003510 | 2 | ดัมพ์คอร์เคอร์เนลต้องถูกปิดใช้งาน ยกเว้นว่าจำเป็น | **ตำแหน่ง** `/etc/security/pscexpert/dodv2/coredumpdev`<br>**แอ็คชันความเข้ากันได้**<br>ปิดใช้งานดัมพ์คอร์เคอร์เนล |
| GEN003540 | 2 | ระบบต้องใช้สแต็กโปรแกรม ที่ไม่สามารถเรียกทำงานได้ | **ตำแหน่ง** `/etc/security/pscexpert/dodv2/sedconfigdod`<br>**แอ็คชันความเข้ากันได้**<br>บังคับใช้การใช้สแต็กโปรแกรมที่ไม่สามารถเรียกทำงานได้ |
| GEN003600 | 2 | ระบบต้องไม่ส่งต่อแพ็กเก็ตที่เราต์แหล่งที่มา IPv4 | **ตำแหน่ง** `/etc/security/pscexpert/dodv2/ntwkoptsdod`<br>**แอ็คชันความเข้ากันได้**<br>ตั้งค่าอ็อพชันเครือข่าย `ipsrcforward` เป็น *0* |
| GEN003601 | 2 | ขนาดคิวแบ็กล็อก TCP ต้องตั้งค่าไว้อย่างเหมาะสม | **ตำแหน่ง** `/etc/security/pscexpert/dodv2/ntwkoptsdod`<br>**แอ็คชันความเข้ากันได้**<br>ตั้งค่าอ็อพชันเครือข่าย `clean_partial_conns` เป็น *1* |
| GEN003603 | 2 | ระบบต้องไม่ตอบสนองต่อ Internet Control Message Protocol version 4 (ICMPv4) echoes ที่ส่งไปยัง แอดเดรสบอร์ดคาสก์ | **ตำแหน่ง** `/etc/security/pscexpert/dodv2/ntwkoptsdod`<br>**แอ็คชันความเข้ากันได้**<br>ตั้งค่าอ็อพชันเครือข่าย `bcastping` เป็น *0* |
| GEN003604 | 2 | ระบบต้องไม่ตอบสนองกับคำร้องขอการประทับเวลา ICMP ที่ส่งไปยังแอดเดรสบอร์ดคาสก์ | **ตำแหน่ง** `/etc/security/pscexpert/dodv2/ntwkoptsdod`<br>**แอ็คชันความเข้ากันได้**<br>ตั้งค่าอ็อพชันเครือข่าย `bcastping` เป็น *0* |
| GEN003605 | 2 | ระบบต้องไม่นำการเราต์แหล่งที่มาที่สงวนไว้ไปยังการตอบสนอง TCP | **ตำแหน่ง** `/etc/security/pscexpert/dodv2/ntwkoptsdod`<br>**แอ็คชันความเข้ากันได้**<br>ตั้งค่าอ็อพชันเครือข่าย `nonlocsrcroute` เป็น *0* |

*ตารางที่ 3. ข้อกำหนดทั่วไปของ DoD (ต่อ)*

| ID จุดตรวจสอบของ Department of Defense STIG | หมวดหมู่ของกฎ STIG | รายละเอียด | ตำแหน่งของสคริปต์ที่นิยามแอ็คชัน และผลลัพธ์ของแอ็คชันที่เปิดใช้งานความเข้ากันได้ |
|---|---|---|---|
| GEN003606 | 2 | ระบบต้องปกป้องแอ็พพลิเคชันโลคัล จากการสร้างแพ็กเก็ตที่เราต์แหล่งที่มา | **ตำแหน่ง** `/etc/security/pscexpert/dodv2/ntwkoptsdod`<br>**แอ็คชันความเข้ากันได้**<br>ตั้งค่าอ็อพชันเครือข่าย `ipsrcroutesend` เป็น *0* |
| GEN003607 | 2 | ระบบต้องไม่ยอมรับแพ็กเก็ต IPv4 ที่เราต์ แหล่งที่มา | **ตำแหน่ง** `/etc/security/pscexpert/dodv2/ntwkoptsdod`<br>**แอ็คชันความเข้ากันได้**<br>ปิดใช้งานความสามารถในการยอมรับแพ็กเก็ต IPv4 ที่เราต์แหล่งที่มา |
| GEN003609 | 2 | ระบบต้องละเว้นข้อความการเปลี่ยนทิศทาง IPv4 ICMP | **ตำแหน่ง** `/etc/security/pscexpert/dodv2/ntwkoptsdod`<br>**แอ็คชันความเข้ากันได้**<br>ตั้งค่าอ็อพชันเครือข่าย `ipignoreredirects` เป็น *1* |
| GEN003610 | 2 | ระบบต้องไม่ส่งข้อความการเปลี่ยนทิศทาง IPv4 ICMP | **ตำแหน่ง** `/etc/security/pscexpert/dodv2/ntwkoptsdod`<br>**แอ็คชันความเข้ากันได้**<br>ตั้งค่าอ็อพชันเครือข่าย `ipsendredirects` เป็น *0* |
| GEN003612 | 2 | ระบบต้องถูกกำหนดคอนฟิกเพื่อใช้ TCP syncookies เมื่อ TCP SYN flood เกิดขึ้น | **ตำแหน่ง** `/etc/security/pscexpert/dodv2/ntwkoptsdod`<br>**แอ็คชันความเข้ากันได้**<br>ตั้งค่าอ็อพชันเครือข่าย `clean_partial_conns` เป็น *1* |
| GEN003640 | 2 | ระบบไฟล์ root ต้องใช้การทำเจอร์นัล หรือเมธอดอื่นของการทำให้มั่นใจถึงความสอดคล้องกันของระบบไฟล์ | **ตำแหน่ง** `/etc/security/pscexpert/dodv2/chkjournal`<br>**แอ็คชันความเข้ากันได้**<br>เปิดใช้งานการทำเจอร์นัลบนระบบไฟล์ root |

*ตารางที่ 3. ข้อกำหนดทั่วไปของ DoD (ต่อ)*

| ID จุดตรวจสอบของ Department of Defense STIG | หมวดหมู่ของกฎ STIG | รายละเอียด | ตำแหน่งของสคริปต์ที่นิยามแอ็คชัน และผลลัพธ์ของแอ็คชันที่เปิดใช้งานความเข้ากันได้ |
|---|---|---|---|
| GEN003660 | 2 | ระบบต้องทำบันทึกข้อมูล การพิสูจน์ตัวตน | **ตำแหน่ง** `/etc/security/pscexpert/dodv2/chsyslogdod`<br>**แอ็คชันความเข้ากันได้**<br>เปิดใช้งานการทำบันทึกข้อมูล `auth` และ `info` |
| GEN003700 | 2 | `inetd` และ `xinetd` ต้องปิดใช้งานหรือถอนออกหากไม่มีเซอร์วิสเครือข่ายที่ใช้อยู่ | **ตำแหน่ง** `/etc/security/pscexpert/dodv2/dodv2services`<br>**แอ็คชันความเข้ากันได้**<br>ตรวจสอบให้แน่ใจว่า ระบบตรงกับข้อกำหนดที่ระบุไว้ |
| GEN003810 | 2 | เซอร์วิส `portmap` หรือ `rpcbind` ต้องไม่รันจนกว่าจะจำเป็น | **ตำแหน่ง** `/etc/security/pscexpert/dodv2/dodv2services`<br>**แอ็คชันความเข้ากันได้**<br>ตรวจสอบให้แน่ใจว่า ระบบตรงกับข้อกำหนดที่ระบุไว้ |
| GEN003815 | 2 | เซอร์วิส `portmap` หรือ `rpcbind` ต้องไม่ถูกติดตั้งไว้จนกว่าจะถูกใช้ | **ตำแหน่ง** `/etc/security/pscexpert/dodv2/dodv2services`<br>**แอ็คชันความเข้ากันได้**<br>ตรวจสอบให้แน่ใจว่า ระบบตรงกับข้อกำหนดที่ระบุไว้ |
| GEN003820-3860 | 1,2,3 | `rsh`, `rexexec`, and `telnet` daemons และเซอร์วิส `rlogind` ต้องไม่ถูกรัน | **ตำแหน่ง** `/etc/security/pscexpert/dodv2/inetdservices`<br>**แอ็คชันความเข้ากันได้**<br>ปิดใช้งาน daemons และเซอร์ที่จำเป็นโดยใส่คอมเมนต์ รายการในไฟล์ `/etc/inetd.conf` |
| GEN003865 | 2 | เครื่องมือการวิเคราะห์เครือข่ายต้องไม่ถูกติดตั้งไว้ | **ตำแหน่ง** `/etc/security/pscexpert/dodv2/dodv2services`<br>**แอ็คชันความเข้ากันได้**<br>ตรวจสอบให้แน่ใจว่า ระบบตรงกับข้อกำหนดที่ระบุไว้ |

*ตารางที่ 3. ข้อกำหนดทั่วไปของ DoD (ต่อ)*

| ID จุดตรวจสอบของ Department of Defense STIG | หมวดหมู่ของกฎ STIG | รายละเอียด | ตำแหน่งของสคริปต์ที่นิยามแอ็คชัน และผลลัพธ์ของแอ็คชันที่เปิดใช้งานความเข้ากันได้ |
|---|---|---|---|
| GEN003900 | 2 | ไฟล์ `hosts.lpd` (หรือเทียบเท่า) ต้องไม่มีเครื่องหมายบวก (+) | **ตำแหน่ง** `/etc/security/pscexpert/dodv2/printers`<br>**แอ็คชันความเข้ากันได้**<br>ตรวจสอบให้แน่ใจว่า ระบบตรงกับข้อกำหนดที่ระบุไว้ |
| GEN004220 | 1 | แอคเคาต์การดูแลจัดการต้องไม่รันเว็บเบราว์เซอร์ ยกเว้นว่าจำเป็นต้องมีสำหรับการดูแลจัดการเซอร์วิสโลคัล | **ตำแหน่ง** `/etc/security/pscexpert/dodv2/dodv2cat1`<br>**แอ็คชันความเข้ากันได้**<br>แสดงผลลัพธ์ของการทดสอบกฎที่ระบุเฉพาะ |
| GEN004460 | 2 | กฎนี้ทำบันทึกข้อมูล `auth` และ `info` | **ตำแหน่ง** `/etc/security/pscexpert/dodv2/chsyslogdod`<br>**แอ็คชันความเข้ากันได้**<br>เปิดใช้งานการทำบันทึกข้อมูล `auth` และ `info` |
| GEN004540 | 2 | กฎนี้ปิดใช้งานคำสั่งวิธีใช้ `sendmail` | **ตำแหน่ง** `/etc/security/pscexpert/dodv2/sendmailhelp`<br>`/etc/security/pscexpert/dodv2/dodv2cmntrows`<br>**แอ็คชันความเข้ากันได้**<br>ปิดใช้งานคำสั่งที่ระบุเฉพาะ |
| GEN004580 | 2 | ระบบต้องไม่ใช้ไฟล์ `.forward` | **ตำแหน่ง** `/etc/security/pscexpert/dodv2/forward`<br>**แอ็คชันความเข้ากันได้**<br>ปิดใช้งานไฟล์ที่ระบุ<br>**หมายเหตุ:** ค่าติดตั้งนี้ไม่ได้ถูกเปลี่ยนโดยอัตโนมัติเมื่อรีเซ็ตนโยบายเป็น นโยบายดีฟอลต์ของ AIX โดยใช้ไฟล์ `DoDv2_to_AIXDefault.xml` คุณต้องเปลี่ยนค่าติดตั้งนี้แบบแมนวล |

*ตารางที่ 3. ข้อกำหนดทั่วไปของ DoD (ต่อ)*

| ID จุดตรวจสอบของ Department of Defense STIG | หมวดหมู่ของกฎ STIG | รายละเอียด | ตำแหน่งของสคริปต์ที่นิยามแอ็คชัน และผลลัพธ์ของแอ็คชันที่เปิดใช้งานความเข้ากันได้ |
|---|---|---|---|
| GEN004600 | 1 | เซอร์วิส SMTP ต้องเป็น เวอร์ชันปัจจุบัน | **ตำแหน่ง** `/etc/security/pscexpert/dodv2/SMTP_ver`<br>**แอ็คชันความเข้ากันได้**<br>ตรวจสอบให้แน่ใจว่าเวอร์ชันล่าสุดของเซอร์วิสที่ระบุไว้กำลังรันอยู่<br>**หมายเหตุ:** ค่าติดตั้งนี้ไม่ได้ถูกเปลี่ยนโดยอัตโนมัติเมื่อรีเซ็ตนโยบายเป็น นโยบายดีฟอลต์ของ AIX โดยใช้ไฟล์ `DoDv2_to_AIXDefault.xml` คุณต้องเปลี่ยนค่าติดตั้งนี้แบบแมนวล |
| GEN004620 | 2 | เซิร์ฟเวอร์ `sendmail` ต้องปิดใช้งานคุณลักษณะการดีบัก | **ตำแหน่ง** `/etc/security/pscexpert/dodv2/SMTP_ver`<br>**แอ็คชันความเข้ากันได้**<br>ปิดใช้งานคุณสมบัติการดีบัก `sendmail` |
| GEN004640 | 1 | เซอร์วิส SMTP ต้องไม่มี `uudecode` alias ที่แอ็คทีฟ | **ตำแหน่ง** `/etc/security/pscexpert/dodv2/SMTPuucode`<br>**แอ็คชันความเข้ากันได้**<br>ปิดใช้งาน `uudecode` alias |
| GEN004710 | 2 | การรีเลย์เมลต้องเป็นข้อจำกัด | **ตำแหน่ง** `/etc/security/pscexpert/dodv2/sendmaildod`<br>**แอ็คชันความเข้ากันได้**<br>จำกัดการรีเลย์เมล |
| GEN004800 | 1,2,3 | FTP ที่ไม่ได้เข้ารหัสไว้ต้องไม่ถูกใช้บน ระบบ | **ตำแหน่ง** `/etc/security/pscexpert/dodv2/inetdservices`<br>**แอ็คชันความเข้ากันได้**<br>ปิดใช้งาน daemons และเซอร์ที่จำเป็นโดยใส่คอมเมนต์ รายการในไฟล์ `/etc/inetd.conf` |

*ตารางที่ 3. ข้อกำหนดทั่วไปของ DoD (ต่อ)*

| ID จุดตรวจสอบของ Department of Defense STIG | หมวดหมู่ของกฎ STIG | รายละเอียด | ตำแหน่งของสคริปต์ที่นิยามแอ็คชัน และผลลัพธ์ของแอ็คชันที่เปิดใช้งานความเข้ากันได้ |
|---|---|---|---|
| GEN004820 | 2 | FTP แบบไม่ระบุชื่อต้องไม่แอ็คทีฟบนระบบ จนกว่าจะได้รับสิทธิ์ | **ตำแหน่ง** `/etc/security/pscexpert/dodv2/anonuser`<br>**แอ็คชันความเข้ากันได้**<br>ปิดใช้งาน FTP แบบไม่ระบุชื่อบนระบบ<br>**หมายเหตุ:** ค่าติดตั้งนี้ไม่ได้ถูกเปลี่ยนโดยอัตโนมัติเมื่อรีเซ็ตนโยบายเป็น นโยบายดีฟอลต์ของ AIX โดยใช้ไฟล์ `DoDv2_to_AIXDefault.xml` คุณต้องเปลี่ยนค่าติดตั้งนี้แบบแมนวล |
| GEN004840 | 2 | ถ้าระบบเป็นเซิร์ฟเวอร์ FTP แบบไม่ระบุชื่อ ระบบจะต้องแยกออกเป็นเครือข่าย Demilitarized Zone (DMZ) | **ตำแหน่ง** `/etc/security/pscexpert/dodv2/anonuser`<br>**แอ็คชันความเข้ากันได้**<br>ตรวจสอบให้แน่ใจว่า FTP แบบไม่ระบุชื่อบนระบบอยู่บนเครือข่าย DMZ |
| GEN004880 | 2 | ไฟล์ `ftpusers` ต้องมีอยู่ | **ตำแหน่ง** `/etc/security/pscexpert/dodv2/chdodftpusers`<br>**แอ็คชันความเข้ากันได้**<br>ตรวจสอบให้แน่ใจว่า ไฟล์ที่ระบุอยู่บนระบบ |
| GEN004900 | 2 | ไฟล์ `ftpusers` ต้องมีชื่อแอคเคาต์ที่ไม่อนุญาตให้ใช้โปรโตคอล FTP | **ตำแหน่ง** `/etc/security/pscexpert/dodv2/chdodftpusers`<br>**แอ็คชันความเข้ากันได้**<br>ตรวจสอบให้แน่ใจว่า ไฟล์มีชื่อแอคเคาต์ที่จำเป็นต้องมี |

*ตารางที่ 3. ข้อกำหนดทั่วไปของ DoD (ต่อ)*

| ID จุดตรวจสอบของ Department of Defense STIG | หมวดหมู่ของกฎ STIG | รายละเอียด | ตำแหน่งของสคริปต์ที่นิยามแอ็คชัน และผลลัพธ์ของแอ็คชันที่เปิดใช้งานความเข้ากันได้ |
|---|---|---|---|
| GEN005000 | 1 | แอคเคาต์ FTP ที่ไม่ระบุชื่อต้องไม่มีเชลล์ การทำงาน | **ตำแหน่ง** `/etc/security/pscexpert/dodv2/usershells`<br>**แอ็คชันความเข้ากันได้**<br>ถอนเชลล์ออกจากแอคเคาต์ FTP ที่ไม่ระบุชื่อ<br>**หมายเหตุ:** ค่าติดตั้งนี้ไม่ได้ถูกเปลี่ยนโดยอัตโนมัติเมื่อรีเซ็ตนโยบายเป็น นโยบายดีฟอลต์ของ AIX โดยใช้ไฟล์ `DoDv2_to_AIXDefault.xml` คุณต้องเปลี่ยนค่าติดตั้งนี้แบบแมนวล |
| GEN005080 | 1 | `TFTP` daemon ต้องทำงาน ในโหมดความปลอดภัย ซึ่งจัดเตรียมการเข้าถึงไดเร็กทอรีเดี่ยว บนระบบโฮสต์ไฟล์เท่านั้น | **ตำแหน่ง** `/etc/security/pscexpert/dodv2/tftpdod`<br>**แอ็คชันความเข้ากันได้**<br>ตรวจสอบให้แน่ใจว่า daemon ตรงกับข้อกำหนดที่ระบุไว้ |
| GEN005120 | 2 | TFTP daemon ต้องถูกกำหนดไว้ให้กับข้อมูลจำเพาะของผู้จำหน่าย ซึ่งสอดแทรกแอคเคาต์ผู้ใช้ TFTP เฉพาะงาน เชลล์ที่ไม่มีการล็อกอิน เช่น `/bin/false` และโฮมไดเร็กทอรี ที่เป็นเจ้าของโดยผู้ใช้ TFTP | **ตำแหน่ง** `/etc/security/pscexpert/dodv2/tftpdod`<br>**แอ็คชันความเข้ากันได้**<br>ตรวจสอบให้แน่ใจว่า ระบบตรงกับข้อกำหนดที่ระบุไว้ |
| GEN005140 | 1,2,3 | TFTP daemon ที่แอ็คทีฟใดๆ ต้องได้รับสิทธิ์ และได้รับการอนุมัติในแพ็กเก็ตการรับรองระบบ | **ตำแหน่ง** `/etc/security/pscexpert/dodv2/inetdservices`<br>**แอ็คชันความเข้ากันได้**<br>ตรวจสอบให้แน่ใจว่า daemon ได้รับสิทธิ์ |
| GEN005160 | 1,2 | โฮสต์ X Window System ใดๆ ต้องเขียนไฟล์ `.Xauthority` | **ตำแหน่ง** `/etc/security/pscexpert/dodv2/dodv2disableX`<br>**แอ็คชันความเข้ากันได้**<br>ตรวจสอบให้แน่ใจว่า โฮสต์เขียนไฟล์ที่ระบุเฉพาะ |
| GEN005200 | 1,2 | การแสดงผล X Window System ใดๆ ไม่สามารถเอ็กซ์พอร์ตไปยังพับลิกได้ | **ตำแหน่ง** `/etc/security/pscexpert/dodv2/dodv2disableX`<br>**แอ็คชันความเข้ากันได้**<br>ปิดใช้งานการแพร่กระจายของโปรแกรม ที่ระบุเฉพาะ |

*ตารางที่ 3. ข้อกำหนดทั่วไปของ DoD (ต่อ)*

| ID จุดตรวจสอบของ Department of Defense STIG | หมวดหมู่ของกฎ STIG | รายละเอียด | ตำแหน่งของสคริปต์ที่นิยามแอ็คชัน และผลลัพธ์ของแอ็คชันที่เปิดใช้งานความเข้ากันได้ |
|---|---|---|---|
| GEN005220 | 1,2 | ไฟล์ .Xauthority หรือ X*.hosts (หรือเทียบเท่า) ต้องใช้เพื่อจำกัดการเข้าถึงเซิร์ฟเวอร์ X Window System | **ตำแหน่ง** /etc/security/pscexpert/dodv2/dodv2disableX<br>**แอ็คชันความเข้ากันได้** ตรวจสอบให้แน่ใจว่า ไฟล์ที่ระบุพร้อมใช้งานเพื่อจำกัดการเข้าถึงเซิร์ฟเวอร์ |
| GEN005240 | 1,2 | ยูทิลิตี .Xauthority ต้องอนุญาตให้เข้าถึงโฮสต์ที่ได้รับสิทธิ์เท่านั้น | **ตำแหน่ง** /etc/security/pscexpert/dodv2/dodv2disableX<br>**แอ็คชันความเข้ากันได้** ตรวจสอบให้แน่ใจว่า สิทธิ์ถูกจำกัดในโฮสต์ที่ได้รับสิทธิ์ |
| GEN005260 | 2 | กฎนี้ปิดใช้งานการเชื่อมต่อ X Window System และโปรแกรมจัดการการล็อกอิน XServer | **ตำแหน่ง** /etc/security/pscexpert/dodv2/dodv2cmntrows<br>**แอ็คชันความเข้ากันได้** ปิดใช้งานการเชื่อมต่อที่จำเป็นและโปรแกรมจัดการการล็อกอิน |
| GEN005280 | 1,2,3 | ระบบต้องไม่มีเซอร์วิส UUCP ที่แอ็คทีฟ | **ตำแหน่ง** /etc/security/pscexpert/dodv2/inetdservices<br>**แอ็คชันความเข้ากันได้** ปิดใช้งาน daemons และเซอร์ที่จำเป็นโดยใส่คอมเมนต์ รายการในไฟล์ /etc/inetd.conf |
| GEN005300 | 2 | ชุมชน SNMP ต้องถูกเปลี่ยนจากค่าติดตั้ง ดีฟอลต์ | **ตำแหน่ง** /etc/security/pscexpert/dodv2/chsnmp<br>**แอ็คชันความเข้ากันได้** ตรวจสอบให้แน่ใจว่า ระบบตรงกับข้อกำหนดที่ระบุไว้ |
| GEN005305 | 2 | เซอร์วิส SNMP ต้องใช้เฉพาะ SNMPv3 หรือเวอร์ชัน ถัดมา | **ตำแหน่ง** /etc/security/pscexpert/dodv2/chsnmp<br>**แอ็คชันความเข้ากันได้** ตรวจสอบให้แน่ใจว่า ระบบตรงกับข้อกำหนดที่ระบุไว้ |

*ตารางที่ 3. ข้อกำหนดทั่วไปของ DoD (ต่อ)*

| ID จุดตรวจสอบของ Department of Defense STIG | หมวดหมู่ของกฎ STIG | รายละเอียด | ตำแหน่งของสคริปต์ที่นิยามแอ็คชัน และผลลัพธ์ของแอ็คชันที่เปิดใช้งานความเข้ากันได้ |
|---|---|---|---|
| GEN005306 | 2 | เซอร์วิส SNMP ต้องใช้ FIPS 140-2 | **ตำแหน่ง** `/etc/security/pscexpert/dodv2/chsnmp`<br>**แอ็คชันความเข้ากันได้**<br>ตรวจสอบให้แน่ใจว่า ระบบตรงกับข้อกำหนดที่ระบุไว้ |
| GEN005440 | 2 | ระบบต้องใช้เซิร์ฟเวอร์ syslog แบบรีโมต (โฮสต์บันทึกการทำงาน) | **ตำแหน่ง** `/etc/security/pscexpert/dodv2/EnableTrustedLogging`<br>**แอ็คชันความเข้ากันได้**<br>ตรวจสอบให้แน่ใจว่าระบบกำลังใช้เซิร์ฟเวอร์ syslog แบบรีโมต |
| GEN005450 | 2 | ระบบต้องใช้เซิร์ฟเวอร์ syslog แบบรีโมต (โฮสต์บันทึกการทำงาน) | **ตำแหน่ง** `/etc/security/pscexpert/dodv2/EnableTrustedLogging`<br>**แอ็คชันความเข้ากันได้**<br>ตรวจสอบให้แน่ใจว่าระบบกำลังใช้เซิร์ฟเวอร์ syslog แบบรีโมต |
| GEN005460 | 2 | ระบบต้องใช้เซิร์ฟเวอร์ syslog แบบรีโมต (โฮสต์บันทึกการทำงาน) | **ตำแหน่ง** `/etc/security/pscexpert/dodv2/EnableTrustedLogging`<br>**แอ็คชันความเข้ากันได้**<br>ตรวจสอบให้แน่ใจว่าระบบกำลังใช้เซิร์ฟเวอร์ syslog แบบรีโมต |
| GEN005480 | 2 | ระบบต้องใช้เซิร์ฟเวอร์ syslog แบบรีโมต (โฮสต์บันทึกการทำงาน) | **ตำแหน่ง** `/etc/security/pscexpert/dodv2/EnableTrustedLogging`<br>**แอ็คชันความเข้ากันได้**<br>ตรวจสอบให้แน่ใจว่าระบบกำลังใช้เซิร์ฟเวอร์ syslog แบบรีโมต |
| GEN005500 | 2 | SSH daemon ต้องถูกกำหนดคอนฟิก เพื่อใช้เฉพาะโปรโตคอล Secure Shell เวอร์ชัน 2 (SSHv2) | **ตำแหน่ง** `/etc/security/pscexpert/dodv2/sshDoDconfig`<br>**แอ็คชันความเข้ากันได้**<br>ตรวจสอบให้แน่ใจว่า ระบบตรงกับข้อกำหนดที่ระบุไว้ |

*ตารางที่ 3. ข้อกำหนดทั่วไปของ DoD (ต่อ)*

| ID จุดตรวจสอบของ Department of Defense STIG | หมวดหมู่ของกฎ STIG | รายละเอียด | ตำแหน่งของสคริปต์ที่นิยามแอ็คชัน และผลลัพธ์ของแอ็คชันที่เปิดใช้งานความเข้ากันได้ |
|---|---|---|---|
| GEN005501 | 2 | ไคลเอ็นต์ SSH ต้องถูกกำหนดคอนฟิกไว้เพื่อใช้เฉพาะโปรโตคอล SSHv2 | **ตำแหน่ง** `/etc/security/pscexpert/dodv2/sshDoDconfig`<br>**แอ็คชันความเข้ากันได้**<br>ตรวจสอบให้แน่ใจว่า ระบบตรงกับข้อกำหนดที่ระบุไว้ |
| GEN005504 | 2 | SSH daemon ต้อง listen แอดเดรสเครือข่ายการจัดการ ยกเว้นว่าได้รับสิทธิ์ให้ใช้ ที่นอกเหนือจากการจัดการ | **ตำแหน่ง** `/etc/security/pscexpert/dodv2/sshDoDconfig`<br>**แอ็คชันความเข้ากันได้**<br>ตรวจสอบให้แน่ใจว่า ระบบตรงกับข้อกำหนดที่ระบุไว้ |
| GEN005505 | 2 | SSH daemon ต้องถูกกำหนดคอนฟิกเพื่อใช้เฉพาะ ciphers ที่สอดคล้องกับมาตรฐาน Federal Information Processing Standards (FIPS) 140-2 | **ตำแหน่ง** `/etc/security/pscexpert/dodv2/sshDoDconfig`<br>**แอ็คชันความเข้ากันได้**<br>ตรวจสอบให้แน่ใจว่า ระบบตรงกับข้อกำหนดที่ระบุไว้ |
| GEN005506 | 2 | SSH daemon ต้องถูกกำหนดคอนฟิก เพื่อใช้เฉพาะ ciphers ที่สอดคล้องกับมาตรฐาน FIPS 140-2 | **ตำแหน่ง** `/etc/security/pscexpert/dodv2/sshDoDconfig`<br>**แอ็คชันความเข้ากันได้**<br>ตรวจสอบให้แน่ใจว่า ระบบตรงกับข้อกำหนดที่ระบุไว้ |
| GEN005507 | 2 | SSH daemon ต้องถูกกำหนดคอนฟิก เพื่อใช้เฉพาะ Message Authentication Codes (MACs) ด้วยอัลกอริทึมการแฮช ของการเข้ารหัสที่สอดคล้องกับมาตรฐาน FIPS 140-2 | **ตำแหน่ง** `/etc/security/pscexpert/dodv2/sshDoDconfig`<br>**แอ็คชันความเข้ากันได้**<br>ตรวจสอบให้แน่ใจว่า ระบบตรงกับข้อกำหนดที่ระบุไว้ |
| GEN005510 | 2 | ไคลเอ็นต์ SSH ต้องถูกกำหนดคอนฟิก เพื่อใช้เฉพาะ MACs พร้อมกับ ciphers ที่สอดคล้องกับมาตรฐาน FIPS 140-2 | **ตำแหน่ง** `/etc/security/pscexpert/dodv2/sshDoDconfig`<br>**แอ็คชันความเข้ากันได้**<br>ตรวจสอบให้แน่ใจว่า ระบบตรงกับข้อกำหนดที่ระบุไว้ |

*ตารางที่ 3. ข้อกำหนดทั่วไปของ DoD (ต่อ)*

| ID จุดตรวจสอบของ Department of Defense STIG | หมวดหมู่ของกฎ STIG | รายละเอียด | ตำแหน่งของสคริปต์ที่นิยามแอ็คชัน และผลลัพธ์ของแอ็คชันที่เปิดใช้งานความเข้ากันได้ |
|---|---|---|---|
| GEN005511 | 2 | ไคลเอ็นต์ SSH ต้องถูกกำหนดคอนฟิก เพื่อใช้เฉพาะ MACs พร้อมกับ ciphers ที่สอดคล้องกับมาตรฐาน FIPS 140-2 | **ตำแหน่ง** `/etc/security/pscexpert/dodv2/sshDoDconfig`<br>**แอ็คชันความเข้ากันได้**<br>ตรวจสอบให้แน่ใจว่า ระบบตรงกับข้อกำหนดที่ระบุไว้ |
| GEN005512 | 2 | SSH daemon ต้องถูกกำหนดคอนฟิก เพื่อใช้เฉพาะ MACs ด้วยอัลกอริทึมการแฮชของการเข้ารหัส ที่สอดคล้องกับ FIPS 140-2 มาตรฐาน | **ตำแหน่ง** `/etc/security/pscexpert/dodv2/sshDoDconfig`<br>**แอ็คชันความเข้ากันได้**<br>ตรวจสอบให้แน่ใจว่า ระบบตรงกับข้อกำหนดที่ระบุไว้ |
| GEN005521 | 2 | SSH daemon ต้องจำกัดการล็อกอินแบบระบุผู้ใช้ กลุ่ม หรือทั้งสองแบบ | **ตำแหน่ง** `/etc/security/pscexpert/dodv2/sshDoDconfig`<br>**แอ็คชันความเข้ากันได้**<br>ตรวจสอบให้แน่ใจว่า ระบบตรงกับข้อกำหนดที่ระบุไว้ |
| GEN005536 | 2 | SSH daemon ต้องดำเนินการ ตรวจสอบโหมดแบบจำกัดของไฟล์คอนฟิกูเรชันโฮมไดเร็กทอรี | **ตำแหน่ง** `/etc/security/pscexpert/dodv2/sshDoDconfig`<br>**แอ็คชันความเข้ากันได้**<br>ตรวจสอบให้แน่ใจว่า ระบบตรงกับข้อกำหนดที่ระบุไว้ |
| GEN005537 | 2 | SSH daemon ต้องใช้การแยกสิทธิพิเศษ | **ตำแหน่ง** `/etc/security/pscexpert/dodv2/sshDoDconfig`<br>**แอ็คชันความเข้ากันได้**<br>ตรวจสอบให้แน่ใจว่า ระบบตรงกับข้อกำหนดที่ระบุไว้ |
| GEN005538 | 2 | SSH daemon ต้องไม่อนญาตให้ `rhosts` พิสูจน์ตัวตนโดยใช้ Rivest-Shamir-Adleman (RSA) cryptosystem | **ตำแหน่ง** `/etc/security/pscexpert/dodv2/sshDoDconfig`<br>**แอ็คชันความเข้ากันได้**<br>ตรวจสอบให้แน่ใจว่า ระบบตรงกับข้อกำหนดที่ระบุไว้ |

*ตารางที่ 3. ข้อกำหนดทั่วไปของ DoD (ต่อ)*

| ID จุดตรวจสอบของ Department of Defense STIG | หมวดหมู่ของกฎ STIG | รายละเอียด | ตำแหน่งของสคริปต์ที่นิยามแอ็คชัน และผลลัพธ์ของแอ็คชันที่เปิดใช้งานความเข้ากันได้ |
|---|---|---|---|
| GEN005539 | 2 | SSH daemon ต้องไม่อนุญาต ให้บีบอัดหรือต้องอนุญาตให้บีบอัดหลังจากการพิสูจน์ตัวตน เป็นผลสำเร็จ | **ตำแหน่ง** `/etc/security/pscexpert/dodv2/sshDoDconfig`<br>**แอ็คชันความเข้ากันได้**<br>ตรวจสอบให้แน่ใจว่า ระบบตรงกับข้อกำหนดที่ระบุไว้ |
| GEN005550 | 2 | SSH daemon ต้องถูกกำหนดคอนฟิก ด้วยแบนเนอร์ล็อกออน DoD | **ตำแหน่ง** `/etc/security/pscexpert/dodv2/sshDoDconfig`<br>**แอ็คชันความเข้ากันได้**<br>ตรวจสอบให้แน่ใจว่า ระบบตรงกับข้อกำหนดที่ระบุไว้ |
| GEN005560 | 2 | กำหนดว่ามีเกตเวย์ดีฟอลต์ ที่ถูกกำหนดคอนฟิกไว้สำหรับ IPv4 | **ตำแหน่ง** `/etc/security/pscexpert/dodv2/chkgtway`<br>**แอ็คชันความเข้ากันได้**<br>ตรวจสอบให้แน่ใจว่า ระบบตรงกับข้อกำหนดที่ระบุไว้<br>**หมายเหตุ:** ค่าติดตั้งนี้ไม่ได้ถูกเปลี่ยนโดยอัตโนมัติเมื่อรีเซ็ตนโยบายเป็น นโยบายดีฟอลต์ของ AIX โดยใช้ไฟล์ `DoDv2_to_AIXDefault.xml` คุณต้องเปลี่ยนค่าติดตั้งนี้แบบแมนวล<br>**หมายเหตุ:** ถ้าระบบของคุณ กำลังรันโปรโตคอล IPv6 ให้ตรวจสอบค่าติดตั้ง *ipv6_enabled* ในไฟล์ `/etc/security/pscexpert/ipv6.conf` ว่าตั้งค่า `yes` ไว้ ถ้าระบบไม่ได้ใช้ IPv6 ให้ตรวจสอบให้แน่ใจว่าค่า *ipv6_enabled* ถูกตั้งค่าเป็น `no` |

*ตารางที่ 3. ข้อกำหนดทั่วไปของ DoD (ต่อ)*

| ID จุดตรวจสอบของ Department of Defense STIG | หมวดหมู่ของกฎ STIG | รายละเอียด | ตำแหน่งของสคริปต์ที่นิยามแอ็คชัน และผลลัพธ์ของแอ็คชันที่เปิดใช้งานความเข้ากันได้ |
|---|---|---|---|
| GEN005570 | 2 | กำหนดว่ามีเกตเวย์ดีฟอลต์ ที่ถูกกำหนดคอนฟิกไว้สำหรับ IPv6 | **ตำแหน่ง** `/etc/security/pscexpert/dodv2/chkgtway`<br>**แอ็คชันความเข้ากันได้**<br>ตรวจสอบให้แน่ใจว่า ระบบตรงกับข้อกำหนดที่ระบุไว้<br>**หมายเหตุ:** ค่าติดตั้งนี้ไม่ได้ถูกเปลี่ยนโดยอัตโนมัติเมื่อรีเซ็ตนโยบายเป็น นโยบายดีฟอลต์ของ AIX โดยใช้ไฟล์ `DoDv2_to_AIXDefault.xml` คุณต้องเปลี่ยนค่าติดตั้งนี้แบบแมนวล<br>**หมายเหตุ:** ถ้าระบบของคุณ กำลังรันโปรโตคอล IPv6 ให้ตรวจสอบค่าติดตั้ง *ipv6_enabled* ในไฟล์ `/etc/security/pscexpert/ipv6.conf` ว่าตั้งค่า `yes` ไว้ ถ้าระบบไม่ได้ใช้ IPv6 ให้ตรวจสอบให้แน่ใจว่าค่า *ipv6_enabled* ถูกตั้งค่าเป็น `no` |
| GEN005590 | 2 | ระบบต้องไม่รัน daemons โปรโตคอลการเราต์ใดๆ ยกเว้นระบบคือเราเตอร์ | **ตำแหน่ง** `/etc/security/pscexpert/dodv2/dodv2cmntrows`<br>**แอ็คชันความเข้ากันได้**<br>ตรวจสอบให้แน่ใจว่า ระบบตรงกับข้อกำหนดที่ระบุไว้ |
| GEN005590 | 2 | ระบบต้องไม่รัน daemons โปรโตคอลการเราต์ใดๆ ยกเว้นระบบคือเราเตอร์ | **ตำแหน่ง** `/etc/security/pscexpert/dodv2/dodv2cmntrows`<br>**แอ็คชันความเข้ากันได้**<br>ตรวจสอบให้แน่ใจว่า ระบบตรงกับข้อกำหนดที่ระบุไว้ |
| GEN005600 | 2 | การส่งต่อ IP สำหรับ IPv4 ต้องไม่เปิดใช้งาน ยกเว้นว่าระบบคือเราเตอร์ | **ตำแหน่ง** `/etc/security/pscexpert/dodv2/ntwkoptsdod`<br>**แอ็คชันความเข้ากันได้**<br>ตั้งค่าอ็อพชันเครือข่าย `ipforwarding` เป็น *0* |

*ตารางที่ 3. ข้อกำหนดทั่วไปของ DoD (ต่อ)*

| ID จุดตรวจสอบของ Department of Defense STIG | หมวดหมู่ของกฎ STIG | รายละเอียด | ตำแหน่งของสคริปต์ที่นิยามแอ็คชัน และผลลัพธ์ของแอ็คชันที่เปิดใช้งานความเข้ากันได้ |
|---|---|---|---|
| GEN005610 | 2 | ระบบต้องไม่มีการส่งต่อ IP สำหรับ IPv6 ที่เปิดใช้งาน ยกเว้นระบบคือเราเตอร์ IPv6 | **ตำแหน่ง** `/etc/security/pscexpert/dodv2/ntwkoptsdod`<br>**แอ็คชันความเข้ากันได้**<br>ตั้งค่าอ็อพชันเครือข่าย `ip6forwarding` เป็น *1* |
| GEN005820 | 2 | NFS anonymous UID และ GID ต้องถูกกำหนดคอนฟิก เป็นค่าที่ไม่มีการให้สิทธิ์ | **ตำแหน่ง** `/etc/security/pscexpert/dodv2/nfsoptions`<br>**แอ็คชันความเข้ากันได้**<br>ตรวจสอบให้แน่ใจว่า ID ที่ระบุไว้ไม่มีการให้สิทธิ์ |
| GEN005840 | 2 | เซิร์ฟเวอร์ NFS ต้องถูกกำหนดคอนฟิกไว้เพื่อจำกัด การเข้าถึงระบบไฟล์ไปยังโลคัลโฮสต์ | **ตำแหน่ง** `/etc/security/pscexpert/dodv2/nfsoptions`<br>**แอ็คชันความเข้ากันได้**<br>กำหนดคอนฟิกเซิร์ฟเวอร์ NFS เพื่อจำกัดการเข้าถึงโลคัลโฮสต์ |
| GEN005880 | 2 | เซิร์ฟเวอร์ NFS ต้องไม่ได้รับอนุญาตให้ใช้การเข้าถึง root แบบรีโมต | **ตำแหน่ง** `/etc/security/pscexpert/dodv2/nfsoptions`<br>**แอ็คชันความเข้ากันได้**<br>ปิดใช้งานการเข้าถึง root แบบรีโมตบนเซิร์ฟเวอร์ NFS |
| GEN005900 | 2 | อ็อพชัน *nosuid* ต้องถูกเปิดใช้งานบนไคลเอ็นต์ NFS ที่เมาท์ทั้งหมด | **ตำแหน่ง** `/etc/security/pscexpert/dodv2/nosuid`<br>**แอ็คชันความเข้ากันได้**<br>เปิดใช้งานอ็อพชัน *nosuid* บนไคลเอ็นต์ NFS ที่เมาท์ทั้งหมด |
| GEN006060 | 2 | ระบบต้องไม่รัน `Samba` ยกเว้นว่าจำเป็น | **ตำแหน่ง** `/etc/security/pscexpert/dodv2/dodv2services`<br>**แอ็คชันความเข้ากันได้**<br>ตรวจสอบให้แน่ใจว่า ระบบตรงกับข้อกำหนดที่ระบุไว้ |

*ตารางที่ 3. ข้อกำหนดทั่วไปของ DoD (ต่อ)*

| ID จุดตรวจสอบของ Department of Defense STIG | หมวดหมู่ของกฎ STIG | รายละเอียด | ตำแหน่งของสคริปต์ที่นิยามแอ็คชัน และผลลัพธ์ของแอ็คชันที่เปิดใช้งานความเข้ากันได้ |
|---|---|---|---|
| GEN006380 | 1 | ระบบต้องไม่ใช่ UDP สำหรับ NIS หรือ NIS+ | **ตำแหน่ง** `/etc/security/pscexpert/dodv2/dodv2cat1`<br>**แอ็คชันความเข้ากันได้** แสดงผลลัพธ์ของการทดสอบกฎที่ระบุเฉพาะ |
| GEN006400 | 2 | โปรโตคอล Network Information System (NIS) ต้องไม่ถูกใช้ | **ตำแหน่ง** `/etc/security/pscexpert/dodv2/nisplus`<br>**แอ็คชันความเข้ากันได้** ปิดใช้งานโปรโตคอลที่ระบุเฉพาะ **หมายเหตุ:** ค่าติดตั้งนี้ไม่ได้ถูกเปลี่ยนโดยอัตโนมัติเมื่อรีเซ็ตนโยบายเป็น นโยบายดีฟอลต์ของ AIX โดยใช้ไฟล์ `DoDv2_to_AIXDefault.xml` คุณต้องเปลี่ยนค่าติดตั้งนี้แบบแมนวล |
| GEN006420 | 2 | แม็พ NIS ต้องได้รับการปกป้องโดยใช้โดเมนเนมแบบ ยากที่จะเดา | **ตำแหน่ง** `/etc/security/pscexpert/dodv2/nisplus`<br>**แอ็คชันความเข้ากันได้** ตรวจสอบให้แน่ใจว่า โดเมนเนมยากที่จะกำหนดได้ |
| GEN006460 | 2 | เซิร์ฟเวอร์ NIS+ ใดๆ ต้องทำงานที่ความปลอดภัยระดับ 2 | **ตำแหน่ง** `/etc/security/pscexpert/dodv2/nisplus`<br>**แอ็คชันความเข้ากันได้** ตรวจสอบให้แน่ใจว่า เซิร์ฟเวอร์อยู่ที่ระดับความปลอดภัยที่ต่ำที่สุด **หมายเหตุ:** ค่าติดตั้งนี้ไม่ได้ถูกเปลี่ยนโดยอัตโนมัติเมื่อรีเซ็ตนโยบายเป็น นโยบายดีฟอลต์ของ AIX โดยใช้ไฟล์ `DoDv2_to_AIXDefault.xml` คุณต้องเปลี่ยนค่าติดตั้งนี้แบบแมนวล |
| GEN006480 | 2 | ระบบต้องถูกตรวจสอบทุกสัปดาห์สำหรับไฟล์ `setuid` ที่ไม่ได้รับสิทธิ์ และโมดิฟิเคชันที่ไม่ได้รับสิทธิ์เพื่อให้สิทธิ์กับไฟล์ `setuid` | **ตำแหน่ง** `/etc/security/pscexpert/dodv2/trust`<br>**แอ็คชันความเข้ากันได้** ตรวจสอบทุกสัปดาห์เพื่อระบุความเปลี่ยนแปลงกับไฟล์ ที่ระบุไว้ |

*ตารางที่ 3. ข้อกำหนดทั่วไปของ DoD (ต่อ)*

| ID จุดตรวจสอบของ Department of Defense STIG | หมวดหมู่ของกฎ STIG | รายละเอียด | ตำแหน่งของสคริปต์ที่นิยามแอ็คชัน และผลลัพธ์ของแอ็คชันที่เปิดใช้งานความเข้ากันได้ |
|---|---|---|---|
| GEN006560 | 2 | ระบบต้องถูกตรวจสอบทุกสัปดาห์สำหรับไฟล์ `setuid` ที่ไม่ได้รับสิทธิ์ และโมดิฟิเคชันที่ไม่ได้รับสิทธิ์เพื่อให้สิทธิ์กับไฟล์ `setuid` | **ตำแหน่ง** `/etc/security/pscexpert/dodv2/trust`<br>**แอ็คชันความเข้ากันได้** ตรวจสอบทุกสัปดาห์เพื่อระบุความเปลี่ยนแปลงกับไฟล์ที่ระบุไว้ |
| GEN006580 | 2 | ระบบต้องใช้โปรแกรมควบคุมการเข้าถึง | **ตำแหน่ง** `/etc/security/pscexpert/dodv2/checktcpd`<br>**แอ็คชันความเข้ากันได้** ตรวจสอบให้แน่ใจว่า ระบบตรงกับข้อกำหนดที่ระบุไว้ |
| GEN006600 | 2 | โปรแกรมควบคุมการเข้าถึงของระบบ ต้องจดบันทึกความพยายามในการเข้าถึงระบบแต่ละครั้ง | **ตำแหน่ง** `/etc/security/pscexpert/dodv2/chsyslogdod`<br>**แอ็คชันความเข้ากันได้** ตรวจสอบให้แน่ใจว่าความพยายามในการเข้าถึงถูกจดบันทึกแล้ว |
| GEN006620 | 2 | โปรแกรมควบคุมการเข้าถึงของระบบ ต้องถูกกำหนดคอนฟิกไว้เพื่อให้สิทธิ์หรือปฏิเสธระบบในการเข้าถึงโฮสต์ที่ระบุเฉพาะ | **ตำแหน่ง** `/etc/security/pscexpert/dodv2/chetchostsdod`<br>**แอ็คชันความเข้ากันได้** กำหนดคอนฟิกไฟล์ `hosts.deny` และ `hosts.allow` เป็นค่าติดตั้งที่จำเป็น |
| GEN007020 | 2 | Stream Control Transmission Protocol (SCTP) ต้องถูกปิดใช้งาน | **ตำแหน่ง** `/etc/security/pscexpert/dodv2/dodv2netrules`<br>**แอ็คชันความเข้ากันได้** ปิดใช้งานโปรโตคอลที่ระบุเฉพาะ |

*ตารางที่ 3. ข้อกำหนดทั่วไปของ DoD (ต่อ)*

| ID จุดตรวจสอบของ Department of Defense STIG | หมวดหมู่ของกฎ STIG | รายละเอียด | ตำแหน่งของสคริปต์ที่นิยามแอ็คชัน และผลลัพธ์ของแอ็คชันที่เปิดใช้งานความเข้ากันได้ |
|---|---|---|---|
| GEN007700 | 2 | ตัวจัดการโปรโตคอล IPv6 ต้องไม่โยงกับ สแต็กเครือข่าย ยกเว้นว่าจำเป็น | **ตำแหน่ง** `/etc/security/pscexpert/dodv2/rminet6`<br>**แอ็คชันความเข้ากันได้**<br>ปิดใช้งานตัวจัดการโปรโตคอล IPv6 จากสแต็กเครือข่าย ยกเว้นว่าโปรแกรมจัดการถูกระบุอยู่ในไฟล์ `/etc/ipv6.conf`<br>**หมายเหตุ:** ถ้าระบบของคุณ กำลังรันโปรโตคอล IPv6 ให้ตรวจสอบค่าติดตั้ง *ipv6_enabled* ในไฟล์ `/etc/security/pscexpert/ipv6.conf` ว่าตั้งค่า `yes` ไว้ ถ้าระบบไม่ได้ใช้ IPv6 ให้ตรวจสอบให้แน่ใจว่าค่า *ipv6_enabled* ถูกตั้งค่าเป็น `no` |
| GEN007780 | 2 | ระบบต้องไม่มีท่อ `6to4` ที่เปิดใช้งาน | **ตำแหน่ง** `/etc/security/pscexpert/dodv2/rmiface`<br>**แอ็คชันความเข้ากันได้**<br>ปิดใช้งานท่อที่ระบุไว้<br>**หมายเหตุ:** ค่าติดตั้งนี้ไม่ได้ถูกเปลี่ยนโดยอัตโนมัติเมื่อรีเซ็ตนโยบายเป็น นโยบายดีฟอลต์ของ AIX โดยใช้ไฟล์ `DoDv2_to_AIXDefault.xml` คุณต้องเปลี่ยนค่าติดตั้งนี้แบบแมนวล |
| GEN007820 | 2 | ระบบต้องไม่มี IP ที่ถูกกำหนดคอนฟิกไว้ | **ตำแหน่ง** `/etc/security/pscexpert/dodv2/rmtunnel`<br>**แอ็คชันความเข้ากันได้**<br>ปิดใช้งานท่อ IP<br>**หมายเหตุ:** ค่าติดตั้งนี้ไม่ได้ถูกเปลี่ยนโดยอัตโนมัติเมื่อรีเซ็ตนโยบายเป็น นโยบายดีฟอลต์ของ AIX โดยใช้ไฟล์ `DoDv2_to_AIXDefault.xml` คุณต้องเปลี่ยนค่าติดตั้งนี้แบบแมนวล |

*ตารางที่ 3. ข้อกำหนดทั่วไปของ DoD (ต่อ)*

| ID จุดตรวจสอบของ Department of Defense STIG | หมวดหมู่ของกฎ STIG | รายละเอียด | ตำแหน่งของสคริปต์ที่นิยามแอ็คชัน และผลลัพธ์ของแอ็คชันที่เปิดใช้งานความเข้ากันได้ |
|---|---|---|---|
| GEN007840 | 2 | ไคลเอ็นต์ DHCP ต้องถูกปิดใช้งาน หากไม่ได้ใช้ | **ตำแหน่ง** `/etc/security/pscexpert/dodv2/dodv2services`<br>**แอ็คชันความเข้ากันได้** ตรวจสอบให้แน่ใจว่า ระบบตรงกับข้อกำหนดที่ระบุไว้ |
| GEN007850 | 2 | ไคลเอ็นต์ DHCP ต้องไม่ส่งอัพเดต DNS แบบไดนามิก | **ตำแหน่ง** `/etc/security/pscexpert/dodv2/dodv2services`<br>**แอ็คชันความเข้ากันได้** ตรวจสอบให้แน่ใจว่า ระบบตรงกับข้อกำหนดที่ระบุไว้ |
| GEN007860 | 2 | ระบบต้องละเว้นข้อความการเปลี่ยนทิศทาง IPv6 ICMP | **ตำแหน่ง** `/etc/security/pscexpert/dodv2/ntwkoptsdod`<br>**แอ็คชันความเข้ากันได้** ตั้งค่าอ็อพชันเครือข่าย `ipignoreredirects` เป็น *1* |
| GEN007880 | 2 | ระบบต้องไม่ส่งการเปลี่ยนทิศทาง IPv6 ICMP | **ตำแหน่ง** `/etc/security/pscexpert/dodv2/ntwkoptsdod`<br>**แอ็คชันความเข้ากันได้** ตั้งค่าอ็อพชันเครือข่าย `ipsendredirects` เป็น *0* |
| GEN007900 | 2 | ระบบต้องใช้ตัวกรอง reverse-path สำหรับทราฟฟิกเครือข่าย IPv6 หากระบบใช้ IPv6 | **ตำแหน่ง** `/etc/security/pscexpert/dodv2/chuserstanzadod`<br>**แอ็คชันความเข้ากันได้** ตรวจสอบให้แน่ใจว่า ระบบตรงกับข้อกำหนดที่ระบุไว้ |
| GEN007920 | 2 | ระบบต้องไม่ส่งต่อแพ็กเก็ตที่เราต์แหล่งที่มา IPv6 | **ตำแหน่ง** `/etc/security/pscexpert/dodv2/ntwkoptsdod`<br>**แอ็คชันความเข้ากันได้** ตั้งค่าอ็อพชันเครือข่าย `ip6srcrouteforward` เป็น *0* |

*ตารางที่ 3. ข้อกำหนดทั่วไปของ DoD (ต่อ)*

| ID จุดตรวจสอบของ Department of Defense STIG | หมวดหมู่ของกฎ STIG | รายละเอียด | ตำแหน่งของสคริปต์ที่นิยามแอ็คชัน และผลลัพธ์ของแอ็คชันที่เปิดใช้งานความเข้ากันได้ |
|---|---|---|---|
| GEN007940: GEN003607 | 2 | ระบบต้องไม่ยอมรับแพ็กเก็ตที่เราต์แหล่งที่มา IPv4 หรือ IPv6 | **ตำแหน่ง** `/etc/security/pscexpert/dodv2/ntwkoptsdod`<br>**แอ็คชันความเข้ากันได้**<br>ตั้งค่าอ็อพชันเครือข่าย `ipsrcrouterecv` เป็น *0* |
| GEN007950 | 2 | ระบบต้องไม่ตอบสนองต่อคำร้องขอ ICMPv6 echo ที่ส่งไปยังแอดเดรสบอร์ดคาสก์ | **ตำแหน่ง** `/etc/security/pscexpert/dodv2/ntwkoptsdod`<br>**แอ็คชันความเข้ากันได้**<br>ตั้งค่าอ็อพชันเครือข่าย `bcastping` เป็น *0* |
| GEN008000 | 2 | ถ้าระบบกำลังใช้ Lightweight Directory Access Protocol (LDAP) สำหรับการพิสูจน์ตัวตนหรือข้อมูลแอคเคาต์ ใบรับรองที่ใช้เพื่อพิสูจน์ตัวตนไปยังเซิร์ฟเวอร์ LDAP ต้องถูกจัดเตรียมไว้จาก เมธอด DoD PKI หรือ DoD ที่ได้รับอนุมัติ | **ตำแหน่ง** `/etc/security/pscexpert/dodv2/ldap_config`<br>**แอ็คชันความเข้ากันได้**<br>ตรวจสอบให้แน่ใจว่า ระบบตรงกับข้อกำหนดที่ระบุไว้ |
| GEN008020 | 2 | ถ้าระบบกำลังใช้ LDAP สำหรับการพิสูจน์ตัวตน หรือข้อมูลแอคเคาต์ การเชื่อมต่อ LDAP Transport Layer Security (TLS) ต้องการให้เซิร์ฟเวอร์จัดเตรียมใบรับรองที่มีพาธที่เชื่อถือได้ที่ถูกต้อง | **ตำแหน่ง** `/etc/security/pscexpert/dodv2/ldap_config`<br>**แอ็คชันความเข้ากันได้**<br>ตรวจสอบให้แน่ใจว่า ระบบตรงกับข้อกำหนดที่ระบุไว้ |
| GEN008050 | 2 | ถ้าระบบกำลังใช้ LDAP สำหรับการพิสูจน์ตัวตน หรือข้อมูลแอคเคาต์ ไฟล์ `/etc/ldap.conf` (หรือเทียบเท่า) ต้องไม่มีรหัสผ่าน | **ตำแหน่ง** `/etc/security/pscexpert/dodv2/ldap_config`<br>**แอ็คชันความเข้ากันได้**<br>ตรวจสอบให้แน่ใจว่า ระบบตรงกับข้อกำหนดที่ระบุไว้ |
| GEN008380 | 2 | ระบบต้องถูกตรวจสอบทุกสัปดาห์สำหรับไฟล์ `setuid` ที่ไม่ได้รับสิทธิ์ และโมดิฟิเคชันที่ไม่ได้รับสิทธิ์เพื่อให้สิทธิ์กับไฟล์ `setuid` | **ตำแหน่ง** `/etc/security/pscexpert/dodv2/trust`<br>**แอ็คชันความเข้ากันได้**<br>ตรวจสอบทุกสัปดาห์เพื่อระบุความเปลี่ยนแปลงกับไฟล์ ที่ระบุไว้ |

*ตารางที่ 3. ข้อกำหนดทั่วไปของ DoD (ต่อ)*

| ID จุดตรวจสอบของ Department of Defense STIG | หมวดหมู่ของกฎ STIG | รายละเอียด | ตำแหน่งของสคริปต์ที่นิยามแอ็คชัน และผลลัพธ์ของแอ็คชันที่เปิดใช้งานความเข้ากันได้ |
|---|---|---|---|
| GEN008520 | 2 | ระบบต้องใช้ไฟร์วอลล์โลคัล ที่ปกป้องโฮสต์จากการสแกนพอร์ต ไฟร์วอลล์ต้องสับเปลี่ยนพอร์ตที่มีค่า เป็นเวลา 5 นาที เพื่อปกป้องโฮสต์จากการสแกนพอร์ต | **ตำแหน่ง** `/etc/security/pscexpert/dodv2/ipsecshunports`<br>**แอ็คชันความเข้ากันได้**<br>ตรวจสอบให้แน่ใจว่า ระบบตรงกับข้อกำหนดที่ระบุไว้ |
| GEN008540 | 2 | ไฟร์วอลล์โลคัลของระบบต้องใช้นโยบาย *deny-all*, *allow-by-exception* | **ตำแหน่ง** `/etc/security/pscexpert/dodv2/ipsecshunhosthls`<br>**แอ็คชันความเข้ากันได้**<br>ตรวจสอบให้แน่ใจว่า ระบบตรงกับข้อกำหนดที่ระบุไว้<br>**หมายเหตุ:** คุณสามารถ ป้อนกฎการกรองเพิ่มเติมในไฟล์ `/etc/security/aixpert/bin/filter.txt` กฎเหล่านี้ ถูกรวมไว้โดยสคริปต์ `ipsecshunhosthls.sh` เมื่อคุณใช้โปรไฟล์ รายการต่างๆ ควรอยู่ในรูปแบบ ต่อไปนี้:<br>*`port_number`*`:`*`ip_address`*`:`*`action`*<br>โดยที่ ค่าที่อาจเกิดขึ้นได้สำหรับ *action* คือ `Allow` หรือ `Deny` |
| GEN008600 | 1 | ระบบต้องถูกกำหนดคอนฟิกไว้เพื่อเริ่มต้นจาก คอนฟิกูเรชันบูตระบบ | **ตำแหน่ง** `/etc/security/pscexpert/dodv2/dodv2cat1`<br>**แอ็คชันความเข้ากันได้**<br>ตรวจสอบให้แน่ใจว่าการเริ่มต้นระบบใช้คอนฟิกูเรชันบูตระบบ เท่านั้น |
| GEN008640 | 1 | ระบบต้องไม่ใช้สื่อบันทึกที่สามารถถอดออกได้ เป็นโหลดเดอร์บูต | **ตำแหน่ง** `/etc/security/pscexpert/dodv2/dodv2cat1`<br>**แอ็คชันความเข้ากันได้**<br>ตรวจสอบให้แน่ใจว่า ระบบไม่ได้บูตจากไดรฟ์ที่สามารถถอดออกได้ |

*ตารางที่ 3. ข้อกำหนดทั่วไปของ DoD (ต่อ)*

| ID จุดตรวจสอบของ Department of Defense STIG | หมวดหมู่ของกฎ STIG | รายละเอียด | ตำแหน่งของสคริปต์ที่นิยามแอ็คชัน และผลลัพธ์ของแอ็คชันที่เปิดใช้งานความเข้ากันได้ |
|---|---|---|---|
| GEN009140 | 1,2,3 | ระบบต้องไม่ให้เซอร์วิส chargen แอ็คทีฟ | **ตำแหน่ง** /etc/security/pscexpert/dodv2/inetdservices<br>**แอ็คชันความเข้ากันได้**<br>ปิดใช้งาน daemons และเซอร์ที่จำเป็นโดยใส่คอมเมนต์ รายการในไฟล์ /etc/inetd.conf |
| GEN009160 | 1,2,3 | ระบบต้องไม่มีเซอร์วิส Calendar Management Service Daemon (CMSD) ที่แอ็คทีฟ | **ตำแหน่ง** /etc/security/pscexpert/dodv2/inetdservices<br>**แอ็คชันความเข้ากันได้**<br>ปิดใช้งาน daemons และเซอร์ที่จำเป็นโดยใส่คอมเมนต์ รายการในไฟล์ /etc/inetd.conf |
| GEN009180 | 1,2,3 | ระบบต้องไม่มีเซอร์วิส tool-talk database server (ttdbserver) ที่แอ็คทีฟ | **ตำแหน่ง** /etc/security/pscexpert/dodv2/inetdservices<br>**แอ็คชันความเข้ากันได้**<br>ปิดใช้งาน daemons และเซอร์ที่จำเป็นโดยใส่คอมเมนต์ รายการในไฟล์ /etc/inetd.conf |
| GEN009190 | 1,2,3 | ระบบต้องไม่มีเซอร์วิส comsat ที่แอ็คทีฟ | **ตำแหน่ง** /etc/security/pscexpert/dodv2/inetdservices<br>**แอ็คชันความเข้ากันได้**<br>ปิดใช้งาน daemons และเซอร์ที่จำเป็นโดยใส่คอมเมนต์ รายการในไฟล์ /etc/inetd.conf |
| GEN009200-9330 | 1,2,3 | ระบบไม่สามารถมีเซอร์วิสอื่นๆ และ daemons ที่แอ็คทีฟ | **ตำแหน่ง** /etc/security/pscexpert/dodv2/inetdservices<br>**แอ็คชันความเข้ากันได้**<br>ปิดใช้งาน daemons และเซอร์ที่จำเป็นโดยใส่คอมเมนต์ รายการในไฟล์ /etc/inetd.conf |
| GEN009210 | 2 | ระบบต้องไม่มีเซอร์วิส discard ที่แอ็คทีฟ | **ตำแหน่ง** /etc/security/pscexpert/dodv2/inetdservices<br>**แอ็คชันความเข้ากันได้**<br>ปิดใช้งาน daemons และเซอร์ที่จำเป็นโดยใส่คอมเมนต์ รายการในไฟล์ /etc/inetd.conf |

*ตารางที่ 3. ข้อกำหนดทั่วไปของ DoD (ต่อ)*

| ID จุดตรวจสอบของ Department of Defense STIG | หมวดหมู่ของกฎ STIG | รายละเอียด | ตำแหน่งของสคริปต์ที่นิยามแอ็คชัน และผลลัพธ์ของแอ็คชันที่เปิดใช้งานความเข้ากันได้ |
|---|---|---|---|
| GEN009220 | 2 | ระบบต้องไม่มีเซอร์วิส dtspc ที่แอ็คทีฟ | **ตำแหน่ง** /etc/security/pscexpert/dodv2/inetdservices<br>**แอ็คชันความเข้ากันได้**<br>ปิดใช้งาน daemons และเซอร์ที่จำเป็นโดยใส่คอมเมนต์ รายการในไฟล์ /etc/inetd.conf |
| GEN009230 | 2 | ระบบต้องไม่มีเซอร์วิส echo ที่แอ็คทีฟ | **ตำแหน่ง** /etc/security/pscexpert/dodv2/inetdservices<br>**แอ็คชันความเข้ากันได้**<br>ปิดใช้งาน daemons และเซอร์ที่จำเป็นโดยใส่คอมเมนต์ รายการในไฟล์ /etc/inetd.conf |
| GEN009240 | 2 | ระบบต้องไม่มีเซอร์วิส Internet Message Access Protocol (IMAP) ที่แอ็คทีฟ | **ตำแหน่ง** /etc/security/pscexpert/dodv2/inetdservices<br>**แอ็คชันความเข้ากันได้**<br>ปิดใช้งาน daemons และเซอร์ที่จำเป็นโดยใส่คอมเมนต์ รายการในไฟล์ /etc/inetd.conf |
| GEN009250 | 2 | ระบบต้องไม่มีเซอร์วิส PostOffice Protocol (POP3) ที่แอ็คทีฟ | **ตำแหน่ง** /etc/security/pscexpert/dodv2/inetdservices<br>**แอ็คชันความเข้ากันได้**<br>ปิดใช้งาน daemons และเซอร์ที่จำเป็นโดยใส่คอมเมนต์ รายการในไฟล์ /etc/inetd.conf |
| GEN009260 | 2 | ระบบต้องไม่มีเซอร์วิส talk หรือ ntalk ที่แอ็คทีฟ | **ตำแหน่ง** /etc/security/pscexpert/dodv2/inetdservices<br>**แอ็คชันความเข้ากันได้**<br>ปิดใช้งาน daemons และเซอร์ที่จำเป็นโดยใส่คอมเมนต์ รายการในไฟล์ /etc/inetd.conf |
| GEN009270 | 2 | ระบบต้องไม่มีเซอร์วิส netstat ที่แอ็คทีฟบนกระบวนการ InetD | **ตำแหน่ง** /etc/security/pscexpert/dodv2/inetdservices<br>**แอ็คชันความเข้ากันได้**<br>ปิดใช้งาน daemons และเซอร์ที่จำเป็นโดยใส่คอมเมนต์ รายการในไฟล์ /etc/inetd.conf |

*ตารางที่ 3. ข้อกำหนดทั่วไปของ DoD (ต่อ)*

| ID จุดตรวจสอบของ Department of Defense STIG | หมวดหมู่ของกฎ STIG | รายละเอียด | ตำแหน่งของสคริปต์ที่นิยามแอ็คชัน และผลลัพธ์ของแอ็คชันที่เปิดใช้งานความเข้ากันได้ |
|---|---|---|---|
| GEN009280 | 2 | ระบบต้องไม่มีเซอร์วิส PCNFS ที่แอ็คทีฟ | **ตำแหน่ง** /etc/security/pscexpert/dodv2/inetdservices<br>**แอ็คชันความเข้ากันได้**<br>ปิดใช้งาน daemons และเซอร์ที่จำเป็นโดยใส่คอมเมนต์ รายการในไฟล์ /etc/inetd.conf |
| GEN009290 | 2 | ระบบต้องไม่มีเซอร์วิส systat ที่แอ็คทีฟ | **ตำแหน่ง** /etc/security/pscexpert/dodv2/inetdservices<br>**แอ็คชันความเข้ากันได้**<br>ปิดใช้งาน daemons และเซอร์ที่จำเป็นโดยใส่คอมเมนต์ รายการในไฟล์ /etc/inetd.conf |
| GEN009300 | 2 | เซอร์วิส inetd time ต้อไม่แอ็คทีฟบนระบบบน inetd daemon | **ตำแหน่ง** /etc/security/pscexpert/dodv2/inetdservices<br>**แอ็คชันความเข้ากันได้**<br>ปิดใช้งาน daemons และเซอร์ที่จำเป็นโดยใส่คอมเมนต์ รายการในไฟล์ /etc/inetd.conf |
| GEN009310 | 2 | ระบบต้องไม่มีเซอร์วิส rusersd ที่แอ็คทีฟ | **ตำแหน่ง** /etc/security/pscexpert/dodv2/inetdservices<br>**แอ็คชันความเข้ากันได้**<br>ปิดใช้งาน daemons และเซอร์ที่จำเป็นโดยใส่คอมเมนต์ รายการในไฟล์ /etc/inetd.conf |
| GEN009320 | 2 | ระบบต้องไม่มีเซอร์วิส sprayd ที่แอ็คทีฟ | **ตำแหน่ง** /etc/security/pscexpert/dodv2/inetdservices<br>**แอ็คชันความเข้ากันได้**<br>ปิดใช้งาน daemons และเซอร์ที่จำเป็นโดยใส่คอมเมนต์ รายการในไฟล์ /etc/inetd.conf |
| GEN009330 | 2 | ระบบต้องไม่มีเซอร์วิส rstatd ที่แอ็คทีฟ | **ตำแหน่ง** /etc/security/pscexpert/dodv2/inetdservices<br>**แอ็คชันความเข้ากันได้**<br>ปิดใช้งาน daemons และเซอร์ที่จำเป็นโดยใส่คอมเมนต์ รายการในไฟล์ /etc/inetd.conf |

*ตารางที่ 3. ข้อกำหนดทั่วไปของ DoD (ต่อ)*

| ID จุดตรวจสอบของ Department of Defense STIG | หมวดหมู่ของกฎ STIG | รายละเอียด | ตำแหน่งของสคริปต์ที่นิยามแอ็คชัน และผลลัพธ์ของแอ็คชันที่เปิดใช้งานความเข้ากันได้ |
|---|---|---|---|
| GEN009340 | 2 | โปรแกรมจัดการการล็อกอิน X server ต้องไม่รัน ยกเว้นว่าจำเป็นสำหรับการจัดการกับเซสชัน X11 | **ตำแหน่ง** `/etc/security/pscexpert/dodv2/dodv2cmntrows`<br>**แอ็คชันความเข้ากันได้**<br>กฎนี้ปิดใช้งานการเชื่อมต่อ X Window System และโปรแกรมจัดการการล็อกอิน XServer |

*ตารางที่ 4. ข้อกำหนดความเป็นเจ้าของ DoD*

| ID จุดตรวจสอบของ Department of Defense STIG | รายละเอียด | ตำแหน่งของสคริปต์ที่นิยามแอ็คชัน และผลลัพธ์ของแอ็คชันที่เปิดใช้งานความเข้ากันได้ |
|---|---|---|
| AIX00085 | ไฟล์ `/etc/netsvc.conf` ต้องเป็นเจ้าของโดย root | **ตำแหน่ง** `/etc/security/pscexpert/dodv2/chowndodfiles`<br>**แอ็คชันความเข้ากันได้**<br>ตรวจสอบให้แน่ใจว่าไฟล์ที่ระบุไว้เป็นเจ้าของโดย root |
| AIX00090 | ไฟล์ `/etc/netsvc.conf` ต้องเป็นเจ้าของแบบกลุ่มโดย bin, sys หรือระบบ | **ตำแหน่ง** `/etc/security/pscexpert/dodv2/chowndodfiles`<br>**แอ็คชันความเข้ากันได้**<br>ตรวจสอบให้แน่ใจว่า ไฟล์ที่ระบุไว้เป็นเจ้าของแบบกลุ่ม bin, sys หรือระบบ |
| AIX00320 | ไฟล์ `/etc/ftpaccess.ctl` ต้องเป็นเจ้าของโดย root | **ตำแหน่ง** `/etc/security/pscexpert/dodv2/chowndodfiles`<br>**แอ็คชันความเข้ากันได้**<br>ตรวจสอบให้แน่ใจว่าไฟล์ที่ระบุไว้เป็นเจ้าของโดย root |
| AIX00330 | ไฟล์ `/etc/ftpaccess.ctl` ต้องเป็นเจ้าของแบบกลุ่มโดย bin, sys หรือระบบ | **ตำแหน่ง** `/etc/security/pscexpert/dodv2/chowndodfiles`<br>**แอ็คชันความเข้ากันได้**<br>ตรวจสอบให้แน่ใจว่า ไฟล์ที่ระบุไว้เป็นเจ้าของแบบกลุ่ม bin, sys หรือระบบ |
| GEN000250 | ไฟล์คอนฟิกูเรชันการซิงโครไนซ์เวลา (เช่น `/etc/ntp.conf`) ต้องเป็นเจ้าของโดย root | **ตำแหน่ง** `/etc/security/pscexpert/dodv2/chowndodfiles`<br>**แอ็คชันความเข้ากันได้**<br>ตรวจสอบให้แน่ใจว่าไฟล์ที่ระบุไว้เป็นเจ้าของโดย root |

*ตารางที่ 4. ข้อกำหนดความเป็นเจ้าของ DoD (ต่อ)*

| ID จุดตรวจสอบของ Department of Defense STIG | รายละเอียด | ตำแหน่งของสคริปต์ที่นิยามแอ็คชัน และผลลัพธ์ของแอ็คชันที่เปิดใช้งานความเข้ากันได้ |
|---|---|---|
| GEN000251 | ไฟล์คอนฟิกูเรชันการซิงโครไนซ์เวลา (เช่น `/etc/ntp.conf`) ต้องเป็นเจ้าของแบบกลุ่มโดย bin, sys หรือระบบ | **ตำแหน่ง** `/etc/security/pscexpert/dodv2/chowndodfiles`<br>**แอ็คชันความเข้ากันได้**<br>ตรวจสอบให้แน่ใจว่า ไฟล์ที่ระบุไว้เป็นเจ้าของแบบกลุ่ม bin, sys หรือระบบ |
| GEN001160 | ไฟล์และไดเร็กทอรีทั้งหมดต้องมี เจ้าของที่ถูกต้อง | **ตำแหน่ง** `/etc/security/pscexpert/dodv2/chowndodfiles`<br>**แอ็คชันความเข้ากันได้**<br>ตรวจสอบให้แน่ใจว่า ไฟล์และไดเร็กทอรีทั้งหมดมีเจ้าของที่ถูกต้อง |
| GEN001170 | ไฟล์และไดเร็กทอรีทั้งหมดต้องมีเจ้าของกลุ่ม ที่ถูกต้อง | **ตำแหน่ง** `/etc/security/pscexpert/dodv2/chowndodfiles`<br>**แอ็คชันความเข้ากันได้**<br>ตรวจสอบให้แน่ใจว่า ไฟล์และไดเร็กทอรีทั้งหมดมีเจ้าของที่ถูกต้อง |
| GEN001220 | ไฟล์ของระบบ โปรแกรม และไดเร็กทอรีทั้งหมด ต้องเป็นเจ้าของโดยแอคเคาต์ระบบ | **ตำแหน่ง** `/etc/security/pscexpert/dodv2/chowndodfiles`<br>**แอ็คชันความเข้ากันได้**<br>ตรวจสอบให้แน่ใจว่า ระบบไฟล์โปรแกรม และไดเร็กทอรี เป็นเจ้าของโดยแอคเคาต์ระบบ |
| GEN001240 | ระบบไฟล์ โปแกรม และไดเร็กทอรี ต้องเป็นเจ้าของแบบกลุ่มโดยกลุ่มของระบบ | **ตำแหน่ง** `/etc/security/pscexpert/dodv2/chowndodfiles`<br>**แอ็คชันความเข้ากันได้**<br>ระบบไฟล์โปรแกรม และไดเร็กทอรีทั้งหมดต้องเป็นเจ้าของแบบกลุ่มโดย กลุ่มของระบบ |
| GEN001320 | ไฟล์ Network Information Systems (NIS)/NIS+/yp ต้องเป็นเจ้าของโดย root, sys หรือ bin | **ตำแหน่ง** `/etc/security/pscexpert/dodv2/chowndodfiles`<br>**แอ็คชันความเข้ากันได้**<br>ตรวจสอบให้แน่ใจว่า ไฟล์ที่ระบุไว้เป็นเจ้าของโดย root, sys หรือ bin |

*ตารางที่ 4. ข้อกำหนดความเป็นเจ้าของ DoD (ต่อ)*

| ID จุดตรวจสอบของ Department of Defense STIG | รายละเอียด | ตำแหน่งของสคริปต์ที่นิยามแอ็คชัน และผลลัพธ์ของแอ็คชันที่เปิดใช้งานความเข้ากันได้ |
|---|---|---|
| GEN001340 | ไฟล์ NIS/NIS+/yp ต้องเป็นเจ้าของแบบกลุ่มโดย sys, bin, other หรือระบบ | **ตำแหน่ง** `/etc/security/pscexpert/dodv2/chowndodfiles`<br>**แอ็คชันความเข้ากันได้**<br>ตรวจสอบให้แน่ใจว่า ไฟล์ที่ระบุไว้เป็นเจ้าของโดย sys, bin, other หรือระบบ |
| GEN001362 | ไฟล์ `/etc/resolv.conf` ต้องเป็นเจ้าของโดย root | **ตำแหน่ง** `/etc/security/pscexpert/dodv2/chowndodfiles`<br>**แอ็คชันความเข้ากันได้**<br>ตรวจสอบให้แน่ใจว่าไฟล์ที่ระบุไว้เป็นเจ้าของโดย root |
| GEN001363 | ไฟล์ `/etc/resolv.conf` ต้องเป็นเจ้าของแบบกลุ่มโดย bin, sys หรือระบบ | **ตำแหน่ง** `/etc/security/pscexpert/dodv2/chowndodfiles`<br>**แอ็คชันความเข้ากันได้**<br>ตรวจสอบให้แน่ใจว่า ไฟล์ที่ระบุไว้เป็นเจ้าของแบบกลุ่ม bin, sys หรือระบบ |
| GEN001366 | ไฟล์ `/etc/hosts` ต้องเป็นเจ้าของโดย root | **ตำแหน่ง** `/etc/security/pscexpert/dodv2/chowndodfiles`<br>**แอ็คชันความเข้ากันได้**<br>ตรวจสอบให้แน่ใจว่าไฟล์ที่ระบุไว้เป็นเจ้าของโดย root |
| GEN001367 | ไฟล์ `/etc/hosts` ต้องเป็นเจ้าของแบบกลุ่มโดย bin, sys หรือระบบ | **ตำแหน่ง** `/etc/security/pscexpert/dodv2/chowndodfiles`<br>**แอ็คชันความเข้ากันได้**<br>ตรวจสอบให้แน่ใจว่า ไฟล์ที่ระบุไว้เป็นเจ้าของแบบกลุ่ม bin, sys หรือระบบ |
| GEN001371 | ไฟล์ `/etc/nsswitch.conf` ต้องเป็นเจ้าของโดย root | **ตำแหน่ง** `/etc/security/pscexpert/dodv2/chowndodfiles`<br>**แอ็คชันความเข้ากันได้**<br>ตรวจสอบให้แน่ใจว่าไฟล์ที่ระบุไว้เป็นเจ้าของโดย root |
| GEN001372 | ไฟล์ `/etc/nsswitch.conf` ต้องเป็นเจ้าของแบบกลุ่มโดย root, bin, sys หรือระบบ | **ตำแหน่ง** `/etc/security/pscexpert/dodv2/chowndodfiles`<br>**แอ็คชันความเข้ากันได้**<br>ตรวจสอบให้แน่ใจว่า ไฟล์ที่ระบุไว้เป็นเจ้าของแบบกลุ่มโดย root, bin, sys หรือระบบ |

*ตารางที่ 4. ข้อกำหนดความเป็นเจ้าของ DoD (ต่อ)*

| ID จุดตรวจสอบของ Department of Defense STIG | รายละเอียด | ตำแหน่งของสคริปต์ที่นิยามแอ็คชัน และผลลัพธ์ของแอ็คชันที่เปิดใช้งานความเข้ากันได้ |
|---|---|---|
| GEN001378 | ไฟล์ /etc/passwd ต้องเป็นเจ้าของโดย root | **ตำแหน่ง** /etc/security/pscexpert/dodv2/chowndodfiles<br>**แอ็คชันความเข้ากันได้**<br>ตรวจสอบให้แน่ใจว่าไฟล์ที่ระบุไว้เป็นเจ้าของโดย root |
| GEN001379 | ไฟล์ /etc/passwd ต้องเป็นเจ้าของแบบกลุ่มโดย bin, security, sys หรือระบบ | **ตำแหน่ง** /etc/security/pscexpert/dodv2/chowndodfiles<br>**แอ็คชันความเข้ากันได้**<br>ตรวจสอบให้แน่ใจว่า ไฟล์ที่ระบุไว้เป็นเจ้าของแบบกลุ่ม โดย bin ความปลอดภัย sys หรือระบบ |
| GEN001391 | ไฟล์ /etc/group ต้องเป็นเจ้าของโดย root | **ตำแหน่ง** /etc/security/pscexpert/dodv2/chowndodfiles<br>**แอ็คชันความเข้ากันได้**<br>ตรวจสอบให้แน่ใจว่าไฟล์ที่ระบุไว้เป็นเจ้าของโดย root |
| GEN001392 | ไฟล์ /etc/group ต้องเป็นเจ้าของแบบกลุ่มโดย bin ความปลอดภัย sys หรือระบบ | **ตำแหน่ง** /etc/security/pscexpert/dodv2/chowndodfiles<br>**แอ็คชันความเข้ากันได้**<br>ตรวจสอบให้แน่ใจว่า ไฟล์ที่ระบุไว้เป็นเจ้าของแบบกลุ่ม โดย bin ความปลอดภัย sys หรือระบบ |
| GEN001400 | ไฟล์ /etc/security/passwd ต้องเป็นเจ้าของโดย root | **ตำแหน่ง** /etc/security/pscexpert/dodv2/chowndodfiles<br>**แอ็คชันความเข้ากันได้**<br>ตรวจสอบให้แน่ใจว่าไฟล์ที่ระบุไว้เป็นเจ้าของโดย root |
| GEN001410 | ไฟล์ /etc/security/passwd ต้องเป็นเจ้าของแบบกลุ่มโดย bin ความปลอดภัย sys หรือระบบ | **ตำแหน่ง** /etc/security/pscexpert/dodv2/chowndodfiles<br>**แอ็คชันความเข้ากันได้**<br>ตรวจสอบให้แน่ใจว่า ไฟล์ที่ระบุไว้เป็นเจ้าของแบบกลุ่ม โดย bin ความปลอดภัย sys หรือระบบ |
| GEN001500 | โฮมไดเร็กทอรีของผู้ใช้แบบโต้ตอบทั้งหมด ต้องเป็นเจ้าของโดยผู้ใช้ที่เกี่ยวข้อง | **ตำแหน่ง** /etc/security/pscexpert/dodv2/chowndodfiles<br>**แอ็คชันความเข้ากันได้**<br>ตรวจสอบให้แน่ใจว่า โฮมไดเร็กทอรีของผู้ใช้แบบโต้ตอบทั้งหมด ต้องเป็นเจ้าของโดยผู้ใช้ที่เกี่ยวข้อง |

*ตารางที่ 4. ข้อกำหนดความเป็นเจ้าของ DoD (ต่อ)*

| ID จุดตรวจสอบของ Department of Defense STIG | รายละเอียด | ตำแหน่งของสคริปต์ที่นิยามแอ็คชัน และผลลัพธ์ของแอ็คชันที่เปิดใช้งานความเข้ากันได้ |
|---|---|---|
| GEN001520 | โฮมไดเร็กทอรีของผู้ใช้แบบโต้ตอบต้องเป็นเจ้าของแบบกลุ่ม โดยกลุ่มหลักของเจ้าของโฮมไดเร็กทอรี | **ตำแหน่ง** `/etc/security/pscexpert/dodv2/chowndodfiles`<br>**แอ็คชันความเข้ากันได้**<br>ตรวจสอบให้แน่ใจว่า โฮมไดเร็กทอรีของผู้ใช้แบบโต้ตอบต้องเป็นเจ้าของกลุ่มแบบกลุ่ม โดยกลุ่มหลักของเจ้าของโฮมไดเร็กทอรี |
| GEN001540 | ไฟล์และไดเร็กทอรีทั้งหมดที่มีอยู่ในโฮมไดเร็กทอรีของผู้ใช้แบบโต้ตอบต้องเป็นเจ้าของโดยเจ้าของของ โฮมไดเร็กทอรี | **ตำแหน่ง** `/etc/security/pscexpert/dodv2/chowndodfiles`<br>**แอ็คชันความเข้ากันได้**<br>ตรวจสอบให้แน่ใจว่า ไฟล์และไดเร็กทอรีทั้งหมดที่มีอยู่ใน ไดเร็กทอรีโฮมของผู้ใช้แบบโต้ตอบเป็นเจ้าของโดยเจ้าของ โฮมไดเร็กทอรี |
| GEN001550 | ไฟล์และไดเร็กทอรีทั้งหมดที่มีใน โฮมไดเร็กทอรีของผู้ใช้ต้องเป็นเจ้าของแบบกลุ่มโดยกลุ่มที่ เจ้าของโฮมไดเร็กทอรีเป็นสมาชิก | **ตำแหน่ง** `/etc/security/pscexpert/dodv2/chowndodfiles`<br>**แอ็คชันความเข้ากันได้**<br>ตรวจสอบให้แน่ใจว่า ไฟล์และไดเร็กทอรีทั้งหมดมีอยู่ในโฮมไดเร็กทอรีของผู้ใช้ ต้องเป็นเจ้าของแบบกลุ่มโดยกลุ่มที่เป็นเจ้าของโฮมไดเร็กทอรี เป็นสมาชิก |
| GEN001660 | ระบบทั้งหมดที่เริ่มต้นไฟล์ต้องเป็นเจ้าของโดย root | **ตำแหน่ง** `/etc/security/pscexpert/dodv2/chowndodfiles`<br>**แอ็คชันความเข้ากันได้**<br>ตรวจสอบให้แน่ใจว่า ไฟล์ที่ระบุไว้ซึ่งเป็นเจ้าของโดย root |
| GEN001680 | ระบบทั้งหมดที่เริ่มต้นไฟล์ต้องเป็นเจ้าของแบบกลุ่มโดย sys, bin, other หรือระบบ | **ตำแหน่ง** `/etc/security/pscexpert/dodv2/chowndodfiles`<br>**แอ็คชันความเข้ากันได้**<br>ตรวจสอบให้แน่ใจว่า ไฟล์ที่ระบุไว้เป็นเจ้าของแบบกลุ่มโดย sys, bin, other หรือระบบ |
| GEN001740 | ไฟล์เริ่มต้นทำงานแบบโกลบอลทั้งหมดต้องเป็นเจ้าของโดย root | **ตำแหน่ง** `/etc/security/pscexpert/dodv2/chowndodfiles`<br>**แอ็คชันความเข้ากันได้**<br>ตรวจสอบให้แน่ใจว่า ไฟล์ที่ระบุไว้ซึ่งเป็นเจ้าของโดย root |

*ตารางที่ 4. ข้อกำหนดความเป็นเจ้าของ DoD (ต่อ)*

| ID จุดตรวจสอบของ Department of Defense STIG | รายละเอียด | ตำแหน่งของสคริปต์ที่นิยามแอ็คชัน และผลลัพธ์ของแอ็คชันที่เปิดใช้งานความเข้ากันได้ |
|---|---|---|
| GEN001760 | ไฟล์เริ่มต้นทำงานแบบโกลบอลทั้งหมดต้องเป็นเจ้าของแบบกลุ่มโดย sys, bin, ระบบ หรือความปลอดภัย | **ตำแหน่ง** `/etc/security/pscexpert/dodv2/chowndodfiles`<br>**แอ็คชันความเข้ากันได้**<br>ตรวจสอบให้แน่ใจว่า ไฟล์ที่ระบุไว้เป็นเจ้าของแบบกลุ่มโดย sys, bin, ระบบ หรือความปลอดภัย |
| GEN001820 | ไฟล์และไดเร็กทอรี skeleton ทั้งหมด (โดยทั่วไปแล้ว ใน `/etc/skel`) ต้องเป็นเจ้าของโดย root หรือ bin | **ตำแหน่ง** `/etc/security/pscexpert/dodv2/chowndodfiles`<br>**แอ็คชันความเข้ากันได้**<br>ตรวจสอบให้แน่ใจว่า ไฟล์และไดเร็กทอรีที่ระบุเป็นเจ้าของโดย root หรือ bin |
| GEN001830 | ไฟล์ skeleton ทั้งหมด (โดยทั่วไปแล้ว ใน `/etc/skel`) ต้องเป็นเจ้าของแบบกลุ่มโดยความปลอดภัย | **ตำแหน่ง** `/etc/security/pscexpert/dodv2/chowndodfiles`<br>**แอ็คชันความเข้ากันได้**<br>ตรวจสอบให้แน่ใจว่า ไฟล์ที่ระบุไว้เป็นเจ้าของแบบกลุ่มโดยความปลอดภัย |
| GEN001860 | ไฟล์เริ่มต้นทำงานแบบโกลบอลทั้งหมดต้องเป็นเจ้าของโดย ผู้ใช้หรือ root | **ตำแหน่ง** `/etc/security/pscexpert/dodv2/chowndodfiles`<br>**แอ็คชันความเข้ากันได้**<br>ตรวจสอบให้แน่ใจว่า ไฟล์ที่ระบุไว้เป็นเจ้าของโดยผู้ใช้หรือ root |
| GEN001870 | ไฟล์เริ่มต้นทำงานแบบโลคัลต้องเป็นเจ้าของแบบกลุ่มโดย กลุ่มหลักของผู้ใช้หรือ root | **ตำแหน่ง** `/etc/security/pscexpert/dodv2/chowndodfiles`<br>**แอ็คชันความเข้ากันได้**<br>ตรวจสอบให้แน่ใจว่า ไฟล์เริ่มต้นทำงานโลคัลต้องเป็นเจ้าของกลุ่มโดย กลุ่มหลักของผู้ใช้หรือ root |
| GEN002060 | ไฟล์ `.rhosts`, `.shosts`, `.netrc` หรือ `hosts.equiv` ทั้งหมดต้องสามารถเข้าถึงได้โดย root หรือเจ้าของ | **ตำแหน่ง** `/etc/security/pscexpert/dodv2/chowndodfiles`<br>`/etc/security/pscexpert/dodv2/fpmdodfiles`<br>**แอ็คชันความเข้ากันได้**<br>ตรวจสอบให้แน่ใจว่า root หรือเจ้าของสามารถเข้าถึงไฟล์ ที่ระบุ |

*ตารางที่ 4. ข้อกำหนดความเป็นเจ้าของ DoD (ต่อ)*

| ID จุดตรวจสอบของ Department of Defense STIG | รายละเอียด | ตำแหน่งของสคริปต์ที่นิยามแอ็คชัน และผลลัพธ์ของแอ็คชันที่เปิดใช้งานความเข้ากันได้ |
|---|---|---|
| GEN002100 | ไฟล์ .rhosts ต้องไม่สนับสนุนโดย Pluggable Authentication Module (PAM) | **ตำแหน่ง** /etc/security/pscexpert/dodv2/chowndodfiles<br>**แอ็คชันความเข้ากันได้**<br>ตรวจสอบให้แน่ใจว่า ไฟล์ที่ระบุไว้ไม่พร้อมใช้งานโดยใช้ PAM |
| GEN002200 | ไฟล์เชลล์ทั้งหมดต้องเป็นเจ้าของ root หรือ bin | **ตำแหน่ง** /etc/security/pscexpert/dodv2/chowndodfiles<br>**แอ็คชันความเข้ากันได้**<br>ตรวจสอบให้แน่ใจว่า ไฟล์ที่ระบุไว้เป็นเจ้าของ root หรือ bin |
| GEN002210 | ไฟล์เชลล์ทั้งหมดต้องเป็นเจ้าของแบบกลุ่มโดย root, bin, sys หรือระบบ | **ตำแหน่ง** /etc/security/pscexpert/dodv2/chowndodfiles<br>**แอ็คชันความเข้ากันได้**<br>ตรวจสอบให้แน่ใจ ไฟล์ที่ระบุไว้เป็นเจ้าของแบบกลุ่มโดย root, bin, sys หรือระบบ |
| GEN002340 | อุปกรณ์ออดิโอต้องเป็นเจ้าของโดย root | **ตำแหน่ง** /etc/security/pscexpert/dodv2/chowndodfiles<br>**แอ็คชันความเข้ากันได้**<br>ตรวจสอบให้แน่ใจว่า อุปกรณ์ออดิโอทั้งหมดเป็นเจ้าของโดย root |
| GEN002360 | อุปกรณ์ออดิโอต้องเป็นเจ้าของแบบกลุ่มโดย root, sys, bin หรือระบบ | **ตำแหน่ง** /etc/security/pscexpert/dodv2/chowndodfiles<br>**แอ็คชันความเข้ากันได้**<br>ตรวจสอบให้แน่ใจว่า อุปกรณ์ออดิโอทั้งหมดเป็นเจ้าของแบบกลุ่มโดย root, sys, bin หรือระบบ |
| GEN002520 | ไดเร็กทอรีพับลิกทั้งหมดต้องเป็นเจ้าของโดย root หรือแอคเคาต์แอ็พพลิเคชัน | **ตำแหน่ง** /etc/security/pscexpert/dodv2/chowndodfiles<br>**แอ็คชันความเข้ากันได้**<br>ตรวจสอบให้แน่ใจว่า ไดเร็กทอรีพับลิกทั้งหมดเป็นเจ้าของโดย root หรือแอคเคาต์ แอ็พพลิเคชัน |

*ตารางที่ 4. ข้อกำหนดความเป็นเจ้าของ DoD (ต่อ)*

| ID จุดตรวจสอบของ Department of Defense STIG | รายละเอียด | ตำแหน่งของสคริปต์ที่นิยามแอ็คชัน และผลลัพธ์ของแอ็คชันที่เปิดใช้งานความเข้ากันได้ |
|---|---|---|
| GEN002540 | ไดเร็กทอรีพับลิกทั้งหมดต้องเป็นเจ้าของแบบกลุ่มโดยระบบ หรือกลุ่มแอ็พพลิเคชัน | **ตำแหน่ง** `/etc/security/pscexpert/dodv2/chowndodfiles`<br>**แอ็คชันความเข้ากันได้**<br>ตรวจสอบให้แน่ใจว่า ไดเร็กทอรีพับลิกทั้งหมดเป็นเจ้าของแบบกลุ่มโดยระบบ หรือกลุ่มแอ็พพลิเคชัน |
| GEN002680 | การทำบันทึกระบบตรวจสอบต้องเป็นเจ้าของโดย root | **ตำแหน่ง** `/etc/security/pscexpert/dodv2/chowndodfiles`<br>**แอ็คชันความเข้ากันได้**<br>ตรวจสอบให้แน่ใจว่า ไฟล์ที่ระบุไว้ซึ่งเป็นเจ้าของโดย root |
| GEN002690 | การทำบันทึกระบบตรวจสอบต้องเป็นเจ้าของแบบกลุ่มโดย bin, sys หรือระบบ | **ตำแหน่ง** `/etc/security/pscexpert/dodv2/chowndodfiles`<br>**แอ็คชันความเข้ากันได้**<br>ตรวจสอบให้แน่ใจว่า ไฟล์ที่ระบุไว้เป็นเจ้าของแบบกลุ่มโดย bin, sys หรือระบบ |
| GEN003020 | `Cron` ต้องไม่รันโปรแกรม หรือ ส่วนขยาย ของไดเร็กทอรีที่สามารถเขียนได้ | **ตำแหน่ง** `/etc/security/pscexpert/dodv2/chowndodfiles`<br>**แอ็คชันความเข้ากันได้**<br>ปกป้อง `cron` จากการรันโปรแกรม หรือส่วนขยายไดเร็กทอรีที่สามารถเขียนได้ |
| GEN003040 | `Crontabs` ต้องเป็นเจ้าของโดย root หรือผู้สร้าง crontab | **ตำแหน่ง** `/etc/security/pscexpert/dodv2/chowndodfiles`<br>**แอ็คชันความเข้ากันได้**<br>ตรวจสอบให้แน่ใจว่า crontabs เป็นเจ้าของโดย root หรือโดยผู้สร้าง crontab |
| GEN003050 | ไฟล์ `Crontab` ต้องเป็นเจ้าของแบบกลุ่มโดยระบบ, cron หรือกลุ่มหลักของผู้สร้าง crontab | **ตำแหน่ง** `/etc/security/pscexpert/dodv2/chowndodfiles`<br>**แอ็คชันความเข้ากันได้**<br>ตรวจสอบให้แน่ใจว่า ไฟล์ `crontab` เป็นเจ้าของแบบกลุ่มโดยระบบ system, cron หรือกลุ่มหลักของผู้สร้าง crontab |

*ตารางที่ 4. ข้อกำหนดความเป็นเจ้าของ DoD (ต่อ)*

| ID จุดตรวจสอบของ Department of Defense STIG | รายละเอียด | ตำแหน่งของสคริปต์ที่นิยามแอ็คชัน และผลลัพธ์ของแอ็คชันที่เปิดใช้งานความเข้ากันได้ |
|---|---|---|
| GEN003110 | ไดเร็กทอรี Cron และ crontab ต้องไม่มีรายการควบคุมสิทธิ์ที่ขยายเพิ่ม | **ตำแหน่ง** /etc/security/pscexpert/dodv2/chowndodfiles<br>**แอ็คชันความเข้ากันได้**<br>ตรวจสอบให้แน่ใจว่า ไดเร็กทอรีที่ระบุไว้ ต้องไม่มีรายการควบคุมสิทธิ์ที่ขยายเพิ่ม |
| GEN003120 | ไดเร็กทอรี Cron และ crontab ต้องเป็นเจ้าของโดย root หรือ bin | **ตำแหน่ง** /etc/security/pscexpert/dodv2/chowndodfiles<br>**แอ็คชันความเข้ากันได้**<br>ตรวจสอบให้แน่ใจว่า ไดเร็กทอรี cron และ crontab เป็นเจ้าของโดย root หรือ bin |
| GEN003140 | ไดเร็กทอรี Cron และ crontab ต้องเป็นเจ้าของแบบกลุ่มโดยระบบ, sys, bin หรือ cron | **ตำแหน่ง** /etc/security/pscexpert/dodv2/chowndodfiles<br>**แอ็คชันความเข้ากันได้**<br>ตรวจสอบให้แน่ใจว่า ไดเร็กทอรีที่ระบุไว้เป็นเจ้าของแบบกลุ่มโดยระบบ, sys, bin หรือ cron |
| GEN003160 | การทำบันทึก Cron ต้องถูกนำมาใช้ | **ตำแหน่ง** /etc/security/pscexpert/dodv2/chowndodfiles<br>**แอ็คชันความเข้ากันได้**<br>ตรวจสอบให้แน่ใจว่า การทำบันทึก cron ถูกนำมาใช้ |
| GEN003240 | ไฟล์ cron.allow ต้องเป็นเจ้าของโดย root, bin หรือ sys | **ตำแหน่ง** /etc/security/pscexpert/dodv2/chowndodfiles<br>**แอ็คชันความเข้ากันได้**<br>ตรวจสอบให้แน่ใจว่า ไฟล์ที่ระบุไว้เป็นเจ้าของโดย root, bin หรือ sys |
| GEN003250 | ไฟล์ cron.allow ต้องเป็นเจ้าของแบบกลุ่มโดยระบบ, bin, sys หรือ cron | **ตำแหน่ง** /etc/security/pscexpert/dodv2/chowndodfiles<br>**แอ็คชันความเข้ากันได้**<br>ตรวจสอบให้แน่ใจว่า ไฟล์ที่ระบุไว้เป็นเจ้าของแบบกลุ่มโดยระบบ, bin, sys หรือ cron |
| GEN003260 | ไฟล์ cron.deny ต้องเป็นเจ้าโดย root, bin หรือ sys | **ตำแหน่ง** /etc/security/pscexpert/dodv2/chowndodfiles<br>**แอ็คชันความเข้ากันได้**<br>ตรวจสอบให้แน่ใจว่า ไฟล์ที่ระบุไว้เป็นเจ้าของโดย root, bin หรือ sys |

*ตารางที่ 4. ข้อกำหนดความเป็นเจ้าของ DoD (ต่อ)*

| ID จุดตรวจสอบของ Department of Defense STIG | รายละเอียด | ตำแหน่งของสคริปต์ที่นิยามแอ็คชัน และผลลัพธ์ของแอ็คชันที่เปิดใช้งานความเข้ากันได้ |
|---|---|---|
| GEN003270 | ไฟล์ `cron.deny` ต้องเป็นเจ้าของแบบกลุ่มโดยระบบ, bin, sys หรือ cron | **ตำแหน่ง** `/etc/security/pscexpert/dodv2/chowndodfiles`<br>**แอ็คชันความเข้ากันได้**<br>ตรวจสอบให้แน่ใจว่า ไฟล์ที่ระบุไว้เป็นเจ้าของแบบกลุ่มโดยระบบ, bin, sys หรือ cron |
| GEN003420 | ไดเร็กทอรี `at` ต้องเป็นเจ้าของโดย root, bin, sys, daemon หรือ cron | **ตำแหน่ง** `/etc/security/pscexpert/dodv2/chowndodfiles`<br>**แอ็คชันความเข้ากันได้**<br>ตรวจสอบให้แน่ใจว่า ไดเร็กทอรีที่ระบุไว้เป็นเจ้าของโดย root, sys, daemon หรือ cron |
| GEN003430 | ไดเร็กทอรี `at` ต้องเป็นเจ้าของแบบกลุ่มโดยระบบ, bin, sys หรือ cron | **ตำแหน่ง** `/etc/security/pscexpert/dodv2/chowndodfiles`<br>**แอ็คชันความเข้ากันได้**<br>ตรวจสอบให้แน่ใจว่า ไดเร็กทอรีที่ระบุไว้เป็นเจ้าของแบบกลุ่มโดยระบบ, bin, sys หรือ cron |
| GEN003460 | ไฟล์ `at.allow` ต้องเป็นเจ้าของโดย root, bin หรือ sys | **ตำแหน่ง** `/etc/security/pscexpert/dodv2/chowndodfiles`<br>**แอ็คชันความเข้ากันได้**<br>ตรวจสอบให้แน่ใจว่า ไฟล์ที่ระบุไว้เป็นเจ้าของโดย root, bin หรือ sys |
| GEN003470 | ไฟล์ `at.allow` ต้องเป็นเจ้าของแบบกลุ่มโดยระบบ bin, sys หรือ cron | **ตำแหน่ง** `/etc/security/pscexpert/dodv2/chowndodfiles`<br>**แอ็คชันความเข้ากันได้**<br>ตรวจสอบให้แน่ใจว่า ไฟล์ที่ระบุไว้เป็นเจ้าของแบบกลุ่มโดยระบบ, bin, sys หรือ cron |
| GEN003480 | ไฟล์ `at.deny` ต้องเป็นเจ้าของโดย root, bin หรือ sys | **ตำแหน่ง** `/etc/security/pscexpert/dodv2/chowndodfiles`<br>**แอ็คชันความเข้ากันได้**<br>ตรวจสอบให้แน่ใจว่า ไฟล์ที่ระบุไว้เป็นเจ้าของโดย root, bin หรือ sys |

*ตารางที่ 4. ข้อกำหนดความเป็นเจ้าของ DoD (ต่อ)*

| ID จุดตรวจสอบของ Department of Defense STIG | รายละเอียด | ตำแหน่งของสคริปต์ที่นิยามแอ็คชัน และผลลัพธ์ของแอ็คชันที่เปิดใช้งานความเข้ากันได้ |
|---|---|---|
| GEN003490 | ไฟล์ `at.deny` ต้องเป็นเจ้าของแบบกลุ่มโดยระบบ bin, sys หรือ cron | **ตำแหน่ง** `/etc/security/pscexpert/dodv2/chowndodfiles`<br>**แอ็คชันความเข้ากันได้** ตรวจสอบให้แน่ใจว่า ไฟล์ที่ระบุไว้เป็นเจ้าของแบบกลุ่มโดยระบบ, bin, sys หรือ cron |
| GEN003720 | ไฟล์ `inetd.conf` ไฟล์ `xinetd.conf` และไดเร็กทอรี `xinetd.d` ต้องเป็นเจ้าของโดย root หรือ bin | **ตำแหน่ง** `/etc/security/pscexpert/dodv2/chowndodfiles`<br>**แอ็คชันความเข้ากันได้** ตรวจสอบว่า ไฟล์และไดเร็กทอรีที่ระบุไว้เป็นเจ้าของโดย root หรือ bin |
| GEN003730 | ไฟล์ `inetd.conf` ไฟล์ `xinetd.conf` และไดเร็กทอรี `xinetd.d` ต้องเป็นเจ้าของแบบกลุ่มโดย bin, sys หรือระบบ | **ตำแหน่ง** `/etc/security/pscexpert/dodv2/chowndodfiles`<br>**แอ็คชันความเข้ากันได้** ตรวจสอบให้แน่ใจว่า ไฟล์และไดเร็กทอรีที่ระบุไว้เป็นเจ้าของแบบกลุ่มโดย bin, sys หรือระบบ |
| GEN003760 | ไฟล์ `services` ต้องเป็นเจ้าของโดย root หรือ bin | **ตำแหน่ง** `/etc/security/pscexpert/dodv2/chowndodfiles`<br>**แอ็คชันความเข้ากันได้** ตรวจสอบให้แน่ใจว่า ไฟล์ที่ระบุไว้เป็นเจ้าของโดย root หรือ bin |
| GEN003770 | ไฟล์ `services` ต้องเป็น เจ้าของแบบกลุ่มโดย bin, sys หรือระบบ | **ตำแหน่ง** `/etc/security/pscexpert/dodv2/chowndodfiles`<br>**แอ็คชันความเข้ากันได้** ตรวจสอบให้แน่ใจว่า ไฟล์ที่ระบุไว้เป็นเจ้าของแบบกลุ่ม bin, sys หรือระบบ |
| GEN003920 | ไฟล์ `hosts.lpd` (หรือเทียบเท่า) ต้องเป็นเจ้าของโดย root, bin, sys หรือ lp | **ตำแหน่ง** `/etc/security/pscexpert/dodv2/chowndodfiles`<br>**แอ็คชันความเข้ากันได้** ตรวจสอบให้แน่ใจว่า ไฟล์ที่ระบุไว้เป็นเจ้าของโดย root, bin, sys หรือ lp |

*ตารางที่ 4. ข้อกำหนดความเป็นเจ้าของ DoD (ต่อ)*

| ID จุดตรวจสอบของ Department of Defense STIG | รายละเอียด | ตำแหน่งของสคริปต์ที่นิยามแอ็คชัน และผลลัพธ์ของแอ็คชันที่เปิดใช้งานความเข้ากันได้ |
|---|---|---|
| GEN003930 | ไฟล์ `hosts.lpd` (หรือเทียบเท่า) ต้องเป็นเจ้าของโดย bin, sys หรือระบบ | **ตำแหน่ง** `/etc/security/pscexpert/dodv2/chowndodfiles`<br>**แอ็คชันความเข้ากันได้** ตรวจสอบให้แน่ใจว่า ไฟล์ที่ระบุไว้เป็นเจ้าของแบบกลุ่ม bin, sys หรือระบบ |
| GEN003960 | เจ้าของคำสั่ง **traceroute** ต้องเป็น root | **ตำแหน่ง** `/etc/security/pscexpert/dodv2/chowndodfiles`<br>**แอ็คชันความเข้ากันได้** ตรวจสอบให้แน่ใจว่า เจ้าของคำสั่งเป็น root |
| GEN003980 | คำสั่ง **traceroute** ต้องเป็นเจ้าของแบบกลุ่ม โดย sys, bin หรือระบบ | **ตำแหน่ง** `/etc/security/pscexpert/dodv2/chowndodfiles`<br>**แอ็คชันความเข้ากันได้** ตรวจสอบให้แน่ใจว่า คำสั่งเป็นเจ้าของแบบกลุ่มโดย sys, bin หรือระบบ |
| GEN004360 | ไฟล์ `alias` ต้องเป็นเจ้าของโดย root | **ตำแหน่ง** `/etc/security/pscexpert/dodv2/chowndodfiles`<br>**แอ็คชันความเข้ากันได้** ตรวจสอบให้แน่ใจว่าไฟล์ที่ระบุไว้เป็นเจ้าของโดย root |
| GEN004370 | ไฟล์ `aliases` ต้องเป็นเจ้าของแบบกลุ่มโดย sys, bin หรือระบบ | **ตำแหน่ง** `/etc/security/pscexpert/dodv2/chowndodfiles`<br>**แอ็คชันความเข้ากันได้** ตรวจสอบให้แน่ใจว่า ไฟล์ที่ระบุไว้เป็นเจ้าของกลุ่มโดย sys, bin หรือระบบ |
| GEN004400 | ไฟล์ที่รันผ่านไฟล์ `aliases` ต้องเป็นเจ้าของโดย root และต้องอยู่ภายในไดเร็กทอรีที่เป็นเจ้าของ และสามารถเขียนได้โดย root เท่านั้น | **ตำแหน่ง** `/etc/security/pscexpert/dodv2/chowndodfiles`<br>**แอ็คชันความเข้ากันได้** ตรวจสอบให้แน่ใจว่า ไฟล์ต่างๆ ถูกรันผ่านไฟล์เมล `aliases` เป็นเจ้าของโดย root และต้องอยู่ภายในไดเร็กทอรีที่เป็นเจ้าของ และสามารถเขียนได้โดย root เท่านั้น |

*ตารางที่ 4. ข้อกำหนดความเป็นเจ้าของ DoD (ต่อ)*

| ID จุดตรวจสอบของ Department of Defense STIG | รายละเอียด | ตำแหน่งของสคริปต์ที่นิยามแอ็คชัน และผลลัพธ์ของแอ็คชันที่เปิดใช้งานความเข้ากันได้ |
|---|---|---|
| GEN004410 | ไฟล์ที่รันผ่านไฟล์ `aliases` ต้องเป็นเจ้าของกลุ่มโดย root, bin, sys หรืออื่นๆ ไฟล์เหล่านั้นต้องอยู่ภายในไดเร็กทอรีที่เป็นเจ้าของแบบกลุ่มโดย root, bin, sys หรืออื่นๆ | **ตำแหน่ง** `/etc/security/pscexpert/dodv2/chowndodfiles`<br>**แอ็คชันความเข้ากันได้**<br>ตรวจสอบให้แน่ใจว่า ไฟล์ที่รันผ่านไฟล์เมล `aliases` ต้องเป็นเจ้าของแบบกลุ่มโดย root, bin, sys หรืออื่นๆ และอยู่ภายในไดเร็กทอรี ที่เป็นเจ้าของแบบกลุ่มตาม root, bin, sys หรืออื่นๆ |
| GEN004480 | ไฟล์การทำบันทึกเซอร์วิส SMTP ต้องเป็นของโดย root | **ตำแหน่ง** `/etc/security/pscexpert/dodv2/chowndodfiles`<br>**แอ็คชันความเข้ากันได้**<br>ตรวจสอบให้แน่ใจว่าไฟล์ที่ระบุไว้เป็นเจ้าของโดย root |
| GEN004920 | ไฟล์ `ftpusers` ต้องเป็นเจ้าของโดย root | **ตำแหน่ง** `/etc/security/pscexpert/dodv2/chowndodfiles`<br>**แอ็คชันความเข้ากันได้**<br>ตรวจสอบให้แน่ใจว่าไฟล์ที่ระบุไว้เป็นเจ้าของโดย root |
| GEN004930 | ไฟล์ `ftpusers` ต้องเป็นเจ้าของแบบกลุ่มตาม bin, sys หรือระบบ | **ตำแหน่ง** `/etc/security/pscexpert/dodv2/chowndodfiles`<br>**แอ็คชันความเข้ากันได้**<br>ตรวจสอบให้แน่ใจว่า ไฟล์ที่ระบุไว้เป็นเจ้าของแบบกลุ่ม bin, sys หรือระบบ |
| GEN005360 | ไฟล์ `snmpd.conf` ต้องเป็นเจ้าของโดย root | **ตำแหน่ง** `/etc/security/pscexpert/dodv2/chowndodfiles`<br>**แอ็คชันความเข้ากันได้**<br>ตรวจสอบให้แน่ใจว่าไฟล์ที่ระบุไว้เป็นเจ้าของโดย root |
| GEN005365 | ไฟล์ `snmpd.conf` ต้องเป็นเจ้าของแบบกลุ่มโดย bin, sys หรือระบบ | **ตำแหน่ง** `/etc/security/pscexpert/dodv2/chowndodfiles`<br>**แอ็คชันความเข้ากันได้**<br>ตรวจสอบให้แน่ใจว่า ไฟล์ที่ระบุไว้เป็นเจ้าของแบบกลุ่ม bin, sys หรือระบบ |
| GEN005400 | ไฟล์ `/etc/syslog.conf` ต้องเป็นเจ้าของโดย root | **ตำแหน่ง** `/etc/security/pscexpert/dodv2/chowndodfiles`<br>**แอ็คชันความเข้ากันได้**<br>ตรวจสอบให้แน่ใจว่าไฟล์ที่ระบุไว้เป็นเจ้าของโดย root |

*ตารางที่ 4. ข้อกำหนดความเป็นเจ้าของ DoD (ต่อ)*

| ID จุดตรวจสอบของ Department of Defense STIG | รายละเอียด | ตำแหน่งของสคริปต์ที่นิยามแอ็คชัน และผลลัพธ์ของแอ็คชันที่เปิดใช้งานความเข้ากันได้ |
|---|---|---|
| GEN005420 | ไฟล์ /etc/syslog.conf ต้องเป็นเจ้าของแบบกลุ่มโดย bin, sys หรือระบบ | **ตำแหน่ง** /etc/security/pscexpert/dodv2/chowndodfiles<br>**แอ็คชันความเข้ากันได้**<br>ตรวจสอบให้แน่ใจว่า ไฟล์ที่ระบุไว้เป็นเจ้าของแบบกลุ่ม bin, sys หรือระบบ |
| GEN005610 | ระบบต้องไม่มีการส่งต่อ IP สำหรับ IPv6 ที่เปิดใช้งาน ยกเว้นว่าระบบเป็นเราเตอร์ IPv6 | **ตำแหน่ง** /etc/security/pscexpert/dodv2/chowndodfiles<br>**แอ็คชันความเข้ากันได้**<br>ตรวจสอบให้แน่ใจว่า การส่งต่อ IP สำหรับ IPv6 ต้องไม่เปิดใช้งาน ยกเว้นว่า ระบบต้องถูกใช้เป็นเราเตอร์ IPv6 |
| GEN005740 | ไฟล์คอนฟิกูเรชันเอ็กซ์พอร์ต NFS ต้องเป็นเจ้าของโดย root | **ตำแหน่ง** /etc/security/pscexpert/dodv2/chowndodfiles<br>**แอ็คชันความเข้ากันได้**<br>ตรวจสอบให้แน่ใจว่าไฟล์ที่ระบุไว้เป็นเจ้าของโดย root |
| GEN005750 | ไฟล์คอนฟิกูเรชันเอ็กซ์พอร์ต NFS ต้องเป็นเจ้าของแบบกลุ่มโดย root, bin, sys หรือระบบ | **ตำแหน่ง** /etc/security/pscexpert/dodv2/chowndodfiles<br>**แอ็คชันความเข้ากันได้**<br>ตรวจสอบให้แน่ใจว่า ไฟล์ที่ระบุไว้เป็นเจ้าของแบบกลุ่มโดย root, bin, sys หรือระบบ |
| GEN005800 | ไฟล์ระบบที่เอ็กซ์พอร์ต NFS ทั้งหมดและไดเร็กทอรีระบบ ต้องเป็นเจ้าของโดย root | **ตำแหน่ง** /etc/security/pscexpert/dodv2/chowndodfiles<br>**แอ็คชันความเข้ากันได้**<br>ตรวจสอบให้แน่ใจว่าไฟล์ที่ระบุไว้เป็นเจ้าของโดย root |
| GEN005810 | ไฟล์ระบบที่เอ็กซ์พอร์ต NFS ทั้งหมดและไดเร็กทอรีที่ระบบ ต้องเป็นเจ้าของแบบกลุ่มโดย root, bin, sys หรือระบบ | **ตำแหน่ง** /etc/security/pscexpert/dodv2/chowndodfiles<br>**แอ็คชันความเข้ากันได้**<br>ตรวจสอบให้แน่ใจว่า ไฟล์และไดเร็กทอรีที่ระบุไว้เป็นเจ้าของแบบกลุ่มโดย root, bin, sys หรือระบบ |
| GEN006100 | ไฟล์ /usr/lib/smb.conf ต้องเป็นเจ้าของโดย root | **ตำแหน่ง** /etc/security/pscexpert/dodv2/chowndodfiles<br>**แอ็คชันความเข้ากันได้**<br>ตรวจสอบให้แน่ใจว่าไฟล์ที่ระบุไว้เป็นเจ้าของโดย root |

*ตารางที่ 4. ข้อกำหนดความเป็นเจ้าของ DoD (ต่อ)*

| ID จุดตรวจสอบของ Department of Defense STIG | รายละเอียด | ตำแหน่งของสคริปต์ที่นิยามแอ็คชัน และผลลัพธ์ของแอ็คชันที่เปิดใช้งานความเข้ากันได้ |
|---|---|---|
| GEN006120 | ไฟล์ /usr/lib/smb.conf ต้องเป็นเจ้าของแบบกลุ่มโดย bin, sys หรือระบบ | **ตำแหน่ง** /etc/security/pscexpert/dodv2/chowndodfiles<br>**แอ็คชันความเข้ากันได้** ตรวจสอบให้แน่ใจว่า ไฟล์ที่ระบุไว้เป็นเจ้าของแบบกลุ่ม bin, sys หรือระบบ |
| GEN006160 | ไฟล์ /var/private/smbpasswd ต้องเจ้าของโดย root | **ตำแหน่ง** /etc/security/pscexpert/dodv2/chowndodfiles<br>**แอ็คชันความเข้ากันได้** ตรวจสอบให้แน่ใจว่าไฟล์ที่ระบุไว้เป็นเจ้าของโดย root |
| GEN006180 | ไฟล์ /var/private/smbpasswd ต้องเป็นเจ้าของแบบกลุ่มโดย sys หรือระบบ | **ตำแหน่ง** /etc/security/pscexpert/dodv2/chowndodfiles<br>**แอ็คชันความเข้ากันได้** ตรวจสอบให้แน่ใจว่า ไฟล์ที่ระบุไว้เป็นเจ้าของแบบกลุ่มโดย sys หรือระบบ |
| GEN006340 | ไฟล์ในไดเร็กทอรี /etc/news ต้องเป็นเจ้าของโดย root หรือข่าวสาร | **ตำแหน่ง** /etc/security/pscexpert/dodv2/chowndodfiles<br>**แอ็คชันความเข้ากันได้** ตรวจสอบให้แน่ใจว่า ไดเร็กทอรีที่ระบุไว้เป็นเจ้าของโดย root หรือข่าวสาร |
| GEN006360 | ไฟล์ใน /etc/news ต้องเป็นเจ้าของแบบกลุ่มโดยระบบหรือข่าวสาร | **ตำแหน่ง** /etc/security/pscexpert/dodv2/chowndodfiles<br>**แอ็คชันความเข้ากันได้** ตรวจสอบให้แน่ใจว่า ไฟล์ที่ระบุไว้เป็นเจ้าของแบบกลุ่มโดยระบบหรือ ข่าวสาร |
| GEN008080 | ถ้าระบบกำลังใช้ LDAP สำหรับการพิสูจน์ตัวตน หรือข้อมูลแอคเคาต์ไฟล์ /etc/ldap.conf (หรือ เทียบเท่า) ต้องเป็นเจ้าของโดย root | **ตำแหน่ง** /etc/security/pscexpert/dodv2/chowndodfiles<br>**แอ็คชันความเข้ากันได้** ตรวจสอบให้แน่ใจว่าไฟล์ที่ระบุไว้เป็นเจ้าของโดย root |
| GEN008100 | ถ้าระบบกำลังใช้ LDAP สำหรับการพิสูจน์ตัวตน หรือข้อมูลแอคเคาต์ไฟล์ /etc/ldap.conf (หรือ เทียบเท่า) ต้องเป็นเจ้าของแบบกลุ่มโดยความปลอดภัย, bin, sys หรือระบบ | **ตำแหน่ง** /etc/security/pscexpert/dodv2/chowndodfiles<br>**แอ็คชันความเข้ากันได้** ตรวจสอบให้แน่ใจว่า ไฟล์ที่ระบุไว้เป็นเจ้าของแบบกลุ่ม bin, sys หรือระบบ |

*ตารางที่ 4. ข้อกำหนดความเป็นเจ้าของ DoD (ต่อ)*

| ID จุดตรวจสอบของ Department of Defense STIG | รายละเอียด | ตำแหน่งของสคริปต์ที่นิยามแอ็คชัน และผลลัพธ์ของแอ็คชันที่เปิดใช้งานความเข้ากันได้ |
|---|---|---|
| GEN008140 | ถ้าระบบกำลังใช้ LDAP สำหรับการพิสูจน์ตัวตน หรือข้อมูลแอคเคาต์ ไฟล์หรือไดเร็กทอรีการออกใบรับรอง TLS ต้องเป็นเจ้าของโดย root | **ตำแหน่ง** `/etc/security/pscexpert/dodv2/chowndodfiles`<br>**แอ็คชันความเข้ากันได้**<br>ตรวจสอบให้แน่ใจว่าไฟล์ที่ระบุไว้เป็นเจ้าของโดย root |
| GEN008160 | ถ้าระบบกำลังใช้ LDAP สำหรับการพิสูจน์ตัวตน หรือข้อมูลแอคเคาต์ ไฟล์การออกใบรับรอง TLS หรือไดเร็กทอรี ต้องเป็นเจ้าของแบบกลุ่มโดย root, bin, sys หรือระบบ | **ตำแหน่ง** `/etc/security/pscexpert/dodv2/chowndodfiles`<br>**แอ็คชันความเข้ากันได้**<br>ตรวจสอบให้แน่ใจว่า ไฟล์ที่ระบุไว้เป็นเจ้าของแบบกลุ่ม bin, sys หรือระบบ |

*ตารางที่ 5. DoD มาตรฐานสำหรับการให้สิทธิ์ไฟล์*

| ID จุดตรวจสอบของ Department of Defense STIG | รายละเอียด | ตำแหน่งของสคริปต์ที่นิยามแอ็คชัน และผลลัพธ์ของแอ็คชันที่เปิดใช้งานความเข้ากันได้ |
|---|---|---|
| AIX00100 | ไฟล์ `/etc/netsvc.conf` ต้องมีโหมด 0644 หรือโหมดที่ได้รับสิทธิ์น้อย | **ตำแหน่ง** `/etc/security/pscexpert/dodv2/fpmdodfiles`<br>**แอ็คชันความเข้ากันได้**<br>ตรวจสอบให้แน่ใจว่า ไฟล์ที่ถูกตั้งค่าเป็นโหมดการให้สิทธิ์ที่ระบุไว้ หรือเป็นค่าที่ได้รับสิทธิ์น้อย |
| AIX00340 | ไฟล์ `/etc/ftpaccess.ctl` ต้องมีโหมด 0640 หรือโหมดที่ได้รับสิทธิ์น้อย | **ตำแหน่ง** `/etc/security/pscexpert/dodv2/fpmdodfiles`<br>**แอ็คชันความเข้ากันได้**<br>ตรวจสอบให้แน่ใจว่า ไฟล์ที่ถูกตั้งค่าเป็นโหมดการให้สิทธิ์ที่ระบุไว้ หรือเป็นค่าที่ได้รับสิทธิ์น้อย |
| GEN000252 | ไฟล์คอนฟิกูเรชันการซิงโครไนซ์เวลา (เช่น `/etc/ntp.conf`) ต้องมีโหมด 0640 หรือโหมดที่ได้รับสิทธิ์น้อย | **ตำแหน่ง** `/etc/security/pscexpert/dodv2/fpmdodfiles`<br>**แอ็คชันความเข้ากันได้**<br>ตรวจสอบให้แน่ใจว่า ไฟล์ที่ถูกตั้งค่าเป็นโหมดการให้สิทธิ์ที่ระบุไว้ หรือเป็นค่าที่ได้รับสิทธิ์น้อย |
| GEN000920 | โฮมไดเร็กทอรีของแอคเคาต์ root (นอกเหนือจาก `/`) ต้องมีโหมด 0700 | **ตำแหน่ง** `/etc/security/pscexpert/dodv2/fpmdodfiles`<br>**แอ็คชันความเข้ากันได้**<br>ตรวจสอบให้แน่ใจว่า ไดเร็กทอรีถูกตั้งค่าเป็นโหมดการให้สิทธิ์ที่ระบุไว้ หรือเป็นค่าที่ได้รับสิทธิ์น้อย |

*ตารางที่ 5. DoD มาตรฐานสำหรับการให้สิทธิ์ไฟล์ (ต่อ)*

| ID จุดตรวจสอบของ Department of Defense STIG | รายละเอียด | ตำแหน่งของสคริปต์ที่นิยามแอ็คชัน และผลลัพธ์ของแอ็คชันที่เปิดใช้งานความเข้ากันได้ |
|---|---|---|
| GEN001140 | ไฟล์และไดเร็กทอรีระบบต้องไม่มี การให้สิทธิ์เข้าถึง | **ตำแหน่ง** `/etc/security/pscexpert/dodv2/fpmdodfiles`<br>**แอ็คชันความเข้ากันได้**<br>ตรวจสอบให้แน่ใจว่า การให้สิทธิ์เข้าถึงสอดคล้องกัน |
| GEN001180 | ไฟล์ daemon เซอร์วิสเครือข่ายทั้งหมดต้องมีโหมด 0755 หรือโหมดที่ได้รับสิทธิ์น้อย | **ตำแหน่ง** `/etc/security/pscexpert/dodv2/fpmdodfiles`<br>**แอ็คชันความเข้ากันได้**<br>ตรวจสอบให้แน่ใจว่า ไฟล์ถูกตั้งค่าโหมดการให้สิทธิ์ที่ระบุไว้ หรือเป็นค่าที่ได้รับสิทธิ์น้อย |
| GEN001200 | ไฟล์คำสั่งของระบบทั้งหมดต้องมีโหมด 0755 หรือโหมดที่ได้รับสิทธิ์น้อย | **ตำแหน่ง** `/etc/security/pscexpert/dodv2/fpmdodfiles`<br>**แอ็คชันความเข้ากันได้**<br>ตรวจสอบให้แน่ใจว่า ไฟล์ถูกตั้งค่าโหมดการให้สิทธิ์ที่ระบุไว้ หรือเป็นค่าที่ได้รับสิทธิ์น้อย |
| GEN001260 | ไฟล์การบันทึกของระบบต้องมีโหมด 0640 หรือโหมด ที่ได้รับสิทธิ์น้อย | **ตำแหน่ง** `/etc/security/pscexpert/dodv2/fpmdodfiles`<br>**แอ็คชันความเข้ากันได้**<br>ตรวจสอบให้แน่ใจว่า ไฟล์ถูกตั้งค่าโหมดการให้สิทธิ์ที่ระบุไว้ หรือเป็นค่าที่ได้รับสิทธิ์น้อย |
| GEN001280 | ไฟล์เพจแบบแมนวลต้องมีโหมด 0644 หรือโหมด ที่ได้รับสิทธิ์น้อย | **ตำแหน่ง** `/etc/security/pscexpert/dodv2/fpmdodfiles`<br>**แอ็คชันความเข้ากันได้**<br>ตรวจสอบให้แน่ใจว่า ไฟล์ถูกตั้งค่าโหมดการให้สิทธิ์ที่ระบุไว้ หรือเป็นค่าที่ได้รับสิทธิ์น้อย |
| GEN001300 | ไฟล์ไลบรารีต้องมีโหมด 0755 หรือโหมด ที่ได้รับสิทธิ์น้อย | **ตำแหน่ง** `/etc/security/pscexpert/dodv2/fpmdodfiles`<br>**แอ็คชันความเข้ากันได้**<br>ตรวจสอบให้แน่ใจว่า ไฟล์ถูกตั้งค่าโหมดการให้สิทธิ์ที่ระบุไว้ หรือเป็นค่าที่ได้รับสิทธิ์น้อย |

*ตารางที่ 5. DoD มาตรฐานสำหรับการให้สิทธิ์ไฟล์ (ต่อ)*

| ID จุดตรวจสอบของ Department of Defense STIG | รายละเอียด | ตำแหน่งของสคริปต์ที่นิยามแอ็คชัน และผลลัพธ์ของแอ็คชันที่เปิดใช้งานความเข้ากันได้ |
|---|---|---|
| GEN001360 | ไฟล์ NIS/NIS+/yp ต้องมีโหมด 0755 หรือโหมดที่ได้รับสิทธิ์น้อย | **ตำแหน่ง** `/etc/security/pscexpert/dodv2/fpmdodfiles`<br>**แอ็คชันความเข้ากันได้**<br>ตรวจสอบให้แน่ใจว่า ไฟล์ถูกตั้งค่าโหมดการให้สิทธิ์ที่ระบุไว้ หรือเป็นค่าที่ได้รับสิทธิ์น้อย |
| GEN001364 | ไฟล์ `/etc/resolv.conf` ต้องมีโหมด 0644 หรือโหมดที่ได้รับสิทธิ์น้อย | **ตำแหน่ง** `/etc/security/pscexpert/dodv2/fpmdodfiles`<br>**แอ็คชันความเข้ากันได้**<br>ตรวจสอบให้แน่ใจว่า ไฟล์ที่ถูกตั้งค่าเป็นโหมดการให้สิทธิ์ที่ระบุไว้ หรือเป็นค่าที่ได้รับสิทธิ์น้อย |
| GEN001368 | ไฟล์ `/etc/hosts` ต้องมีโหมด 0644 หรือโหมดที่ได้รับสิทธิ์น้อย | **ตำแหน่ง** `/etc/security/pscexpert/dodv2/fpmdodfiles`<br>**แอ็คชันความเข้ากันได้**<br>ตรวจสอบให้แน่ใจว่า ไฟล์ที่ถูกตั้งค่าเป็นโหมดการให้สิทธิ์ที่ระบุไว้ หรือเป็นค่าที่ได้รับสิทธิ์น้อย |
| GEN001373 | ไฟล์ `/etc/nsswitch.conf` ต้องมีโหมด 0644 หรือโหมดที่ได้รับสิทธิ์น้อย | **ตำแหน่ง** `/etc/security/pscexpert/dodv2/fpmdodfiles`<br>**แอ็คชันความเข้ากันได้**<br>ตรวจสอบให้แน่ใจว่า ไฟล์ที่ถูกตั้งค่าเป็นโหมดการให้สิทธิ์ที่ระบุไว้ หรือเป็นค่าที่ได้รับสิทธิ์น้อย |
| GEN001380 | ไฟล์ `/etc/passwd` ต้องมีโหมด 0644 หรือโหมดที่ได้รับสิทธิ์น้อย | **ตำแหน่ง** `/etc/security/pscexpert/dodv2/fpmdodfiles`<br>**แอ็คชันความเข้ากันได้**<br>ตรวจสอบให้แน่ใจว่า ไฟล์ที่ถูกตั้งค่าเป็นโหมดการให้สิทธิ์ที่ระบุไว้ หรือเป็นค่าที่ได้รับสิทธิ์น้อย |
| GEN001393 | ไฟล์ `/etc/group` ต้องมีโหมด 0644 หรือโหมดที่ได้รับสิทธิ์น้อย | **ตำแหน่ง** `/etc/security/pscexpert/dodv2/fpmdodfiles`<br>**แอ็คชันความเข้ากันได้**<br>ตรวจสอบให้แน่ใจว่า ไฟล์ที่ถูกตั้งค่าเป็นโหมดการให้สิทธิ์ที่ระบุไว้ หรือเป็นค่าที่ได้รับสิทธิ์น้อย |

*ตารางที่ 5. DoD มาตรฐานสำหรับการให้สิทธิ์ไฟล์ (ต่อ)*

| ID จุดตรวจสอบของ Department of Defense STIG | รายละเอียด | ตำแหน่งของสคริปต์ที่นิยามแอ็คชัน และผลลัพธ์ของแอ็คชันที่เปิดใช้งานความเข้ากันได้ |
|---|---|---|
| GEN001420 | ไฟล์ /etc/security/passwd ต้องมีโหมด 0400 | **ตำแหน่ง** /etc/security/pscexpert/dodv2/fpmdodfiles<br>**แอ็คชันความเข้ากันได้**<br>ตรวจสอบให้แน่ใจว่า ไฟล์ที่ถูกตั้งค่าเป็นโหมดการให้สิทธิ์ที่ระบุไว้ หรือเป็นค่าที่ได้รับสิทธิ์น้อย |
| GEN001480 | โฮมไดเร็กทอรีของผู้ใช้ทั้งหมดต้องมีโหมด 0750 หรือได้รับสิทธิ์น้อย | **ตำแหน่ง** /etc/security/pscexpert/dodv2/fpmdodfiles<br>**แอ็คชันความเข้ากันได้**<br>ตรวจสอบให้แน่ใจว่า ไฟล์ที่ถูกตั้งค่าเป็นโหมดการให้สิทธิ์ที่ระบุไว้ หรือเป็นค่าที่ได้รับสิทธิ์น้อย |
| GEN001560 | ไฟล์และไดเร็กทอรีทั้งหมดที่มีอยู่ในโฮมไดเร็กทอรีของผู้ใช้ต้องมีโหมด 0750 หรือโหมดที่มีการให้สิทธิ์ น้อย | **ตำแหน่ง** /etc/security/pscexpert/dodv2/fpmdodfiles<br>**แอ็คชันความเข้ากันได้**<br>ตรวจสอบให้แน่ใจว่า ไฟล์ถูกตั้งค่าโหมดการให้สิทธิ์ที่ระบุไว้ หรือเป็นค่าที่ได้รับสิทธิ์น้อย |
| GEN001580 | สคริปต์การควบคุมการรันทั้งหมดต้องมีโหมด 0755 หรือโหมดที่ได้รับสิทธิ์น้อย | **ตำแหน่ง** /etc/security/pscexpert/dodv2/fpmdodfiles<br>**แอ็คชันความเข้ากันได้**<br>ตรวจสอบให้แน่ใจว่า ไฟล์ถูกตั้งค่าโหมดการให้สิทธิ์ที่ระบุไว้ หรือเป็นค่าที่ได้รับสิทธิ์น้อย |
| GEN001640 | การรันสคริปต์การควบคุมต้องไม่รันโปรแกรมหรือสคริปต์ที่สามารถเขียนได้ | **ตำแหน่ง** /etc/security/pscexpert/dodv2/fpmdodfiles<br>**แอ็คชันความเข้ากันได้**<br>ตรวจสอบโปรแกรม เช่น cron สำหรับโปรแกรมหรือสคริปต์ ที่สามารถเขียนได้ |
| GEN001720 | ไฟล์การเริ่มต้นทำงานแบบโกลบอลทั้งหมดต้องมีโหมด 0644 หรือโหมดที่ได้รับสิทธิ์น้อย | **ตำแหน่ง** /etc/security/pscexpert/dodv2/fpmdodfiles<br>**แอ็คชันความเข้ากันได้**<br>ตรวจสอบให้แน่ใจว่า ไฟล์ถูกตั้งค่าโหมดการให้สิทธิ์ที่ระบุไว้ หรือเป็นค่าที่ได้รับสิทธิ์น้อย |

*ตารางที่ 5. DoD มาตรฐานสำหรับการให้สิทธิ์ไฟล์ (ต่อ)*

| ID จุดตรวจสอบของ Department of Defense STIG | รายละเอียด | ตำแหน่งของสคริปต์ที่นิยามแอ็คชัน และผลลัพธ์ของแอ็คชันที่เปิดใช้งานความเข้ากันได้ |
|---|---|---|
| GEN001800 | ไฟล์ skeleton ทั้งหมด (ตัวอย่างเช่น ไฟล์ใน `/etc/skel`) ต้องมีโหมด 0644 หรือโหมดที่ได้รับสิทธิ์น้อย | **ตำแหน่ง** `/etc/security/pscexpert/dodv2/fpmdodfiles`<br>**แอ็คชันความเข้ากันได้**<br>ตรวจสอบให้แน่ใจว่า ไฟล์ถูกตั้งค่าโหมดการให้สิทธิ์ที่ระบุไว้ หรือเป็นค่าที่ได้รับสิทธิ์น้อย |
| GEN001880 | ไฟล์การเริ่มต้นทำงานแบบโลคัลทั้งหมดต้องมีโหมด 0740 หรือโหมดที่ได้รับสิทธิ์น้อย | **ตำแหน่ง** `/etc/security/pscexpert/dodv2/fpmdodfiles`<br>**แอ็คชันความเข้ากันได้**<br>ตรวจสอบให้แน่ใจว่า ไฟล์ถูกตั้งค่าโหมดการให้สิทธิ์ที่ระบุไว้ หรือเป็นค่าที่ได้รับสิทธิ์น้อย |
| GEN002220 | ไฟล์เชลล์ทั้งหมดต้องมีโหมด 0755 หรือโหมด ที่ได้รับสิทธิ์น้อย | **ตำแหน่ง** `/etc/security/pscexpert/dodv2/fpmdodfiles`<br>**แอ็คชันความเข้ากันได้**<br>ตรวจสอบให้แน่ใจว่า ไฟล์ถูกตั้งค่าโหมดการให้สิทธิ์ที่ระบุไว้ หรือเป็นค่าที่ได้รับสิทธิ์น้อย |
| GEN002320 | อุปกรณ์ออดิโอต้องมีโหมด 0660 หรือโหมด ที่ได้รับสิทธิ์น้อย | **ตำแหน่ง** `/etc/security/pscexpert/dodv2/fpmdodfiles`<br>**แอ็คชันความเข้ากันได้**<br>ตรวจสอบให้แน่ใจว่า อุปกรณ์ออดิโอถูกตั้งค่าเป็นโหมดการให้สิทธิ์ ที่ระบุเฉพาะ หรือเป็นค่าที่ได้สิทธิ์น้อย |
| GEN002560 | ดีฟอลต์ของระบบและดีฟอลต์ของผู้ใช้ `umask` ต้องเป็น 077 | **ตำแหน่ง** `/etc/security/pscexpert/dodv2/fpmdodfiles`<br>**แอ็คชันความเข้ากันได้**<br>ตรวจสอบให้แน่ใจว่า ค่าติดตั้งที่ระบุไว้เป็น *077* |
| GEN002700 | ไฟล์การบันทึกของระบบต้องมีโหมด 0640 หรือโหมด ที่ได้รับสิทธิ์น้อย | **ตำแหน่ง** `/etc/security/pscexpert/dodv2/fpmdodfiles`<br>**แอ็คชันความเข้ากันได้**<br>ตรวจสอบให้แน่ใจว่า ไฟล์ถูกตั้งค่าโหมดการให้สิทธิ์ที่ระบุไว้ หรือเป็นค่าที่ได้รับสิทธิ์น้อย |

*ตารางที่ 5. DoD มาตรฐานสำหรับการให้สิทธิ์ไฟล์ (ต่อ)*

| ID จุดตรวจสอบของ Department of Defense STIG | รายละเอียด | ตำแหน่งของสคริปต์ที่นิยามแอ็คชัน และผลลัพธ์ของแอ็คชันที่เปิดใช้งานความเข้ากันได้ |
|---|---|---|
| GEN002717 | ไฟล์ที่สามารถเรียกทำงานกับเครื่องมือการตรวจสอบระบบต้องมีโหมด 0750 หรือโหมดที่ได้รับสิทธิ์น้อย | **ตำแหน่ง** `/etc/security/pscexpert/dodv2/fpmdodfiles`<br>**แอ็คชันความเข้ากันได้**<br>ตรวจสอบให้แน่ใจว่า ไฟล์ถูกตั้งค่าโหมดการให้สิทธิ์ที่ระบุไว้ หรือเป็นค่าที่ได้รับสิทธิ์น้อย |
| GEN002980 | ไฟล์ `cron.allow` ต้องมีโหมด 0600 หรือโหมดที่ได้รับสิทธิ์น้อย | **ตำแหน่ง** `/etc/security/pscexpert/dodv2/fpmdodfiles`<br>**แอ็คชันความเข้ากันได้**<br>ตรวจสอบให้แน่ใจว่า ไฟล์ที่ถูกตั้งค่าเป็นโหมดการให้สิทธิ์ที่ระบุไว้ หรือเป็นค่าที่ได้รับสิทธิ์น้อย |
| GEN003080 | ไฟล์ Crontab ต้องมีโหมด 0600 หรือโหมด ที่ได้รับสิทธิ์น้อย | **ตำแหน่ง** `/etc/security/pscexpert/dodv2/fpmdodfiles`<br>**แอ็คชันความเข้ากันได้**<br>ตรวจสอบให้แน่ใจว่า ไฟล์ถูกตั้งค่าโหมดการให้สิทธิ์ที่ระบุไว้ หรือเป็นค่าที่ได้รับสิทธิ์น้อย |
| GEN003090 | ไฟล์ `Crontab` ต้องไม่ access control lists (ACLs) ที่ขยายเพิ่ม | **ตำแหน่ง** `/etc/security/pscexpert/dodv2/fpmdodfiles`<br>**แอ็คชันความเข้ากันได้**<br>ตรวจสอบให้แน่ใจว่า ไฟล์ที่ระบุไว้ไม่มี ACLs. ที่ระบุ |
| GEN003100 | ไดเร็กทอรี Cron และ crontab ต้องมีโหมด 0755 หรือโหมดที่ได้รับสิทธิ์น้อย | **ตำแหน่ง** `/etc/security/pscexpert/dodv2/fpmdodfiles`<br>**แอ็คชันความเข้ากันได้**<br>ตรวจสอบให้แน่ใจว่า ไดเร็กทอรีที่ระบุเฉพาะถูกตั้งค่าเป็นโหมดการให้สิทธิ์ที่ระบุไว้ หรือเป็นค่าที่ได้รับสิทธิ์น้อย |
| GEN003180 | ไฟล์ `cronlog` ต้องมีโหมด 0600 หรือโหมดที่ได้รับสิทธิ์น้อย | **ตำแหน่ง** `/etc/security/pscexpert/dodv2/fpmdodfiles`<br>**แอ็คชันความเข้ากันได้**<br>ตรวจสอบให้แน่ใจว่า ไฟล์ที่ถูกตั้งค่าเป็นโหมดการให้สิทธิ์ที่ระบุไว้ หรือเป็นค่าที่ได้รับสิทธิ์น้อย |

*ตารางที่ 5. DoD มาตรฐานสำหรับการให้สิทธิ์ไฟล์ (ต่อ)*

| ID จุดตรวจสอบของ Department of Defense STIG | รายละเอียด | ตำแหน่งของสคริปต์ที่นิยามแอ็คชัน และผลลัพธ์ของแอ็คชันที่เปิดใช้งานความเข้ากันได้ |
|---|---|---|
| GEN003200 | ไฟล์ `cron.deny` ต้องมีโหมด 0600 หรือโหมดที่ได้รับสิทธิ์น้อย | **ตำแหน่ง** `/etc/security/pscexpert/dodv2/fpmdodfiles`<br>**แอ็คชันความเข้ากันได้**<br>ตรวจสอบให้แน่ใจว่า ไฟล์ที่ถูกตั้งค่าเป็นโหมดการให้สิทธิ์ที่ระบุไว้ หรือเป็นค่าที่ได้รับสิทธิ์น้อย |
| GEN003252 | ไฟล์ `at.deny` ต้องมีโหมด 0640 หรือโหมดที่ได้รับสิทธิ์น้อย | **ตำแหน่ง** `/etc/security/pscexpert/dodv2/fpmdodfiles`<br>**แอ็คชันความเข้ากันได้**<br>ตรวจสอบให้แน่ใจว่า ไฟล์ที่ถูกตั้งค่าเป็นโหมดการให้สิทธิ์ที่ระบุไว้ หรือเป็นค่าที่ได้รับสิทธิ์น้อย |
| GEN003340 | ไฟล์ `at.allow` ต้องมีโหมด 0600 หรือโหมดที่ได้รับสิทธิ์น้อย | **ตำแหน่ง** `/etc/security/pscexpert/dodv2/fpmdodfiles`<br>**แอ็คชันความเข้ากันได้**<br>ตรวจสอบให้แน่ใจว่า ไฟล์ที่ถูกตั้งค่าเป็นโหมดการให้สิทธิ์ที่ระบุไว้ หรือเป็นค่าที่ได้รับสิทธิ์น้อย |
| GEN003400 | ไดเร็กทอรี `at` ต้องมีโหมด 0755 หรือโหมดที่ได้รับสิทธิ์น้อย | **ตำแหน่ง** `/etc/security/pscexpert/dodv2/fpmdodfiles`<br>**แอ็คชันความเข้ากันได้**<br>ตรวจสอบให้แน่ใจว่า ไดเร็กทอรีถูกตั้งค่าเป็นโหมดการให้สิทธิ์ที่ระบุไว้ หรือเป็นค่าที่ได้รับสิทธิ์น้อย |
| GEN003440 | งาน `At` ต้องไม่ตั้งค่าพารามิเตอร์ `umask` เป็นค่าที่น้อยกว่า 077 | **ตำแหน่ง** `/etc/security/pscexpert/dodv2/fpmdodfiles`<br>**แอ็คชันความเข้ากันได้**<br>ตรวจสอบให้แน่ใจว่า พารามิเตอร์ถูกตั้งค่าเป็นโหมดการให้สิทธิ์ที่ระบุไว้ หรือเป็นค่าที่ได้รับสิทธิ์น้อย |
| GEN003740 | ไฟล์ `inetd.conf` และ `xinetd.conf` ต้องมีโหมด 0440 หรือโหมดที่ได้รับสิทธิ์น้อย | **ตำแหน่ง** `/etc/security/pscexpert/dodv2/fpmdodfiles`<br>**แอ็คชันความเข้ากันได้**<br>ตรวจสอบให้แน่ใจว่า ไฟล์ถูกตั้งค่าโหมดการให้สิทธิ์ที่ระบุไว้ หรือเป็นค่าที่ได้รับสิทธิ์น้อย |

*ตารางที่ 5. DoD มาตรฐานสำหรับการให้สิทธิ์ไฟล์ (ต่อ)*

| ID จุดตรวจสอบของ Department of Defense STIG | รายละเอียด | ตำแหน่งของสคริปต์ที่นิยามแอ็คชัน และผลลัพธ์ของแอ็คชันที่เปิดใช้งานความเข้ากันได้ |
|---|---|---|
| GEN003780 | ไฟล์ services ต้องมีโหมด 0444 หรือโหมดที่ได้รับสิทธิ์น้อย | **ตำแหน่ง** /etc/security/pscexpert/dodv2/fpmdodfiles<br>**แอ็คชันความเข้ากันได้**<br>ตรวจสอบให้แน่ใจว่า ไฟล์ที่ถูกตั้งค่าเป็นโหมดการให้สิทธิ์ที่ระบุไว้ หรือเป็นค่าที่ได้รับสิทธิ์น้อย |
| GEN003940 | ไฟล์ hosts.lpd (หรือ เทียบเท่า) ต้องมีโหมด 0644 หรือโหมดที่ได้รับสิทธิ์น้อย | **ตำแหน่ง** /etc/security/pscexpert/dodv2/fpmdodfiles<br>**แอ็คชันความเข้ากันได้**<br>ตรวจสอบให้แน่ใจว่า ไฟล์ที่ถูกตั้งค่าเป็นโหมดการให้สิทธิ์ที่ระบุไว้ หรือเป็นค่าที่ได้รับสิทธิ์น้อย |
| GEN004000 | ไฟล์ traceroute ต้องมีโหมด 0700 หรือโหมดที่ได้รับสิทธิ์น้อย | **ตำแหน่ง** /etc/security/pscexpert/dodv2/fpmdodfiles<br>**แอ็คชันความเข้ากันได้**<br>ตรวจสอบให้แน่ใจว่า ไฟล์ที่ถูกตั้งค่าเป็นโหมดการให้สิทธิ์ที่ระบุไว้ หรือเป็นค่าที่ได้รับสิทธิ์น้อย |
| GEN004380 | ไฟล์ alias ต้องมีโหมด 0644 หรือโหมดที่ได้รับสิทธิ์น้อย | **ตำแหน่ง** /etc/security/pscexpert/dodv2/fpmdodfiles<br>**แอ็คชันความเข้ากันได้**<br>ตรวจสอบให้แน่ใจว่า ไฟล์ที่ถูกตั้งค่าเป็นโหมดการให้สิทธิ์ที่ระบุไว้ หรือเป็นค่าที่ได้รับสิทธิ์น้อย |
| GEN004420 | ไฟล์ที่รันผ่านไฟล์เมล aliases ต้องมีโหมด 0755 หรือโหมดที่ได้รับสิทธิ์น้อย | **ตำแหน่ง** /etc/security/pscexpert/dodv2/fpmdodfiles<br>**แอ็คชันความเข้ากันได้**<br>ตรวจสอบให้แน่ใจว่า ไฟล์ถูกตั้งค่าโหมดการให้สิทธิ์ที่ระบุไว้ หรือเป็นค่าที่ได้รับสิทธิ์น้อย |
| GEN004500 | ไฟล์การทำบันทึกเซอร์วิส SMTP ต้องมีโหมด 0644 หรือโหมดที่ได้รับสิทธิ์น้อย | **ตำแหน่ง** /etc/security/pscexpert/dodv2/fpmdodfiles<br>**แอ็คชันความเข้ากันได้**<br>ตรวจสอบให้แน่ใจว่า ไฟล์ที่ถูกตั้งค่าเป็นโหมดการให้สิทธิ์ที่ระบุไว้ หรือเป็นค่าที่ได้รับสิทธิ์น้อย |

*ตารางที่ 5. DoD มาตรฐานสำหรับการให้สิทธิ์ไฟล์ (ต่อ)*

| ID จุดตรวจสอบของ Department of Defense STIG | รายละเอียด | ตำแหน่งของสคริปต์ที่นิยามแอ็คชัน และผลลัพธ์ของแอ็คชันที่เปิดใช้งานความเข้ากันได้ |
|---|---|---|
| GEN004940 | ไฟล์ `ftpusers` ต้องมีโหมด 0640 หรือโหมดที่ได้รับสิทธิ์น้อย | **ตำแหน่ง** `/etc/security/pscexpert/dodv2/fpmdodfiles`<br>**แอ็คชันความเข้ากันได้**<br>ตรวจสอบให้แน่ใจว่า ไฟล์ที่ถูกตั้งค่าเป็นโหมดการให้สิทธิ์ที่ระบุไว้ หรือเป็นค่าที่ได้รับสิทธิ์น้อย |
| GEN005040 | ผู้ใช้ FTP ทั้งหมดต้องมีค่าติดตั้งดีฟอลต์ `umask` เป็น 077 | **ตำแหน่ง** `/etc/security/pscexpert/dodv2/fpmdodfiles`<br>**แอ็คชันความเข้ากันได้**<br>ตรวจสอบให้แน่ใจว่า ค่าติดตั้งเป็นค่าที่ถูกต้อง |
| GEN005100 | `TFTP` daemon ต้องมีโหมด 0755 หรือโหมดที่ได้รับสิทธิ์น้อย | **ตำแหน่ง** `/etc/security/pscexpert/dodv2/fpmdodfiles`<br>**แอ็คชันความเข้ากันได้**<br>ตรวจสอบให้แน่ใจว่า daemon ถูกตั้งค่าโหมดที่ระบุไว้ หรือเป็นค่า ที่ได้รับสิทธิ์น้อย |
| GEN005180 | ไฟล์ `.Xauthority` ต้องมีโหมด 0600 หรือโหมดที่ได้รับสิทธิ์น้อย | **ตำแหน่ง** `/etc/security/pscexpert/dodv2/fpmdodfiles`<br>**แอ็คชันความเข้ากันได้**<br>ตรวจสอบให้แน่ใจว่า ไฟล์ถูกตั้งค่าโหมดการให้สิทธิ์ที่ระบุไว้ หรือเป็นค่าที่ได้รับสิทธิ์น้อย |
| GEN005320 | ไฟล์ `snmpd.conf` ต้องมีโหมด 0600 หรือโหมดที่ได้รับสิทธิ์น้อย | **ตำแหน่ง** `/etc/security/pscexpert/dodv2/fpmdodfiles`<br>**แอ็คชันความเข้ากันได้**<br>ตรวจสอบให้แน่ใจว่า ไฟล์ที่ถูกตั้งค่าเป็นโหมดการให้สิทธิ์ที่ระบุไว้ หรือเป็นค่าที่ได้รับสิทธิ์น้อย |
| GEN005340 | ไฟล์ Management Information Base (MIB) ต้องมีโหมด 0640 หรือโหมดที่ได้รับสิทธิ์น้อย | **ตำแหน่ง** `/etc/security/pscexpert/dodv2/fpmdodfiles`<br>**แอ็คชันความเข้ากันได้**<br>ตรวจสอบให้แน่ใจว่า ไฟล์ถูกตั้งค่าโหมดการให้สิทธิ์ที่ระบุไว้ หรือเป็นค่าที่ได้รับสิทธิ์น้อย |
| GEN005390 | ไฟล์ `/etc/syslog.conf` ต้องมีโหมด 0640 หรือโหมดที่ได้รับสิทธิ์น้อย | **ตำแหน่ง** `/etc/security/pscexpert/dodv2/fpmdodfiles`<br>**แอ็คชันความเข้ากันได้**<br>ตรวจสอบให้แน่ใจว่า ไฟล์ที่ถูกตั้งค่าเป็นโหมดการให้สิทธิ์ที่ระบุไว้ หรือเป็นค่าที่ได้รับสิทธิ์น้อย |

*ตารางที่ 5. DoD มาตรฐานสำหรับการให้สิทธิ์ไฟล์ (ต่อ)*

| ID จุดตรวจสอบของ Department of Defense STIG | รายละเอียด | ตำแหน่งของสคริปต์ที่นิยามแอ็คชัน และผลลัพธ์ของแอ็คชันที่เปิดใช้งานความเข้ากันได้ |
|---|---|---|
| GEN005522 | ไฟล์ฮ็อตคีย์พับลิก SSH ต้องมีโหมด 0644 หรือโหมดที่ได้รับสิทธิ์น้อย | **ตำแหน่ง** `/etc/security/pscexpert/dodv2/fpmdodfiles`<br>**แอ็คชันความเข้ากันได้**<br>ตรวจสอบให้แน่ใจว่า ไฟล์ถูกตั้งค่าโหมดการให้สิทธิ์ที่ระบุไว้ หรือเป็นค่าที่ได้รับสิทธิ์น้อย |
| GEN005523 | ไฟล์ฮ็อตคีย์ไพรเวต SSH ต้องมีโหมด 0600 หรือโหมดที่ได้รับสิทธิ์น้อย | **ตำแหน่ง** `/etc/security/pscexpert/dodv2/fpmdodfiles`<br>**แอ็คชันความเข้ากันได้**<br>ตรวจสอบให้แน่ใจว่า ไฟล์ถูกตั้งค่าโหมดการให้สิทธิ์ที่ระบุไว้ หรือเป็นค่าที่ได้รับสิทธิ์น้อย |
| GEN006140 | ไฟล์ `/usr/lib/smb.conf` ต้องมีโหมด 0644 หรือโหมดที่ได้รับสิทธิ์น้อย | **ตำแหน่ง** `/etc/security/pscexpert/dodv2/fpmdodfiles`<br>**แอ็คชันความเข้ากันได้**<br>ตรวจสอบให้แน่ใจว่า ไฟล์ที่ถูกตั้งค่าเป็นโหมดการให้สิทธิ์ที่ระบุไว้ หรือเป็นค่าที่ได้รับสิทธิ์น้อย |
| GEN006200 | ไฟล์ `/var/private/smbpasswd` ต้องมีโหมด 0600 หรือโหมดที่ได้รับสิทธิ์น้อย | **ตำแหน่ง** `/etc/security/pscexpert/dodv2/fpmdodfiles`<br>**แอ็คชันความเข้ากันได้**<br>ตรวจสอบให้แน่ใจว่า ไฟล์ที่ถูกตั้งค่าเป็นโหมดการให้สิทธิ์ที่ระบุไว้ หรือเป็นค่าที่ได้รับสิทธิ์น้อย |
| GEN006260 | ไฟล์ `/etc/news/hosts.nntp` (หรือเทียบเท่า) ต้องมีโหมด 0600 หรือโหมดที่ได้รับสิทธิ์น้อย | **ตำแหน่ง** `/etc/security/pscexpert/dodv2/fpmdodfiles`<br>**แอ็คชันความเข้ากันได้**<br>ตรวจสอบให้แน่ใจว่า ไฟล์ที่ถูกตั้งค่าเป็นโหมดการให้สิทธิ์ที่ระบุไว้ หรือเป็นค่าที่ได้รับสิทธิ์น้อย |
| GEN006280 | ไฟล์ `/etc/news/hosts.nntp.nolimit` (หรือเทียบเท่า) ต้องมีโหมด 0600 หรือโหมดที่ได้รับสิทธิ์น้อย | **ตำแหน่ง** `/etc/security/pscexpert/dodv2/fpmdodfiles`<br>**แอ็คชันความเข้ากันได้**<br>ตรวจสอบให้แน่ใจว่า ไฟล์ที่ถูกตั้งค่าเป็นโหมดการให้สิทธิ์ที่ระบุไว้ หรือเป็นค่าที่ได้รับสิทธิ์น้อย |

*ตารางที่ 5. DoD มาตรฐานสำหรับการให้สิทธิ์ไฟล์ (ต่อ)*

| ID จุดตรวจสอบของ Department of Defense STIG | รายละเอียด | ตำแหน่งของสคริปต์ที่นิยามแอ็คชัน และผลลัพธ์ของแอ็คชันที่เปิดใช้งานความเข้ากันได้ |
|---|---|---|
| GEN006300 | ไฟล์ /etc/news/nnrp.access (หรือเทียบเท่า) ต้องมีโหมด 0600 หรือโหมดที่ได้รับสิทธิ์น้อย | **ตำแหน่ง** /etc/security/pscexpert/dodv2/fpmdodfiles<br>**แอ็คชันความเข้ากันได้**<br>ตรวจสอบให้แน่ใจว่า ไฟล์ที่ถูกตั้งค่าเป็นโหมดการให้สิทธิ์ที่ระบุไว้ หรือเป็นค่าที่ได้รับสิทธิ์น้อย |
| GEN006320 | ไฟล์ /etc/news/passwd.nntp (หรือเทียบเท่า) ต้องมีโหมด 0600 หรือโหมดที่ได้รับสิทธิ์น้อย | **ตำแหน่ง** /etc/security/pscexpert/dodv2/fpmdodfiles<br>**แอ็คชันความเข้ากันได้**<br>ตรวจสอบให้แน่ใจว่า ไฟล์ที่ถูกตั้งค่าเป็นโหมดการให้สิทธิ์ที่ระบุไว้ หรือเป็นค่าที่ได้รับสิทธิ์น้อย |
| GEN008060 | ถ้าระบบกำลังใช้ LDAP สำหรับการพิสูจน์ตัวตน หรือข้อมูลแอคเคาต์ไฟล์ /etc/ldap.conf (หรือ เทียบเท่า) ต้องมีโหมด 0644 หรือได้รับสิทธิ์น้อย | **ตำแหน่ง** /etc/security/pscexpert/dodv2/fpmdodfiles<br>**แอ็คชันความเข้ากันได้**<br>ตรวจสอบให้แน่ใจว่า ไฟล์ที่ถูกตั้งค่าเป็นโหมดการให้สิทธิ์ที่ระบุไว้ หรือเป็นค่าที่ได้รับสิทธิ์น้อย |
| GEN008180 | ถ้าระบบกำลังใช้ LDAP สำหรับการพิสูจน์ตัวตน หรือข้อมูลแอคเคาต์ไฟล์การออกใบรับรอง TLS ไดเร็กทอรี หรือทั้งสอง ต้องมีโหมด 0644 (0755 สำหรับไดเร็กทอรี) หรือได้รับสิทธิ์น้อย | **ตำแหน่ง** /etc/security/pscexpert/dodv2/fpmdodfiles<br>**แอ็คชันความเข้ากันได้**<br>ตรวจสอบให้แน่ใจว่า ไฟล์ไดเร็กทอรีที่ระบุเฉพาะ หรือทั้งสอง ถูกตั้งค่าเป็นโหมดการให้สิทธิ์ที่ระบุเฉพาะ หรือเป็นค่าที่ได้รับสิทธิ์น้อย |

*ตารางที่ 6. ข้อกำหนดเกี่ยวกับ DoD access control list (ACL)*

| ID จุดตรวจสอบ Department of Defense STIG | รายละเอียด | ตำแหน่งของสคริปต์ที่นิยามแอ็คชัน และผลลัพธ์ของแอ็คชันที่เปิดใช้งานความเข้ากันได้ |
|---|---|---|
| AIX00110 | ไฟล์ /etc/netsvc.conf ไม่ต้องมี access control list (ACL) ขยายเพิ่ม | **ตำแหน่ง** /etc/security/pscexpert/dodv2/acldodfiles<br>**แอ็คชันความเข้ากันได้**<br>ปิดใช้งาน ACL ที่ขยายเพิ่มที่ระบุไว้<br>**หมายเหตุ:** ค่าติดตั้งนี้ไม่ได้ถูกเปลี่ยนโดยอัตโนมัติเมื่อรีเซ็ตนโยบายเป็น นโยบายดีฟอลต์ของ AIX โดยใช้ไฟล์ DoDv2_to_AIXDefault.xml คุณต้องเปลี่ยนค่าติดตั้งนี้แบบแมนวล |

*ตารางที่ 6. ข้อกำหนดเกี่ยวกับ DoD access control list (ACL) (ต่อ)*

| ID จุดตรวจสอบ Department of Defense STIG | รายละเอียด | ตำแหน่งของสคริปต์ที่นิยามแอ็คชัน และผลลัพธ์ของแอ็คชันที่เปิดใช้งานความเข้ากันได้ |
|---|---|---|
| AIX00350 | ไฟล์ /etc/ftpaccess.ctl ต้องไม่มี ACL ที่ขยายเพิ่ม | **ตำแหน่ง** /etc/security/pscexpert/dodv2/acldodfiles<br>**แอ็คชันความเข้ากันได้**<br>ปิดใช้งาน ACL ที่ขยายเพิ่มที่ระบุไว้<br>**หมายเหตุ:** ค่าติดตั้งนี้ไม่ได้ถูกเปลี่ยนโดยอัตโนมัติเมื่อรีเซ็ตนโยบายเป็น นโยบายดีฟอลต์ของ AIX โดยใช้ไฟล์ DoDv2_to_AIXDefault.xml คุณต้องเปลี่ยนค่าติดตั้งนี้แบบแมนวล |
| GEN000253 | ไฟล์คอนฟิกูเรชันการซิงโครไนซ์เวลา (เช่น /etc/ntp.conf) ต้องไม่มี ACL ที่ขยายเพิ่ม | **ตำแหน่ง** /etc/security/pscexpert/dodv2/acldodfiles<br>**แอ็คชันความเข้ากันได้**<br>ปิดใช้งาน ACL ที่ขยายเพิ่มที่ระบุไว้<br>**หมายเหตุ:** ค่าติดตั้งนี้ไม่ได้ถูกเปลี่ยนโดยอัตโนมัติเมื่อรีเซ็ตนโยบายเป็น นโยบายดีฟอลต์ของ AIX โดยใช้ไฟล์ DoDv2_to_AIXDefault.xml คุณต้องเปลี่ยนค่าติดตั้งนี้แบบแมนวล |
| GEN000930 | โฮมไดเร็กทอรีของแอคเคาต์ root ต้องไม่มี ACL ที่ขยายเพิ่ม | **ตำแหน่ง** /etc/security/pscexpert/dodv2/acldodfiles<br>**แอ็คชันความเข้ากันได้**<br>ปิดใช้งาน ACL ที่ขยายเพิ่มที่ระบุไว้<br>**หมายเหตุ:** ค่าติดตั้งนี้ไม่ได้ถูกเปลี่ยนโดยอัตโนมัติเมื่อรีเซ็ตนโยบายเป็น นโยบายดีฟอลต์ของ AIX โดยใช้ไฟล์ DoDv2_to_AIXDefault.xml คุณต้องเปลี่ยนค่าติดตั้งนี้แบบแมนวล |
| GEN001190 | ไฟล์ daemon เซอร์วิสเครือข่ายทั้งหมดไม่มี ACLs ที่ขยายเพิ่ม | **ตำแหน่ง** /etc/security/pscexpert/dodv2/acldodfiles<br>**แอ็คชันความเข้ากันได้**<br>ปิดใช้งาน ACL ที่ขยายเพิ่มที่ระบุไว้<br>**หมายเหตุ:** ค่าติดตั้งนี้ไม่ได้ถูกเปลี่ยนโดยอัตโนมัติเมื่อรีเซ็ตนโยบายเป็น นโยบายดีฟอลต์ของ AIX โดยใช้ไฟล์ DoDv2_to_AIXDefault.xml คุณต้องเปลี่ยนค่าติดตั้งนี้แบบแมนวล |

*ตารางที่ 6. ข้อกำหนดเกี่ยวกับ DoD access control list (ACL) (ต่อ)*

| ID จุดตรวจสอบ Department of Defense STIG | รายละเอียด | ตำแหน่งของสคริปต์ที่นิยามแอ็คชัน และผลลัพธ์ของแอ็คชันที่เปิดใช้งานความเข้ากันได้ |
|---|---|---|
| GEN001210 | ไฟล์คำสั่งระบบทั้งหมดไม่ต้องมี ACLs ที่ขยายเพิ่ม | **ตำแหน่ง** `/etc/security/pscexpert/dodv2/acldodfiles`<br>**แอ็คชันความเข้ากันได้**<br>ปิดใช้งาน ACL ที่ขยายเพิ่มที่ระบุไว้<br>**หมายเหตุ:** ค่าติดตั้งนี้ไม่ได้ถูกเปลี่ยนโดยอัตโนมัติเมื่อรีเซ็ตนโยบายเป็น นโยบายดีฟอลต์ของ AIX โดยใช้ไฟล์ `DoDv2_to_AIXDefault.xml` คุณต้องเปลี่ยนค่าติดตั้งนี้แบบแมนวล |
| GEN001270 | ไฟล์การทำบันทึกระบบต้องไม่มี ACLs ที่ขยายเพิ่ม ยกเว้นว่าจำเป็นต่อการสนับสนุนซอฟต์แวร์ที่ได้รับสิทธิ์ | **ตำแหน่ง** `/etc/security/pscexpert/dodv2/acldodfiles`<br>**แอ็คชันความเข้ากันได้**<br>ปิดใช้งาน ACL ที่ขยายเพิ่มที่ระบุไว้<br>**หมายเหตุ:** ค่าติดตั้งนี้ไม่ได้ถูกเปลี่ยนโดยอัตโนมัติเมื่อรีเซ็ตนโยบายเป็น นโยบายดีฟอลต์ของ AIX โดยใช้ไฟล์ `DoDv2_to_AIXDefault.xml` คุณต้องเปลี่ยนค่าติดตั้งนี้แบบแมนวล |
| GEN001310 | ไฟล์ไลบรารีทั้งหมดต้องไม่มี ACLs ที่ขยายเพิ่ม | **ตำแหน่ง** `/etc/security/pscexpert/dodv2/acldodfiles`<br>**แอ็คชันความเข้ากันได้**<br>ปิดใช้งาน ACL ที่ขยายเพิ่มที่ระบุไว้<br>**หมายเหตุ:** ค่าติดตั้งนี้ไม่ได้ถูกเปลี่ยนโดยอัตโนมัติเมื่อรีเซ็ตนโยบายเป็น นโยบายดีฟอลต์ของ AIX โดยใช้ไฟล์ `DoDv2_to_AIXDefault.xml` คุณต้องเปลี่ยนค่าติดตั้งนี้แบบแมนวล |
| GEN001361 | ไฟล์คำสั่ง NIS/NIS+/yp ต้องไม่มี ACLs ที่ขยายเพิ่ม | **ตำแหน่ง** `/etc/security/pscexpert/dodv2/acldodfiles`<br>**แอ็คชันความเข้ากันได้**<br>ปิดใช้งาน ACL ที่ขยายเพิ่มที่ระบุไว้<br>**หมายเหตุ:** ค่าติดตั้งนี้ไม่ได้ถูกเปลี่ยนโดยอัตโนมัติเมื่อรีเซ็ตนโยบายเป็น นโยบายดีฟอลต์ของ AIX โดยใช้ไฟล์ `DoDv2_to_AIXDefault.xml` คุณต้องเปลี่ยนค่าติดตั้งนี้แบบแมนวล |

*ตารางที่ 6. ข้อกำหนดเกี่ยวกับ DoD access control list (ACL) (ต่อ)*

| ID จุดตรวจสอบ Department of Defense STIG | รายละเอียด | ตำแหน่งของสคริปต์ที่นิยามแอ็คชัน และผลลัพธ์ของแอ็คชันที่เปิดใช้งานความเข้ากันได้ |
|---|---|---|
| GEN001365 | ไฟล์ /etc/resolv.conf ต้องไม่มี ACL ที่ขยายเพิ่ม | **ตำแหน่ง** /etc/security/pscexpert/dodv2/acldodfiles<br>**แอ็คชันความเข้ากันได้**<br>ปิดใช้งาน ACL ที่ขยายเพิ่มที่ระบุไว้<br>**หมายเหตุ:** ค่าติดตั้งนี้ไม่ได้ถูกเปลี่ยนโดยอัตโนมัติเมื่อรีเซ็ตนโยบายเป็น นโยบายดีฟอลต์ของ AIX โดยใช้ไฟล์ DoDv2_to_AIXDefault.xml คุณต้องเปลี่ยนค่าติดตั้งนี้แบบแมนวล |
| GEN001369 | ไฟล์ /etc/hosts ต้องไม่มี ACL ที่ขยายเพิ่ม | **ตำแหน่ง** /etc/security/pscexpert/dodv2/acldodfiles<br>**แอ็คชันความเข้ากันได้**<br>ปิดใช้งาน ACL ที่ขยายเพิ่มที่ระบุไว้<br>**หมายเหตุ:** ค่าติดตั้งนี้ไม่ได้ถูกเปลี่ยนโดยอัตโนมัติเมื่อรีเซ็ตนโยบายเป็น นโยบายดีฟอลต์ของ AIX โดยใช้ไฟล์ DoDv2_to_AIXDefault.xml คุณต้องเปลี่ยนค่าติดตั้งนี้แบบแมนวล |
| GEN001374 | ไฟล์ /etc/nsswitch.conf ต้องไม่มี ACL ที่ขยายเพิ่ม | **ตำแหน่ง** /etc/security/pscexpert/dodv2/acldodfiles<br>**แอ็คชันความเข้ากันได้**<br>ปิดใช้งาน ACL ที่ขยายเพิ่มที่ระบุไว้<br>**หมายเหตุ:** ค่าติดตั้งนี้ไม่ได้ถูกเปลี่ยนโดยอัตโนมัติเมื่อรีเซ็ตนโยบายเป็น นโยบายดีฟอลต์ของ AIX โดยใช้ไฟล์ DoDv2_to_AIXDefault.xml คุณต้องเปลี่ยนค่าติดตั้งนี้แบบแมนวล |
| GEN001390 | ไฟล์ /etc/passwd ต้องไม่มี ACL ที่ขยายเพิ่ม | **ตำแหน่ง** /etc/security/pscexpert/dodv2/acldodfiles<br>**แอ็คชันความเข้ากันได้**<br>ปิดใช้งาน ACL ที่ขยายเพิ่มที่ระบุไว้<br>**หมายเหตุ:** ค่าติดตั้งนี้ไม่ได้ถูกเปลี่ยนโดยอัตโนมัติเมื่อรีเซ็ตนโยบายเป็น นโยบายดีฟอลต์ของ AIX โดยใช้ไฟล์ DoDv2_to_AIXDefault.xml คุณต้องเปลี่ยนค่าติดตั้งนี้แบบแมนวล |

*ตารางที่ 6. ข้อกำหนดเกี่ยวกับ DoD access control list (ACL) (ต่อ)*

| ID จุดตรวจสอบ Department of Defense STIG | รายละเอียด | ตำแหน่งของสคริปต์ที่นิยามแอ็คชัน และผลลัพธ์ของแอ็คชันที่เปิดใช้งานความเข้ากันได้ |
|---|---|---|
| GEN001394 | ไฟล์ /etc/group ต้องไม่มี ACL ที่ขยายเพิ่ม | **ตำแหน่ง** /etc/security/pscexpert/dodv2/acldodfiles<br>**แอ็คชันความเข้ากันได้**<br>ปิดใช้งาน ACL ที่ขยายเพิ่มที่ระบุไว้<br>**หมายเหตุ:** ค่าติดตั้งนี้ไม่ได้ถูกเปลี่ยนโดยอัตโนมัติเมื่อรีเซ็ตนโยบายเป็น นโยบายดีฟอลต์ของ AIX โดยใช้ไฟล์ DoDv2_to_AIXDefault.xml คุณต้องเปลี่ยนค่าติดตั้งนี้แบบแมนวล |
| GEN001430 | ไฟล์ /etc/security/passwd ต้องไม่มี ACL ที่ขยายเพิ่ม | **ตำแหน่ง** /etc/security/pscexpert/dodv2/acldodfiles<br>**แอ็คชันความเข้ากันได้**<br>ปิดใช้งาน ACL ที่ขยายเพิ่มที่ระบุไว้<br>**หมายเหตุ:** ค่าติดตั้งนี้ไม่ได้ถูกเปลี่ยนโดยอัตโนมัติเมื่อรีเซ็ตนโยบายเป็น นโยบายดีฟอลต์ของ AIX โดยใช้ไฟล์ DoDv2_to_AIXDefault.xml คุณต้องเปลี่ยนค่าติดตั้งนี้แบบแมนวล |
| GEN001570 | ไฟล์และไดเร็กทอรีทั้งหมดที่มี อยู่ในโฮมไดเร็กทอรีต้องไม่มี ACLs ที่ขยายเพิ่ม | **ตำแหน่ง** /etc/security/pscexpert/dodv2/acldodfiles<br>**แอ็คชันความเข้ากันได้**<br>ปิดใช้งาน ACL ที่ขยายเพิ่มที่ระบุไว้<br>**หมายเหตุ:** ค่าติดตั้งนี้ไม่ได้ถูกเปลี่ยนโดยอัตโนมัติเมื่อรีเซ็ตนโยบายเป็น นโยบายดีฟอลต์ของ AIX โดยใช้ไฟล์ DoDv2_to_AIXDefault.xml คุณต้องเปลี่ยนค่าติดตั้งนี้แบบแมนวล |
| GEN001590 | การรันสคริปต์การควบคุมทั้งหมดต้องไม่มี ACLs ที่ขยายเพิ่ม | **ตำแหน่ง** /etc/security/pscexpert/dodv2/acldodfiles<br>**แอ็คชันความเข้ากันได้**<br>ปิดใช้งาน ACL ที่ขยายเพิ่มที่ระบุไว้<br>**หมายเหตุ:** ค่าติดตั้งนี้ไม่ได้ถูกเปลี่ยนโดยอัตโนมัติเมื่อรีเซ็ตนโยบายเป็น นโยบายดีฟอลต์ของ AIX โดยใช้ไฟล์ DoDv2_to_AIXDefault.xml คุณต้องเปลี่ยนค่าติดตั้งนี้แบบแมนวล |

*ตารางที่ 6. ข้อกำหนดเกี่ยวกับ DoD access control list (ACL) (ต่อ)*

| ID จุดตรวจสอบ Department of Defense STIG | รายละเอียด | ตำแหน่งของสคริปต์ที่นิยามแอ็คชัน และผลลัพธ์ของแอ็คชันที่เปิดใช้งานความเข้ากันได้ |
|---|---|---|
| GEN001730 | ไฟล์การเริ่มต้นทำงานแบบโกลบอลทั้งหมดต้องไม่มี ACLs ที่ขยายเพิ่ม | **ตำแหน่ง** `/etc/security/pscexpert/dodv2/acldodfiles`<br>**แอ็คชันความเข้ากันได้**<br>ปิดใช้งาน ACL ที่ขยายเพิ่มที่ระบุไว้<br>**หมายเหตุ:** ค่าติดตั้งนี้ไม่ได้ถูกเปลี่ยนโดยอัตโนมัติเมื่อรีเซ็ตนโยบายเป็น นโยบายดีฟอลต์ของ AIX โดยใช้ไฟล์ `DoDv2_to_AIXDefault.xml` คุณต้องเปลี่ยนค่าติดตั้งนี้แบบแมนวล |
| GEN001810 | ไฟล์ Skeleton ต้องไม่มี ACLs ที่ขยายเพิ่ม | **ตำแหน่ง** `/etc/security/pscexpert/dodv2/acldodfiles`<br>**แอ็คชันความเข้ากันได้**<br>ปิดใช้งาน ACL ที่ขยายเพิ่มที่ระบุไว้<br>**หมายเหตุ:** ค่าติดตั้งนี้ไม่ได้ถูกเปลี่ยนโดยอัตโนมัติเมื่อรีเซ็ตนโยบายเป็น นโยบายดีฟอลต์ของ AIX โดยใช้ไฟล์ `DoDv2_to_AIXDefault.xml` คุณต้องเปลี่ยนค่าติดตั้งนี้แบบแมนวล |
| GEN001890 | ไฟล์การเริ่มต้นทำงานแบบโลคัลต้องไม่มี ACLs ที่ขยายเพิ่ม | **ตำแหน่ง** `/etc/security/pscexpert/dodv2/acldodfiles`<br>**แอ็คชันความเข้ากันได้**<br>ปิดใช้งาน ACL ที่ขยายเพิ่มที่ระบุไว้<br>**หมายเหตุ:** ค่าติดตั้งนี้ไม่ได้ถูกเปลี่ยนโดยอัตโนมัติเมื่อรีเซ็ตนโยบายเป็น นโยบายดีฟอลต์ของ AIX โดยใช้ไฟล์ `DoDv2_to_AIXDefault.xml` คุณต้องเปลี่ยนค่าติดตั้งนี้แบบแมนวล |
| GEN002230 | ไฟล์เซลล์ทั้งหมดต้องไม่มี ACLs ที่ขยายเพิ่ม | **ตำแหน่ง** `/etc/security/pscexpert/dodv2/acldodfiles`<br>**แอ็คชันความเข้ากันได้**<br>ปิดใช้งาน ACL ที่ขยายเพิ่มที่ระบุไว้<br>**หมายเหตุ:** ค่าติดตั้งนี้ไม่ได้ถูกเปลี่ยนโดยอัตโนมัติเมื่อรีเซ็ตนโยบายเป็น นโยบายดีฟอลต์ของ AIX โดยใช้ไฟล์ `DoDv2_to_AIXDefault.xml` คุณต้องเปลี่ยนค่าติดตั้งนี้แบบแมนวล |

*ตารางที่ 6. ข้อกำหนดเกี่ยวกับ DoD access control list (ACL) (ต่อ)*

| ID จุดตรวจสอบ Department of Defense STIG | รายละเอียด | ตำแหน่งของสคริปต์ที่นิยามแอ็คชัน และผลลัพธ์ของแอ็คชันที่เปิดใช้งานความเข้ากันได้ |
|---|---|---|
| GEN002330 | อุปกรณ์ออดิโอต้องไม่มี ACLs ที่ขยายเพิ่ม | **ตำแหน่ง** `/etc/security/pscexpert/dodv2/acldodfiles`<br>**แอ็คชันความเข้ากันได้**<br>ปิดใช้งาน ACL ที่ขยายเพิ่มที่ระบุไว้<br>**หมายเหตุ:** ค่าติดตั้งนี้ไม่ได้ถูกเปลี่ยนโดยอัตโนมัติเมื่อรีเซ็ตนโยบายเป็น นโยบายดีฟอลต์ของ AIX โดยใช้ไฟล์ `DoDv2_to_AIXDefault.xml` คุณต้องเปลี่ยนค่าติดตั้งนี้แบบแมนวล |
| GEN002710 | ไฟล์การตรวจสอบระบบทั้งหมดต้องไม่มี ACLs ที่ขยายเพิ่ม | **ตำแหน่ง** `/etc/security/pscexpert/dodv2/acldodfiles`<br>**แอ็คชันความเข้ากันได้**<br>ปิดใช้งาน ACL ที่ขยายเพิ่มที่ระบุไว้<br>**หมายเหตุ:** ค่าติดตั้งนี้ไม่ได้ถูกเปลี่ยนโดยอัตโนมัติเมื่อรีเซ็ตนโยบายเป็น นโยบายดีฟอลต์ของ AIX โดยใช้ไฟล์ `DoDv2_to_AIXDefault.xml` คุณต้องเปลี่ยนค่าติดตั้งนี้แบบแมนวล |
| GEN002990 | ACLs ที่ขยายเพิ่มควรปิดใช้งานสำหรับไฟล์ `cron.allow` และ `cron.deny` | **ตำแหน่ง** `/etc/security/pscexpert/dodv2/acldodfiles`<br>**แอ็คชันความเข้ากันได้**<br>ปิดใช้งาน ACL ที่ขยายเพิ่มที่ระบุไว้<br>**หมายเหตุ:** ค่าติดตั้งนี้ไม่ได้ถูกเปลี่ยนโดยอัตโนมัติเมื่อรีเซ็ตนโยบายเป็น นโยบายดีฟอลต์ของ AIX โดยใช้ไฟล์ `DoDv2_to_AIXDefault.xml` คุณต้องเปลี่ยนค่าติดตั้งนี้แบบแมนวล |
| GEN003090 | ไฟล์ Crontab ต้องไม่มี ACLs ที่ขยายเพิ่ม | **ตำแหน่ง** `/etc/security/pscexpert/dodv2/acldodfiles`<br>**แอ็คชันความเข้ากันได้**<br>ปิดใช้งาน ACL ที่ขยายเพิ่มที่ระบุไว้<br>**หมายเหตุ:** ค่าติดตั้งนี้ไม่ได้ถูกเปลี่ยนโดยอัตโนมัติเมื่อรีเซ็ตนโยบายเป็น นโยบายดีฟอลต์ของ AIX โดยใช้ไฟล์ `DoDv2_to_AIXDefault.xml` คุณต้องเปลี่ยนค่าติดตั้งนี้แบบแมนวล |

*ตารางที่ 6. ข้อกำหนดเกี่ยวกับ DoD access control list (ACL) (ต่อ)*

| ID จุดตรวจสอบ Department of Defense STIG | รายละเอียด | ตำแหน่งของสคริปต์ที่นิยามแอ็คชัน และผลลัพธ์ของแอ็คชันที่เปิดใช้งานความเข้ากันได้ |
|---|---|---|
| GEN003110 | ไดเร็กทอรี Cron และ crontab ต้องไม่มี ACLs ที่ขยายเพิ่ม | **ตำแหน่ง** `/etc/security/pscexpert/dodv2/acldodfiles`<br>**แอ็คชันความเข้ากันได้**<br>ปิดใช้งาน ACL ที่ขยายเพิ่มที่ระบุไว้<br>**หมายเหตุ:** ค่าติดตั้งนี้ไม่ได้ถูกเปลี่ยนโดยอัตโนมัติเมื่อรีเซ็ตนโยบายเป็น นโยบายดีฟอลต์ของ AIX โดยใช้ไฟล์ `DoDv2_to_AIXDefault.xml` คุณต้องเปลี่ยนค่าติดตั้งนี้แบบแมนวล |
| GEN003190 | ไฟล์การทำบันทึก cron ต้องไม่มี ACLs ที่ขยายเพิ่ม | **ตำแหน่ง** `/etc/security/pscexpert/dodv2/acldodfiles`<br>**แอ็คชันความเข้ากันได้**<br>ปิดใช้งาน ACL ที่ขยายเพิ่มที่ระบุไว้<br>**หมายเหตุ:** ค่าติดตั้งนี้ไม่ได้ถูกเปลี่ยนโดยอัตโนมัติเมื่อรีเซ็ตนโยบายเป็น นโยบายดีฟอลต์ของ AIX โดยใช้ไฟล์ `DoDv2_to_AIXDefault.xml` คุณต้องเปลี่ยนค่าติดตั้งนี้แบบแมนวล |
| GEN003210 | ไฟล์ `cron.deny` ต้องไม่มี ACL ที่ขยายเพิ่ม | **ตำแหน่ง** `/etc/security/pscexpert/dodv2/acldodfiles`<br>**แอ็คชันความเข้ากันได้**<br>ปิดใช้งาน ACL ที่ขยายเพิ่มที่ระบุไว้<br>**หมายเหตุ:** ค่าติดตั้งนี้ไม่ได้ถูกเปลี่ยนโดยอัตโนมัติเมื่อรีเซ็ตนโยบายเป็น นโยบายดีฟอลต์ของ AIX โดยใช้ไฟล์ `DoDv2_to_AIXDefault.xml` คุณต้องเปลี่ยนค่าติดตั้งนี้แบบแมนวล |
| GEN003245 | ไฟล์ `at.allow` ต้องไม่มี ACL ที่ขยายเพิ่ม | **ตำแหน่ง** `/etc/security/pscexpert/dodv2/acldodfiles`<br>**แอ็คชันความเข้ากันได้**<br>ปิดใช้งาน ACL ที่ขยายเพิ่มที่ระบุไว้<br>**หมายเหตุ:** ค่าติดตั้งนี้ไม่ได้ถูกเปลี่ยนโดยอัตโนมัติเมื่อรีเซ็ตนโยบายเป็น นโยบายดีฟอลต์ของ AIX โดยใช้ไฟล์ `DoDv2_to_AIXDefault.xml` คุณต้องเปลี่ยนค่าติดตั้งนี้แบบแมนวล |

*ตารางที่ 6. ข้อกำหนดเกี่ยวกับ DoD access control list (ACL) (ต่อ)*

| ID จุดตรวจสอบ Department of Defense STIG | รายละเอียด | ตำแหน่งของสคริปต์ที่นิยามแอ็คชัน และผลลัพธ์ของแอ็คชันที่เปิดใช้งานความเข้ากันได้ |
|---|---|---|
| GEN003255 | ไฟล์ `at.deny` ต้องไม่มี ACL ที่ขยายเพิ่ม | **ตำแหน่ง** `/etc/security/pscexpert/dodv2/acldodfiles`<br>**แอ็คชันความเข้ากันได้**<br>ปิดใช้งาน ACL ที่ขยายเพิ่มที่ระบุไว้<br>**หมายเหตุ:** ค่าติดตั้งนี้ไม่ได้ถูกเปลี่ยนโดยอัตโนมัติเมื่อรีเซ็ตนโยบายเป็น นโยบายดีฟอลต์ของ AIX โดยใช้ไฟล์ `DoDv2_to_AIXDefault.xml` คุณต้องเปลี่ยนค่าติดตั้งนี้แบบแมนวล |
| GEN003410 | ไดเร็กทอรี `at` ต้องไม่มี ACL ที่ขยายเพิ่ม | **ตำแหน่ง** `/etc/security/pscexpert/dodv2/acldodfiles`<br>**แอ็คชันความเข้ากันได้**<br>ปิดใช้งาน ACL ที่ขยายเพิ่มที่ระบุไว้<br>**หมายเหตุ:** ค่าติดตั้งนี้ไม่ได้ถูกเปลี่ยนโดยอัตโนมัติเมื่อรีเซ็ตนโยบายเป็น นโยบายดีฟอลต์ของ AIX โดยใช้ไฟล์ `DoDv2_to_AIXDefault.xml` คุณต้องเปลี่ยนค่าติดตั้งนี้แบบแมนวล |
| GEN003745 | ไฟล์ `inetd.conf` และ `xinetd.conf` ต้องไม่มี ACLs ที่ขยายเพิ่ม | **ตำแหน่ง** `/etc/security/pscexpert/dodv2/acldodfiles`<br>**แอ็คชันความเข้ากันได้**<br>ปิดใช้งาน ACL ที่ขยายเพิ่มที่ระบุไว้<br>**หมายเหตุ:** ค่าติดตั้งนี้ไม่ได้ถูกเปลี่ยนโดยอัตโนมัติเมื่อรีเซ็ตนโยบายเป็น นโยบายดีฟอลต์ของ AIX โดยใช้ไฟล์ `DoDv2_to_AIXDefault.xml` คุณต้องเปลี่ยนค่าติดตั้งนี้แบบแมนวล |
| GEN003790 | ไฟล์เซอร์วิสต้องไม่มี ACL ที่ขยายเพิ่ม | **ตำแหน่ง** `/etc/security/pscexpert/dodv2/acldodfiles`<br>**แอ็คชันความเข้ากันได้**<br>ปิดใช้งาน ACL ที่ขยายเพิ่มที่ระบุไว้<br>**หมายเหตุ:** ค่าติดตั้งนี้ไม่ได้ถูกเปลี่ยนโดยอัตโนมัติเมื่อรีเซ็ตนโยบายเป็น นโยบายดีฟอลต์ของ AIX โดยใช้ไฟล์ `DoDv2_to_AIXDefault.xml` คุณต้องเปลี่ยนค่าติดตั้งนี้แบบแมนวล |

*ตารางที่ 6. ข้อกำหนดเกี่ยวกับ DoD access control list (ACL) (ต่อ)*

| ID จุดตรวจสอบ Department of Defense STIG | รายละเอียด | ตำแหน่งของสคริปต์ที่นิยามแอ็คชัน และผลลัพธ์ของแอ็คชันที่เปิดใช้งานความเข้ากันได้ |
|---|---|---|
| GEN003950 | ไฟล์ `hosts.lpd` (หรือ เทียบเท่า) ต้องไม่มี ACL ที่ขยายเพิ่ม | **ตำแหน่ง** `/etc/security/pscexpert/dodv2/acldodfiles`<br>**แอ็คชันความเข้ากันได้**<br>ปิดใช้งาน ACL ที่ขยายเพิ่มที่ระบุไว้<br>**หมายเหตุ:** ค่าติดตั้งนี้ไม่ได้ถูกเปลี่ยนโดยอัตโนมัติเมื่อรีเซ็ตนโยบายเป็น นโยบายดีฟอลต์ของ AIX โดยใช้ไฟล์ `DoDv2_to_AIXDefault.xml` คุณต้องเปลี่ยนค่าติดตั้งนี้แบบแมนวล |
| GEN004010 | ไฟล์ `traceroute` ต้องไม่มี ACL ที่ขยายเพิ่ม | **ตำแหน่ง** `/etc/security/pscexpert/dodv2/acldodfiles`<br>**แอ็คชันความเข้ากันได้**<br>ปิดใช้งาน ACL ที่ขยายเพิ่มที่ระบุไว้<br>**หมายเหตุ:** ค่าติดตั้งนี้ไม่ได้ถูกเปลี่ยนโดยอัตโนมัติเมื่อรีเซ็ตนโยบายเป็น นโยบายดีฟอลต์ของ AIX โดยใช้ไฟล์ `DoDv2_to_AIXDefault.xml` คุณต้องเปลี่ยนค่าติดตั้งนี้แบบแมนวล |
| GEN004390 | ไฟล์ `alias` ต้องไม่มี ACL ที่ขยายเพิ่ม | **ตำแหน่ง** `/etc/security/pscexpert/dodv2/acldodfiles`<br>**แอ็คชันความเข้ากันได้**<br>ปิดใช้งาน ACL ที่ขยายเพิ่มที่ระบุไว้<br>**หมายเหตุ:** ค่าติดตั้งนี้ไม่ได้ถูกเปลี่ยนโดยอัตโนมัติเมื่อรีเซ็ตนโยบายเป็น นโยบายดีฟอลต์ของ AIX โดยใช้ไฟล์ `DoDv2_to_AIXDefault.xml` คุณต้องเปลี่ยนค่าติดตั้งนี้แบบแมนวล |
| GEN004430 | ไฟล์ที่รันผ่านไฟล์เมล `aliases` ต้องไม่มี ACLs ที่ขยายเพิ่ม | **ตำแหน่ง** `/etc/security/pscexpert/dodv2/acldodfiles`<br>**แอ็คชันความเข้ากันได้**<br>ปิดใช้งาน ACL ที่ขยายเพิ่มที่ระบุไว้<br>**หมายเหตุ:** ค่าติดตั้งนี้ไม่ได้ถูกเปลี่ยนโดยอัตโนมัติเมื่อรีเซ็ตนโยบายเป็น นโยบายดีฟอลต์ของ AIX โดยใช้ไฟล์ `DoDv2_to_AIXDefault.xml` คุณต้องเปลี่ยนค่าติดตั้งนี้แบบแมนวล |

*ตารางที่ 6. ข้อกำหนดเกี่ยวกับ DoD access control list (ACL) (ต่อ)*

| ID จุดตรวจสอบ Department of Defense STIG | รายละเอียด | ตำแหน่งของสคริปต์ที่นิยามแอ็คชัน และผลลัพธ์ของแอ็คชันที่เปิดใช้งานความเข้ากันได้ |
|---|---|---|
| GEN004510 | ไฟล์การทำบันทึกเซอร์วิส SMTP ต้องไม่มี ACL ที่ขยายเพิ่ม | **ตำแหน่ง** `/etc/security/pscexpert/dodv2/acldodfiles`<br>**แอ็คชันความเข้ากันได้**<br>ปิดใช้งาน ACL ที่ขยายเพิ่มที่ระบุไว้<br>**หมายเหตุ:** ค่าติดตั้งนี้ไม่ได้ถูกเปลี่ยนโดยอัตโนมัติเมื่อรีเซ็ตนโยบายเป็น นโยบายดีฟอลต์ของ AIX โดยใช้ไฟล์ `DoDv2_to_AIXDefault.xml` คุณต้องเปลี่ยนค่าติดตั้งนี้แบบแมนวล |
| GEN004950 | ไฟล์ `ftpusers` ต้องไม่มี ACL ที่ขยายเพิ่ม | **ตำแหน่ง** `/etc/security/pscexpert/dodv2/acldodfiles`<br>**แอ็คชันความเข้ากันได้**<br>ปิดใช้งาน ACL ที่ขยายเพิ่มที่ระบุไว้<br>**หมายเหตุ:** ค่าติดตั้งนี้ไม่ได้ถูกเปลี่ยนโดยอัตโนมัติเมื่อรีเซ็ตนโยบายเป็น นโยบายดีฟอลต์ของ AIX โดยใช้ไฟล์ `DoDv2_to_AIXDefault.xml` คุณต้องเปลี่ยนค่าติดตั้งนี้แบบแมนวล |
| GEN005190 | ไฟล์ `.Xauthority` ต้องไม่มี ACLs ที่ขยายเพิ่ม | **ตำแหน่ง** `/etc/security/pscexpert/dodv2/acldodfiles`<br>**แอ็คชันความเข้ากันได้**<br>ปิดใช้งาน ACL ที่ขยายเพิ่มที่ระบุไว้<br>**หมายเหตุ:** ค่าติดตั้งนี้ไม่ได้ถูกเปลี่ยนโดยอัตโนมัติเมื่อรีเซ็ตนโยบายเป็น นโยบายดีฟอลต์ของ AIX โดยใช้ไฟล์ `DoDv2_to_AIXDefault.xml` คุณต้องเปลี่ยนค่าติดตั้งนี้แบบแมนวล |
| GEN005350 | ไฟล์ Management Information Base (MIB) ต้องไม่มี ACLs ที่ขยายเพิ่ม | **ตำแหน่ง** `/etc/security/pscexpert/dodv2/acldodfiles`<br>**แอ็คชันความเข้ากันได้**<br>ปิดใช้งาน ACL ที่ขยายเพิ่มที่ระบุไว้<br>**หมายเหตุ:** ค่าติดตั้งนี้ไม่ได้ถูกเปลี่ยนโดยอัตโนมัติเมื่อรีเซ็ตนโยบายเป็น นโยบายดีฟอลต์ของ AIX โดยใช้ไฟล์ `DoDv2_to_AIXDefault.xml` คุณต้องเปลี่ยนค่าติดตั้งนี้แบบแมนวล |

*ตารางที่ 6. ข้อกำหนดเกี่ยวกับ DoD access control list (ACL) (ต่อ)*

| ID จุดตรวจสอบ Department of Defense STIG | รายละเอียด | ตำแหน่งของสคริปต์ที่นิยามแอ็คชัน และผลลัพธ์ของแอ็คชันที่เปิดใช้งานความเข้ากันได้ |
|---|---|---|
| GEN005375 | ไฟล์ `snmpd.conf` ต้องไม่มี ACL ที่ขยายเพิ่ม | **ตำแหน่ง** `/etc/security/pscexpert/dodv2/acldodfiles`<br>**แอ็คชันความเข้ากันได้**<br>ปิดใช้งาน ACL ที่ขยายเพิ่มที่ระบุไว้<br>**หมายเหตุ:** ค่าติดตั้งนี้ไม่ได้ถูกเปลี่ยนโดยอัตโนมัติเมื่อรีเซ็ตนโยบายเป็น นโยบายดีฟอลต์ของ AIX โดยใช้ไฟล์ `DoDv2_to_AIXDefault.xml` คุณต้องเปลี่ยนค่าติดตั้งนี้แบบแมนวล |
| GEN005395 | ไฟล์ `/etc/syslog.conf` ต้องไม่มี ACL ที่ขยายเพิ่ม | **ตำแหน่ง** `/etc/security/pscexpert/dodv2/acldodfiles`<br>**แอ็คชันความเข้ากันได้**<br>ปิดใช้งาน ACL ที่ขยายเพิ่มที่ระบุไว้<br>**หมายเหตุ:** ค่าติดตั้งนี้ไม่ได้ถูกเปลี่ยนโดยอัตโนมัติเมื่อรีเซ็ตนโยบายเป็น นโยบายดีฟอลต์ของ AIX โดยใช้ไฟล์ `DoDv2_to_AIXDefault.xml` คุณต้องเปลี่ยนค่าติดตั้งนี้แบบแมนวล |
| GEN006150 | ไฟล์ `/usr/lib/smb.conf` ต้องไม่มี ACL ที่ขยายเพิ่ม | **ตำแหน่ง** `/etc/security/pscexpert/dodv2/acldodfiles`<br>**แอ็คชันความเข้ากันได้**<br>ปิดใช้งาน ACL ที่ขยายเพิ่มที่ระบุไว้<br>**หมายเหตุ:** ค่าติดตั้งนี้ไม่ได้ถูกเปลี่ยนโดยอัตโนมัติเมื่อรีเซ็ตนโยบายเป็น นโยบายดีฟอลต์ของ AIX โดยใช้ไฟล์ `DoDv2_to_AIXDefault.xml` คุณต้องเปลี่ยนค่าติดตั้งนี้แบบแมนวล |
| GEN006210 | ไฟล์ `/var/private/smbpasswd` ต้องไม่มี ACL ที่ขยายเพิ่ม | **ตำแหน่ง** `/etc/security/pscexpert/dodv2/acldodfiles`<br>**แอ็คชันความเข้ากันได้**<br>ปิดใช้งาน ACL ที่ขยายเพิ่มที่ระบุไว้<br>**หมายเหตุ:** ค่าติดตั้งนี้ไม่ได้ถูกเปลี่ยนโดยอัตโนมัติเมื่อรีเซ็ตนโยบายเป็น นโยบายดีฟอลต์ของ AIX โดยใช้ไฟล์ `DoDv2_to_AIXDefault.xml` คุณต้องเปลี่ยนค่าติดตั้งนี้แบบแมนวล |

*ตารางที่ 6. ข้อกำหนดเกี่ยวกับ DoD access control list (ACL) (ต่อ)*

| ID จุดตรวจสอบ Department of Defense STIG | รายละเอียด | ตำแหน่งของสคริปต์ที่นิยามแอ็คชัน และผลลัพธ์ของแอ็คชันที่เปิดใช้งานความเข้ากันได้ |
|---|---|---|
| GEN006270 | ไฟล์ /etc/news/hosts.nntp ต้องไม่มี ACL ที่ขยายเพิ่ม | **ตำแหน่ง** /etc/security/pscexpert/dodv2/acldodfiles<br>**แอ็คชันความเข้ากันได้**<br>ปิดใช้งาน ACL ที่ขยายเพิ่มที่ระบุไว้<br>**หมายเหตุ:** ค่าติดตั้งนี้ไม่ได้ถูกเปลี่ยนโดยอัตโนมัติเมื่อรีเซ็ตนโยบายเป็น นโยบายดีฟอลต์ของ AIX โดยใช้ไฟล์ DoDv2_to_AIXDefault.xml คุณต้องเปลี่ยนค่าติดตั้งนี้แบบแมนวล |
| GEN006290 | ไฟล์ /etc/news/hosts.nntp.nolimit ต้องไม่มี ACL ที่ขยายเพิ่ม | **ตำแหน่ง** /etc/security/pscexpert/dodv2/acldodfiles<br>**แอ็คชันความเข้ากันได้**<br>ปิดใช้งาน ACL ที่ขยายเพิ่มที่ระบุไว้<br>**หมายเหตุ:** ค่าติดตั้งนี้ไม่ได้ถูกเปลี่ยนโดยอัตโนมัติเมื่อรีเซ็ตนโยบายเป็น นโยบายดีฟอลต์ของ AIX โดยใช้ไฟล์ DoDv2_to_AIXDefault.xml คุณต้องเปลี่ยนค่าติดตั้งนี้แบบแมนวล |
| GEN006310 | ไฟล์ /etc/news/nnrp.access ต้องไม่มี ACL ที่ขยายเพิ่ม | **ตำแหน่ง** /etc/security/pscexpert/dodv2/acldodfiles<br>**แอ็คชันความเข้ากันได้**<br>ปิดใช้งาน ACL ที่ขยายเพิ่มที่ระบุไว้<br>**หมายเหตุ:** ค่าติดตั้งนี้ไม่ได้ถูกเปลี่ยนโดยอัตโนมัติเมื่อรีเซ็ตนโยบายเป็น นโยบายดีฟอลต์ของ AIX โดยใช้ไฟล์ DoDv2_to_AIXDefault.xml คุณต้องเปลี่ยนค่าติดตั้งนี้แบบแมนวล |
| GEN006330 | ไฟล์ /etc/news/passwd.nntp ต้องไม่มี ACL ที่ขยายเพิ่ม | **ตำแหน่ง** /etc/security/pscexpert/dodv2/acldodfiles<br>**แอ็คชันความเข้ากันได้**<br>ปิดใช้งาน ACL ที่ขยายเพิ่มที่ระบุไว้<br>**หมายเหตุ:** ค่าติดตั้งนี้ไม่ได้ถูกเปลี่ยนโดยอัตโนมัติเมื่อรีเซ็ตนโยบายเป็น นโยบายดีฟอลต์ของ AIX โดยใช้ไฟล์ DoDv2_to_AIXDefault.xml คุณต้องเปลี่ยนค่าติดตั้งนี้แบบแมนวล |

*ตารางที่ 6. ข้อกำหนดเกี่ยวกับ DoD access control list (ACL) (ต่อ)*

| ID จุดตรวจสอบ Department of Defense STIG | รายละเอียด | ตำแหน่งของสคริปต์ที่นิยามแอ็คชัน และผลลัพธ์ของแอ็คชันที่เปิดใช้งานความเข้ากันได้ |
|---|---|---|
| GEN008120 | ถ้าระบบกำลังใช้ LDAP สำหรับการพิสูจน์ตัวตน หรือข้อมูลแอคเคาต์ ไฟล์ `/etc/ldap.conf` (หรือ เทียบเท่า access control list (ACL) ที่ขยายเพิ่ม | **ตำแหน่ง** `/etc/security/pscexpert/dodv2/acldodfiles`<br>**แอ็คชันความเข้ากันได้**<br>ตรวจสอบให้แน่ใจว่า ไฟล์ที่ระบุไว้ไม่มี ACL ที่ขยายเพิ่ม<br>**หมายเหตุ:** ค่าติดตั้งนี้ไม่ได้ถูกเปลี่ยนโดยอัตโนมัติเมื่อรีเซ็ตนโยบายเป็น นโยบายดีฟอลต์ของ AIX โดยใช้ไฟล์ `DoDv2_to_AIXDefault.xml` คุณต้องเปลี่ยนค่าติดตั้งนี้แบบแมนวล |
| GEN008200 | ถ้าระบบกำลังใช้ LDAP สำหรับการพิสูจน์ตัวตน หรือข้อมูลแอคเคาต์ ไฟล์การออกใบรับรอง LDAP TLS หรือไดเร็กทอรี (ตามความเหมาะสม) ต้องไม่มี ACL ที่ขยายเพิ่ม | **ตำแหน่ง** `/etc/security/pscexpert/dodv2/acldodfiles`<br>**แอ็คชันความเข้ากันได้**<br>ตรวจสอบให้แน่ใจว่า ไดเร็กทอรีหรือไฟล์ที่ระบุไว้ไม่มี ACL ที่ขยายเพิ่ม<br>**หมายเหตุ:** ค่าติดตั้งนี้ไม่ได้ถูกเปลี่ยนโดยอัตโนมัติเมื่อรีเซ็ตนโยบายเป็น นโยบายดีฟอลต์ของ AIX โดยใช้ไฟล์ `DoDv2_to_AIXDefault.xml` คุณต้องเปลี่ยนค่าติดตั้งนี้แบบแมนวล |

**ข้อมูลที่เกี่ยวข้อง:**

ความเข้ากันได้ STIG ของกระทรวงกลาโหม

## มาตรฐาน Payment Card Industry - Data Security Standard

Payment Card Industry – Data Security Standard (PCI – DSS) จัดหมวดหมู่การรักษาความปลอดภัยด้าน IT เป็น 12 ส่วนที่เรียกว่า ข้อกำหนด 12 ข้อ และขั้นตอนประเมินความปลอดภัย

ข้อกำหนด 12 ข้อ และขั้นตอนประเมินความปลอดภัยของการรักษาความปลอดภัยด้าน IT ที่กำหนดโดย PCI – DSS จะมีรายการต่อไปนี้:

**ข้อกำหนดที่ 1: ติดตั้งและดูแลรักษาคอนฟิกูเรชันไฟล์วอลล์เพื่อ ปกป้องข้อมูลของสมาชิก**
รายการเอกสารของเซอร์วิส และพอร์ตที่จำเป็น สำหรับธุรกิจ ข้อกำหนดนี้จะ ถูกปรับใช้โดยการปิดใช้เซอร์วิสที่ไม่จำเป็น และเซอร์วิสที่ไม่ปลอดภัย

**ข้อกำหนดที่ 2: อย่าใช้ค่าดีฟอลต์ที่กำหนดโดยผู้จำหน่ายสำหรับ รหัสผ่านของระบบและพารามิเตอร์ความปลอดภัยอื่นๆ**
เปลี่ยนค่าดีฟอลต์ที่กำหนดโดยผู้จำหน่ายเสมอก่อน คุณติดตั้งระบบบนเครือข่าย ข้อกำหนดนี้จะถูกปรับใช้โดยการปิดใช้งาน Simple Network Management Protocol (SNMP) daemon

**ข้อกำหนดที่ 3: ปกป้องข้อมูลที่จัดเก็บไว้ของสมาชิก**

ข้อกำหนดนี้จะถูกปรับใช้โดยการเปิดใช้งาน คุณลักษณะ Encrypted File System (EFS) ที่มาพร้อมกับระบบปฏิบัติการ AIX

**ข้อกำหนดที่ 4: เข้ารหัสข้อมูลของสมาชิกเมื่อคุณส่ง ข้อมูลข้ามเครือข่ายพับลิกที่เปิด**

ข้อกำหนดนี้จะถูกปรับใช้โดยการเปิดใช้ คุณลักษณะ IP Security (IPSEC) ที่มาพร้อมกับระบบปฏิบัติการ AIX

**ข้อกำหนดที่ 5: ใช้ และอัพเดตโปรแกรมซอฟต์แวร์ป้องกันไวรัส**

ข้อกำหนดนี้จะถูกปรับใช้โดยการใช้โปรแกรมนโยบาย Trusted Execution Trusted Execution เป็นซอฟต์แวร์ป้องกันไวรัสที่แนะนำ และมีอยู่ในระบบปฏิบัติการ AIX PCI ต้องการให้คุณ บันทึกล็อกจากโปรแกรม Trusted Execution โดยการเปิดใช้ข้อมูล การรักษาความปลอดภัย และการจัดการเหตุการณ์ (SIEM) เพื่อมอนิเตอร์การแจ้งเตือน โดยการรันโปรแกรม Trusted Execution ในโหมดบันทึกเท่านั้น โปรแกรมจะ ไม่หยุดการตรวจสอบเมื่อเกิดข้อผิดพลาดจากแฮชไม่ตรงกัน

**ข้อกำหนดที่ 6: พัฒนาและดูแลรักษาระบบความปลอดภัยและแอ็พพลิเคชัน**

เพื่อปรับใช้ข้อกำหนดนี้ คุณต้องติดตั้ง แพทช์ที่จำเป็นไปยังระบบของคุณด้วยตัวเอง หากคุณซื้อ PowerSC Standard Edition คุณสามารถใช้คุณลักษณะ Trusted Network Connect (TNC)

**ข้อกำหนดที่ 7: จำกัดการเข้าถึงข้อมูลสมาชิก ตามที่ธุรกิจ จำเป็นต้องรู้**

คุณสามารถปรับใช้มาตรการการควบคุมการเข้าถึงที่ปลอดภัย โดยการใช้คุณลักษณะ RBAC เพื่อเปิดใช้กฎและบทบาท RBAC ไม่สามารถ ดำเนินการโดยอัตโนมัติเนื่องจากต้องมีอินพุทของผู้ดูแลระบบเพื่อ เปิดใช้

`RbacEnablement` จะตรวจสอบระบบ เพื่อระบุว่าคุณสมบัติ isso, so และ sa สำหรับบทบาท มีอยู่บนระบบหรือไม่ หากคุณสมบัติเหล่านี้ไม่มีอยู่ สคริปต์ จะสร้างขึ้นมา สคริปต์นี้รันเป็นส่วนหนึ่งของการตรวจสอบ pscexpert ที่จะสมบูรณ์เมื่อรันคำสั่ง เช่น คำสั่ง `pscxpert -c`

**ขั้นตอนที่ 8: กำหนด ID เฉพาะให้กับแต่ละบุคคลที่มีการเข้าถึง คอมพิวเตอร์**

คุณสามารถใช้ข้อกำหนดนี้โดยการเปิดใช้ โปรไฟล์ PCI กฎต่อไปนี้จะใช้ถูกนำมาใช้กับนโยบาย PCI:

- เปลี่ยนแปลงรหัสผ่านผู้ใช้อย่างน้อยทุกๆ 90 วัน
- ต้องมีความยาวรหัสผ่านต่ำสุด 7 ตัวอักษร
- ใช้รหัสผ่านที่มีทั้งตัวเลข และตัวอักษร
- .ไม่อนุญาตให้แต่ละบุคคลส่งรหัสผ่านใหม่ ที่เป็นรหัสผ่านเดียวกับรหัสผ่านสี่ตัวที่ใช้ก่อนหน้านี้
- จำกัดความพยายามในการเข้าถึงซ้ำโดยการล็อก ID ผู้ใช้หลังจากการพยายามเข้าถึงที่ไม่สำเร็จ 6 ครั้ง
- ตั้งค่าช่วงเวลาการล็อกเท่ากับ 30 นาที หรือจนกว่า ผู้ดูแลระบบจะเปิดใช้ ID ผู้ใช้ใหม่อีกครั้ง
- ต้องให้ผู้ใช้ป้อนรหัสผ่านใหม่อีกครั้งเพื่อเปิดใช้ เทอร์มินัลหลังกจากไม่ได้ทำงานเป็นเวลา 15 นาทีหรือนานกว่า

**ข้อกำหนดที่ 9: จำกัดการเข้าถึงทางกายภาพต่อข้อมูลสมาชิก**

จัดเก็บที่เก็บข้อมูลที่มีข้อมูลสมาชิกที่สำคัญ ในห้องที่มีการจำกัดการเข้าถึง

**ข้อกำหนดที่ 10: ติดตามและเฝ้าดูการเข้าถึงรีซอร์สเครือข่าย และข้อมูลสมาชิกทั้งหมด**

ข้อกำหนดนี้จะถูกใช้โดยการล็อกอินเพื่อเข้าถึง คอมโพเนนต์ระบบโดยการเปิดใช้การล็อกออนไปยังคอมโพเนนต์ระบบ โดยอัตโนมัติ

**ข้อกำหนดที่ 11: ทดสอบระบบและกระบวนการด้านความปลอดภัยเป็นประจำ**

ข้อกำหนดนี้จะถูกใช้โดยการใช้คุณลักษณะ Real-Time Compliance

**ข้อกำหนดที่ 12: รักษานโยบายการรักษาความปลอดภัยที่มีข้อมูล ความปลอดภัยของพนักงานและผู้รับจ้าง**

เปิดใช้งานโมเด็มเฉพาะสำหรับผู้จำหน่ายเมื่อจำเป็น ต้องใช้ และปิดใช้งานทันทีหลังจากการใช้ ข้อกำหนดนี้ จะถูกใช้โดยการปิดใช้การล็อกอินรูทแบบรีโมท การเปิดใช้บนพื้นฐาน ที่จำเป็นโดยผู้ดูแลระบบ จากนั้นจะปิดใช้งานเมื่อ ไม่จำเป็นต้องใช้

PowerSC Standard Edition จะลด การจัดการการกำหนดค่าคอนฟิกที่จำเป็นเพื่อให้ตรงตามแนวทางที่กำหนดโดย PCI DSS เวอร์ชัน 2.0 และ PCI DSS เวอร์ชัน 3.0 อย่างไรก็ตาม กระบวนการทั้งหมดไม่สามารถดำเนินการแบบอัตโนมัติ

ตัวอย่างเช่น การจำกัดการเข้าถึงข้อมูลของผู้ถือบัตร ตามข้อกำหนดทางธุรกิจที่ไม่สามารถทำให้เป็นอัตโนมัติ ระบบปฏิบัติการ AIX จะมีเทคโนโลยี ด้านการรักษาความปลอดภัยที่แข็งแกร่ง เช่น Role Based Access Control (RBAC) อย่างไรก็ตาม PowerSC Standard Edition ไม่สาสมารถกำหนดค่าคอนฟิกนี้ โดยอัตโนมัติ เนื่องจากไม่สามารถระบุบุคคลที่ จำเป็นต้องเข้าถึง และบุคคลที่ไม่ต้องเข้าถึงได้ IBM Compliance Expert สามารถทำให้การกำหนดคอนฟิก ของการตั้งค่าการรักษาความปลอดภัยอื่นๆ ที่สอดคล้องกับข้อกำหนด PCI เป็นอัตโนมัติ

เมื่อโปรไฟล์ PCI ถูกนำไปใช้กับสภาวะแวดล้อมแบบฐานข้อมูล พอร์ต TCP และ UDP ต่างๆ ถูกใช้โดยสแต็กของซอฟต์แวร์ถูกปิดใช้งานตามข้อจำกัด คุณต้องเปิดใช้งานพอร์ตเหล่านี้ และปิดใช้งานฟังก์ชัน Trusted Execution เพื่อรันแอ็พพลิเคชันและเวิร์กโหลด รันคำสั่งต่อไปนี้ เพื่อลบข้อจำกัดเกี่ยวกับพอร์ตและปิดใช้งานฟังก์ชัน Trusted Execution :

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

**หมายเหตุ:** ไฟล์สคริปต์ที่กำหนดเองทั้งหมดที่มีไว้ เพื่อรักษามาตรฐาน PCI – DSS จะอยู่ในไดเร็กทอรี `/etc/security/pscexpert/bin`

ตารางต่อไปนี้แสดงวิธี PowerSC Standard Edition ระบุข้อกำหนดของมาตรฐาน PCI DSS โดย การใช้ฟังก์ชันของยูทิลิตี้ AIX Security Expert:

*ตารางที่ 7. การตั้งค่าที่เกี่ยวข้องกับมาตรฐานการปฏิบัติตามข้อกำหนด PCI DSS เวอร์ชัน 2.0 และเวอร์ชัน 3.0*

| การปรับใช้มาตรฐาน PCI DSS เหล่านี้ | ข้อมูลจำเพาะการนำไปปฏิบัติ | การปรับใช้ AIX Security Expert | ตำแหน่งของสคริปต์ที่แก้ไขค่า |
|---|---|---|---|
| 2.1 | เปลี่ยนค่าดีฟอลต์ที่กำหนดโดยผู้จำหน่ายเสมอก่อน การติดตั้งระบบบนเครือข่าย ตัวอย่างเช่น สตริงชุมชนของโปรโตคอลการจัดการเครือข่ายพื้นฐาน รวมถึงรหัสผ่าน และลบ บัญชีที่ไม่จำเป็นออก | ตั้งค่าจำนวนต่ำสุดของสัปดาห์ที่ต้องผ่านไปก่อนที่คุณจะสามารถเปลี่ยนรหัสผ่านให้เท่ากับ 0 สัปดาห์โดยการตั้งค่าพารามิเตอร์ `minage` ให้มีค่าเป็น 0 | `/etc/security/pscexpert/bin/chusrattr` |
| **PCI เวอร์ชัน 2**<br>8.5.9<br>**PCI เวอร์ชัน 3**<br>8.2.4 | เปลี่ยนแปลงรหัสผ่านผู้ใช้อย่างน้อยทุกๆ 90 วัน | ตั้งค่าจำนวนสัปดาห์สูงสุดที่รหัสผ่านจะใช้ได้เป็น 13 สัปดาห์โดย ตั้งค่าพารามิเตอร์ `maxage` เป็นค่า 13 | `/etc/security/pscexpert/bin/chusrattr` |

*ตารางที่ 7. การตั้งค่าที่เกี่ยวข้องกับมาตรฐานการปฏิบัติตามข้อกำหนด PCI DSS เวอร์ชัน 2.0 และเวอร์ชัน 3.0 (ต่อ)*

| การปรับใช้มาตรฐาน PCI DSS เหล่านี้ | ข้อมูลจำเพาะการนำไปปฏิบัติ | การปรับใช้ AIX Security Expert | ตำแหน่งของสคริปต์ที่แก้ไขค่า |
|---|---|---|---|
| 2.1 | เปลี่ยนค่าดีฟอลต์ที่กำหนดโดยผู้จำหน่ายเสมอก่อน การติดตั้งระบบบนเครือข่าย ตัวอย่างเช่น สตริงชุมชนของโปรโตคอลการจัดการเครือข่ายพื้นฐาน รวมถึงรหัสผ่าน และลบ บัญชีที่ไม่จำเป็นออก | ตั้งค่าจำนวนสัปดาห์ที่แอคเคาต์ซึ่งมีรหัสผ่านหมดอายุยังคงอยู่ในระบบได้เป็น 8 สัปดาห์โดยการตั้งค่าพารามิเตอร์ `maxexpired` เป็นค่า 8 | `/etc/security/pscexpert/bin/chusrattr` |
| **PCI เวอร์ชัน 2**<br>8.5.10<br>**PCI เวอร์ชัน 3**<br>8.2.3 | ต้องมีความยาวรหัสผ่านต่ำสุดอย่างน้อย 7 ตัวอักษร | ตั้งค่าความยาวรหัสผ่านขั้นต่ำเป็น 7 อักขระโดยการตั้งค่า พารามิเตอร์ `minlen` เป็นค่า 7 | `/etc/security/pscexpert/bin/chusrattr` |
| **PCI เวอร์ชัน 2**<br>8.5.11<br>**PCI เวอร์ชัน 3**<br>8.2.3 | ใช้รหัสผ่านที่มีทั้งตัวเลขและตัวอักษร | ตั้งค่าจำนวนอักขระแบบตัวอักษรขั้นต่ำที่ต้องการใน รหัสผ่านเป็น 1 การตั้งค่านี้ช่วยให้แน่ใจว่ารหัสผ่านมีอักขระแบบตัวอักษรโดยการตั้งค่าพารามิเตอร์ `minalpha` เป็นค่า 1 | `/etc/security/pscexpert/bin/chusrattr` |
| **PCI เวอร์ชัน 2**<br>8.5.11<br>**PCI เวอร์ชัน 3**<br>8.2.3 | ใช้รหัสผ่านที่มีทั้งตัวเลขและตัวอักษร | ตั้งค่าจำนวนอักขระที่ไม่ใช่ตัวอักษรขั้นต่ำที่ต้องการใน รหัสผ่านเป็น 1 การตั้งค่านี้ช่วยให้แน่ใจว่ารหัสผ่านมีอักขระที่ไม่ใช่ตัวอักษรโดยการตั้งค่าพารามิเตอร์ `minother` เป็นค่า 1 | `/etc/security/pscexpert/bin/chusrattr` |
| **PCI เวอร์ชัน 2**<br>2.1<br>**PCI เวอร์ชัน 3**<br>8.2.2 | เปลี่ยนค่าดีฟอลต์ที่กำหนดโดยผู้จำหน่ายเสมอก่อน การติดตั้งระบบบนเครือข่าย ตัวอย่างเช่น สตริงชุมชนของโปรโตคอลการจัดการเครือข่ายพื้นฐาน รวมถึงรหัสผ่าน และลบ บัญชีที่ไม่จำเป็นออก | ตั้งค่าจำนวนครั้งสูงสุดที่อักขระสามารถซ้ำได้ใน รหัสผ่านเป็น 8 โดยการตั้งค่าพารามิเตอร์ `maxrepeats` เป็นค่า 8 การตั้งค่านี้ บ่งชี้ว่าอักขระในรหัสผ่านสามารถซ้ำกันได้ไม่จำกัดจำนวนครั้งเมื่อ ตราบใดที่เป็นไปตามข้อจำกัดรหัสผ่านข้ออื่นๆ | `/etc/security/pscexpert/bin/chusrattr` |
| **PCI เวอร์ชัน 2**<br>8.5.12<br>**PCI เวอร์ชัน 3**<br>8.2.5 | ไม่อนุญาตให้แต่ละบุคคลส่งรหัสผ่านใหม่ ที่เป็นรหัสผ่านเดียวกับรหัสผ่านสี่ตัวที่ใช้ก่อนหน้านี้ | ตั้งค่าจำนวนสัปดาห์ก่อนที่จะสามารถใช้รหัสผ่านซ้ำได้เป็น 52 โดยการตั้งค่า พารามิเตอร์ `histexpire` เป็นค่า 52 | `/etc/security/pscexpert/bin/chusrattr` |
| **PCI เวอร์ชัน 2**<br>8.5.12<br>**PCI เวอร์ชัน 3**<br>8.2.5 | ไม่อนุญาตให้แต่ละบุคคลส่งรหัสผ่านใหม่ ที่เป็นรหัสผ่านเดียวกับรหัสผ่านสี่ตัวที่ใช้ก่อนหน้านี้ | ตั้งค่าจำนวนรหัสผ่านก่อนหน้าที่คุณไม่สามารถนำมาใช้อีกได้เป็น 4 โดยการตั้งค่า พารามิเตอร์ `histsize` เป็นค่า 4 | `/etc/security/pscexpert/bin/chusrattr` |

*ตารางที่ 7. การตั้งค่าที่เกี่ยวข้องกับมาตรฐานการปฏิบัติตามข้อกำหนด PCI DSS เวอร์ชัน 2.0 และเวอร์ชัน 3.0 (ต่อ)*

| การปรับใช้มาตรฐาน PCI DSS เหล่านี้ | ข้อมูลจำเพาะการนำไปปฏิบัติ | การปรับใช้ AIX Security Expert | ตำแหน่งของสคริปต์ที่แก้ไขค่า |
|---|---|---|---|
| **PCI เวอร์ชัน 2**<br>8.5.13<br>**PCI เวอร์ชัน 3**<br>10.2.4 | จำกัดความพยายามในการเข้าถึงซ้ำโดยการล็อก ID ผู้ใช้หลังจากการพยายามเข้าถึงที่ไม่สำเร็จ 6 ครั้ง | ตั้งค่าจำนวนของความพยายามในการล็อกอินที่ไม่สำเร็จต่อเนื่องกันที่ปิดใช้งาน แอคเคาต์เท่ากับ 6 ครั้ง สำหรับแต่ละบัญชีที่ไม่ใช่ root โดยการตั้งค่าพารามิเตอร์ `loginentries` เป็นค่า 6 | `/etc/security/pscexpert/bin/chusrattr` |
| **PCI เวอร์ชัน 2**<br>8.5.13<br>**PCI เวอร์ชัน 3**<br>10.2.4 | จำกัดความพยายามในการเข้าถึงซ้ำโดยการล็อก ID ผู้ใช้หลังจากการพยายามเข้าถึงที่ไม่สำเร็จ 6 ครั้ง | ตั้งค่าจำนวนครั้งการพยายามล็อกอินที่ไม่สำเร็จติดต่อกันที่ปิดใช้งานพอร์ตเป็น 6 ครั้งโดยการตั้งค่าพารามิเตอร์ `logindisable` เป็นค่า 6 | • `/etc/security/pscexpert/bin/chdefstanza`<br>• `/etc/security/login.cfg` |
| **PCI เวอร์ชัน 2**<br>8.5.14<br>**PCI เวอร์ชัน 3**<br>10.2.4 | ตั้งค่าช่วงเวลาการล็อกเท่ากับ 30 นาที หรือจนกว่า ผู้ดูแลระบบจะเปิดใช้ ID ผู้ใช้ใหม่อีกครั้ง | ตั้งค่าช่วงเวลาที่พอร์ตถูกล็อกหลังจากถูกปิดใช้งานโดย แอ็ตทริบิวต์ *logindisable* เป็น 30 นาทีโดยการตั้งคา พารามิเตอร์ `loginreenable` เป็นค่า 30 | • `/etc/security/pscexpert/bin/chdefstanza`<br>• `/etc/security/login.cfg` |
| 12.3.9 | เปิดใช้งานเทคโนโลยีการเข้าถึงแบบรีโมทสำหรับ ผู้จำหน่ายและหุ้นส่วนทางธุรกิจเฉพาะเมื่อจำเป็นต้องใช้โดยผู้จำหน่ายและหุ้นส่วน ทางธุรกิจ และปิดใช้งานทันทีหลังจากใช้ | ปิดใช้งานฟังก์ชันการล็อกอินรูทแบบรีโมทโดยการตั้งค่า เป็น False ผู้ดูแลระบบสามารถเปิดใช้งานฟังก์ชันการล็อกอิน แบบรีโมทเมื่อต้องการ จากนั้นให้ปิดใช้งานเมื่องาน เสร็จสมบูรณ์ | • `/etc/security/pscexpert/bin/chuserstanza`<br>• `/etc/security/user` |
| 8.1 | กำหนด ID เฉพาะให้กับผู้ใช้ทั้งหมดก่อนที่จะอนุญาต ให้สามารถเข้าถึงคอมโพเนนต์ระบบหรือข้อมูลของผู้ถือบัตร | เปิดใช้งานฟังก์ชันโดยแน่ใจว่าผู้ใช้ทั้งหมด มีชื่อผู้ใช้ที่ไม่ซ้ำกันก่อนที่จะสามารถเข้าถึงคอมโพเนนต์ระบบ หรือ ข้อมูลผู้ถือบัตรโดยการตั้งค่าฟังก์ชันนั้นให้มีค่าเป็น True | • `/etc/security/pscexpert/bin/chuserstanza`<br>• `/etc/security/user` |
| 10.2 | เปิดใช้งานการตรวจสอบบนระบบ | เปิดใช้งานการตรวจสอบไฟล์ไลบรารีบน ระบบ | `/etc/security/pscexpert/bin/pciaudit` |
| **PCI เวอร์ชัน 2**<br>1.1.5<br>2.2.2<br>**PCI เวอร์ชัน 3**<br>2.2.2 | ปิดใช้งานเซอร์วิสที่ไม่จำเป็นและที่ไม่ปลอดภัย ซึ่งรวมถึง `lpd` daemon | หยุด `lpd` daemon และคอมเม้นต์รายการที่เกี่ยวข้องในไฟล์ `/etc/inittab` ที่สตาร์ท daemon โดยอัตโนมัติ | `/etc/security/pscexpert/bin/comntrows` |
| **PCI เวอร์ชัน 2**<br>1.1.5<br>2.2.2<br>**PCI เวอร์ชัน 3**<br>2.2.2 | ปิดใช้งานเซอร์วิสที่ไม่ปลอดภัย และเซอร์วิสที่ไม่จำเป็น ซึ่งรวมถึง Common Desktop Environment (CDE) | ปิดใช้งานฟังก์ชัน CDE เมื่อ layer four traceroute (LFT) ไม่ถูกกำหนดค่าคอนฟิกไว้ | `/etc/security/pscexpert/bin/comntrows` |

*ตารางที่ 7. การตั้งค่าที่เกี่ยวข้องกับมาตรฐานการปฏิบัติตามข้อกำหนด PCI DSS เวอร์ชัน 2.0 และเวอร์ชัน 3.0 (ต่อ)*

| การปรับใช้มาตรฐาน PCI DSS เหล่านี้ | ข้อมูลจำเพาะการนำไปปฏิบัติ | การปรับใช้ AIX Security Expert | ตำแหน่งของสคริปต์ที่แก้ไขค่า |
|---|---|---|---|
| **PCI เวอร์ชัน 2**<br>1.1.5<br>2.2.2<br>**PCI เวอร์ชัน 3**<br>2.2.2 | ปิดใช้งานเซอร์วิสที่ไม่ปลอดภัย และเซอร์วิสที่ไม่จำเป็น ซึ่งรวมถึง timed daemon | หยุด timed daemon และ คอมเม้นต์รายการที่เกี่ยวข้องในไฟล์ /etc/rc.tcpip ที่สตาร์ท daemon โดยอัตโนมัติ | /etc/security/pscexpert/bin/rctcpip |
| **PCI เวอร์ชัน 2**<br>1.1.5<br>2.2.2<br>**PCI เวอร์ชัน 3**<br>2.2.2 | ปิดใช้งานเซอร์วิสที่ไม่จำเป็น และที่ไม่ปลอดภัย ซึ่งรวมถึง NTP daemon | หยุด NTP daemon และคอมเม้นต์รายการที่เกี่ยวข้องในไฟล์ /etc/rc.tcpip ที่สตาร์ท daemon โดยอัตโนมัติ | /etc/security/pscexpert/bin/rctcpip |
| **PCI เวอร์ชัน 2**<br>1.1.5<br>2.2.2<br>**PCI เวอร์ชัน 3**<br>2.2.2 | ปิดใช้งานเซอร์วิสที่ไม่จำเป็น และที่ไม่ปลอดภัย ซึ่งรวมถึง rwhod daemon | หยุด rwhod daemon และ คอมเม้นต์รายการที่เกี่ยวข้องในไฟล์ /etc/rc.tcpip ที่สตาร์ท daemon โดยอัตโนมัติ | /etc/security/pscexpert/bin/rctcpip |
| **PCI เวอร์ชัน 2**<br>2.1<br>**PCI เวอร์ชัน 3**<br>2.1.1 | เปลี่ยนค่าดีฟอลต์ที่กำหนดโดยผู้จำหน่ายก่อนการติดตั้ง ระบบบนเครือข่าย ซึ่งรวมถึงการปิดใช้งาน SNMP daemon | หยุด SNMP daemon และคอมเม้นต์รายการที่เกี่ยวข้องในไฟล์ /etc/rc.tcpip ที่สตาร์ท daemon โดยอัตโนมัติ | /etc/security/pscexpert/bin/rctcpip |
| **PCI เวอร์ชัน 2**<br>2.1<br>**PCI เวอร์ชัน 3**<br>2.1.1 | เปลี่ยนค่าดีฟอลต์ที่กำหนดโดยผู้จำหน่ายก่อนการติดตั้ง ระบบบนเครือข่าย ซึ่งรวมถึงการปิดใช้งาน SNMPMIBD daemon | ปิดใช้งาน SNMPMIBD daemon โดยการใส่เครื่องหมายข้อคิดเห็น รายการที่เกี่ยวข้องในไฟล์ /etc/rc.tcpip ที่เริ่มทำงาน daemon โดยอัตโนมัติ | /etc/security/pscexpert/bin/rctcpip |
| 2.1 | เปลี่ยนค่าดีฟอลต์ที่กำหนดโดยผู้จำหน่ายก่อนการติดตั้ง ระบบบนเครือข่าย ซึ่งรวมถึงการปิดใช้งาน AIXMIBD daemon | ปิดใช้งาน AIXMIBD daemon โดยการใส่เครื่องหมายข้อคิดเห็น รายการที่เกี่ยวข้องในไฟล์ /etc/rc.tcpip ที่เริ่มทำงาน daemon โดยอัตโนมัติ | /etc/security/pscexpert/bin/rctcpip |
| 2.1 | เปลี่ยนค่าดีฟอลต์ที่กำหนดโดยผู้จำหน่ายก่อนการติดตั้ง ระบบบนเครือข่าย ซึ่งรวมถึงการปิดใช้งาน HOSTMIBD daemon | ปิดใช้งาน HOSTMIBD daemon โดยการใส่เครื่องหมายข้อคิดเห็น รายการที่เกี่ยวข้องในไฟล์ /etc/rc.tcpip ที่เริ่มทำงาน daemon โดยอัตโนมัติ | /etc/security/pscexpert/bin/rctcpip |

*ตารางที่ 7. การตั้งค่าที่เกี่ยวข้องกับมาตรฐานการปฏิบัติตามข้อกำหนด PCI DSS เวอร์ชัน 2.0 และเวอร์ชัน 3.0 (ต่อ)*

| การปรับใช้มาตรฐาน PCI DSS เหล่านี้ | ข้อมูลจำเพาะการนำไปปฏิบัติ | การปรับใช้ AIX Security Expert | ตำแหน่งของสคริปต์ที่แก้ไขค่า |
|---|---|---|---|
| **PCI เวอร์ชัน 2**<br>1.1.5<br>2.2.2<br>**PCI เวอร์ชัน 3**<br>2.2.2 | ปิดใช้งานเซอร์วิสที่ไม่ปลอดภัย และเซอร์วิสที่ไม่จำเป็น ซึ่งรวมถึง DPID2 daemon | หยุด DPID2 daemon และ คอมเม้นต์รายการที่เกี่ยวข้องในไฟล์ /etc/rc.tcpip ที่สตาร์ท daemon โดยอัตโนมัติ | /etc/security/pscexpert/bin/rctcpip |
| **PCI เวอร์ชัน 2**<br>2.1<br>**PCI เวอร์ชัน 3**<br>2.2.2 | เปลี่ยนค่าดีฟอลต์ที่กำหนดโดยผู้จำหน่ายก่อนการติดตั้ง ระบบบนเครือข่าย ซึ่งรวมถึงการหยุดเซิร์ฟเวอร์ DHCP | ปิดใช้งานเซิร์ฟเวอร์ DHCP | /etc/security/pscexpert/bin/rctcpip |
| **PCI เวอร์ชัน 2**<br>1.1.5<br>2.2.2<br>**PCI เวอร์ชัน 3**<br>2.2.2 | ปิดใช้งานเซอร์วิสที่ไม่ปลอดภัย และเซอร์วิสที่ไม่จำเป็น ซึ่งรวมถึง เอเจนต์ DHCP | หยุดและปิดใช้งานเอเจนต์รีเลย์ DHCP และคอมเม้นต์รายการที่เกี่ยวข้องในไฟล์ /etc/rc.tcpip ที่สตาร์ทเอเจนต์โดยอัตโนมัติ | /etc/security/pscexpert/bin/rctcpip |
| **PCI เวอร์ชัน 2**<br>1.1.5<br>2.2.2<br>**PCI เวอร์ชัน 3**<br>2.2.2 | ปิดใช้งานเซอร์วิสที่ไม่จำเป็น และที่ไม่ปลอดภัย ซึ่งรวมถึง rshd daemon | หยุดและปิดใช้งานอินสแตนซ์ทั้งหมดของ rshd daemon และ เซอร์วิสเชลล์ และใส่เครื่องหมายข้อคิดเห็นรายการที่เกี่ยวข้องในไฟล์ /etc/inetd.conf ที่เริ่มทำงานอินสแตนซ์โดยอัตโนมัติ | /etc/security/pscexpert/bin/cominetdconf |
| **PCI เวอร์ชัน 2**<br>1.1.5<br>2.2.2<br>**PCI เวอร์ชัน 3**<br>2.2.2 | ปิดใช้งานเซอร์วิสที่ไม่ปลอดภัย และเซอร์วิสที่ไม่จำเป็น ซึ่งรวมถึง rlogind daemon | หยุดและปิดใช้งานอินสแตนซ์ทั้งหมดของ rlogind daemon และ เซอร์วิส rlogin ยูทิลิตี้ AIX Security Expert ยังคอมเม้นต์รายการที่เกี่ยวข้องในไฟล์ /etc/inetd.conf ที่สตาร์ทอินสแตนซ์โดยอัตโนมัติ | /etc/security/pscexpert/bin/cominetdconf |
| **PCI เวอร์ชัน 2**<br>1.1.5<br>2.2.2<br>**PCI เวอร์ชัน 3**<br>2.2.2 | ปิดใช้งานเซอร์วิสที่ไม่จำเป็น และที่ไม่ปลอดภัย ซึ่งรวมถึง rexecd daemon | หยุดและปิดใช้งานอินสแตนซ์ทั้งหมดของ rexecd daemon ยูทิลิตี้ AIX Security Expert ยังคอมเม้นต์รายการที่เกี่ยวข้อง ในไฟล์ /etc/inetd.conf ที่สตาร์ท daemon โดยอัตโนมัติ | /etc/security/pscexpert/bin/cominetdconf |

*ตารางที่ 7. การตั้งค่าที่เกี่ยวข้องกับมาตรฐานการปฏิบัติตามข้อกำหนด PCI DSS เวอร์ชัน 2.0 และเวอร์ชัน 3.0 (ต่อ)*

| การปรับใช้มาตรฐาน PCI DSS เหล่านี้ | ข้อมูลจำเพาะการนำไปปฏิบัติ | การปรับใช้ AIX Security Expert | ตำแหน่งของสคริปต์ที่แก้ไขค่า |
|---|---|---|---|
| **PCI เวอร์ชัน 2**<br>1.1.5<br>2.2.2<br>**PCI เวอร์ชัน 3**<br>2.2.2 | ปิดใช้งานเซอร์วิสที่ไม่ปลอดภัย และเซอร์วิสที่ไม่จำเป็น ซึ่งรวมถึง comsat daemon | หยุดและปิดใช้งานอินสแตนซ์ทั้งหมดของ comsat daemon ยูทิลิตี้ AIX Security Expert ยังคอมเม้นต์รายการที่เกี่ยวข้อง ในไฟล์ /etc/inetd.conf ที่สตาร์ท daemon โดยอัตโนมัติ | /etc/security/pscexpert/bin/cominetdconf |
| **PCI เวอร์ชัน 2**<br>1.1.5<br>2.2.2<br>**PCI เวอร์ชัน 3**<br>2.2.2 | ปิดใช้งานเซอร์วิสที่ไม่จำเป็น และที่ไม่ปลอดภัย ซึ่งรวมถึง fingerd daemon | หยุดและปิดใช้งานอินสแตนซ์ทั้งหมดของ fingerd daemon ยูทิลิตี้ AIX Security Expert ยังคอมเม้นต์รายการที่เกี่ยวข้อง ในไฟล์ /etc/inetd.conf ที่สตาร์ท daemon โดยอัตโนมัติ | /etc/security/pscexpert/bin/cominetdconf |
| **PCI เวอร์ชัน 2**<br>1.1.5<br>2.2.2<br>**PCI เวอร์ชัน 3**<br>2.2.2 | ปิดใช้งานเซอร์วิสที่ไม่ปลอดภัย และเซอร์วิสที่ไม่จำเป็น ซึ่งรวมถึง systat daemon | หยุดและปิดใช้งานอินสแตนซ์ทั้งหมดของ systat daemon ยูทิลิตี้ AIX Security Expert ยังคอมเม้นต์รายการที่เกี่ยวข้อง ในไฟล์ /etc/inetd.conf ที่สตาร์ท daemon โดยอัตโนมัติ | /etc/security/pscexpert/bin/cominetdconf |
| 2.1 | เปลี่ยนค่าดีฟอลต์ที่กำหนดโดยผู้จำหน่ายก่อนการติดตั้ง ระบบบนเครือข่าย ซึ่งรวมถึงการปิดใช้งานคำสั่ง netstat | ปิดใช้งานคำสั่ง netstat โดยการใส่เครื่องหมายข้อคิดเห็น รายการที่เกี่ยวข้องในไฟล์ /etc/inetd.conf | /etc/security/pscexpert/bin/cominetdconf |
| **PCI เวอร์ชัน 2**<br>1.1.5<br>2.2.2<br>**PCI เวอร์ชัน 3**<br>2.2.3 | ปิดใช้งานเซอร์วิสที่ไม่จำเป็น และที่ไม่ปลอดภัย ซึ่งรวมถึง tftp daemon | หยุดและปิดใช้งานอินสแตนซ์ทั้งหมดของ tftp daemon ยูทิลิตี้ AIX Security Expert ยังคอมเม้นต์รายการที่เกี่ยวข้อง ในไฟล์ /etc/inetd.conf ที่สตาร์ท daemon โดยอัตโนมัติ | /etc/security/pscexpert/bin/cominetdconf |
| **PCI เวอร์ชัน 2**<br>1.1.5<br>2.2.2<br>**PCI เวอร์ชัน 3**<br>2.2.2 | ปิดใช้งานเซอร์วิสที่ไม่ปลอดภัย และเซอร์วิสที่ไม่จำเป็น ซึ่งรวมถึง talkd daemon | หยุดและปิดใช้งานอินสแตนซ์ทั้งหมดของ talkd daemon ยูทิลิตี้ AIX Security Expert ยังคอมเม้นต์รายการที่เกี่ยวข้อง ในไฟล์ /etc/inetd.conf ที่สตาร์ท daemon โดยอัตโนมัติ | /etc/security/pscexpert/bin/cominetdconf |
| **PCI เวอร์ชัน 2**<br>1.1.5<br>2.2.2<br>**PCI เวอร์ชัน 3**<br>2.2.2 | ปิดใช้งานเซอร์วิสที่ไม่จำเป็น และที่ไม่ปลอดภัย ซึ่งรวมถึง rquotad daemon | หยุดและปิดใช้งานอินสแตนซ์ทั้งหมดของ rquotad daemon ยูทิลิตี้ AIX Security Expert ยังคอมเม้นต์รายการที่เกี่ยวข้อง ในไฟล์ /etc/inetd.conf ที่สตาร์ท daemon โดยอัตโนมัติ | /etc/security/pscexpert/bin/cominetdconf |

*ตารางที่ 7. การตั้งค่าที่เกี่ยวข้องกับมาตรฐานการปฏิบัติตามข้อกำหนด PCI DSS เวอร์ชัน 2.0 และเวอร์ชัน 3.0 (ต่อ)*

| การปรับใช้มาตรฐาน PCI DSS เหล่านี้ | ข้อมูลจำเพาะการนำไปปฏิบัติ | การปรับใช้ AIX Security Expert | ตำแหน่งของสคริปต์ที่แก้ไขค่า |
|---|---|---|---|
| **PCI เวอร์ชัน 2**<br>1.1.5<br>2.2.2<br>**PCI เวอร์ชัน 3**<br>2.2.2 | ปิดใช้งานเซอร์วิสที่ไม่ปลอดภัย และเซอร์วิสที่ไม่จำเป็น ซึ่งรวมถึง rstatd daemon | หยุดและปิดใช้งานอินสแตนซ์ทั้งหมดของ rstatd daemon ยูทิลิตี้ AIX Security Expert ยังคอมเม้นต์รายการที่เกี่ยวข้อง ในไฟล์ /etc/inetd.conf ที่สตาร์ท daemon โดยอัตโนมัติ | /etc/security/pscexpert/bin/cominetdconf |
| **PCI เวอร์ชัน 2**<br>1.1.5<br>2.2.2<br>**PCI เวอร์ชัน 3**<br>2.2.2 | ปิดใช้งานเซอร์วิสที่ไม่จำเป็น และที่ไม่ปลอดภัย ซึ่งรวมถึง rusersd daemon | หยุดและปิดใช้งานอินสแตนซ์ทั้งหมดของ rusersd daemon ยูทิลิตี้ AIX Security Expert ยังคอมเม้นต์รายการที่เกี่ยวข้อง ในไฟล์ /etc/inetd.conf ที่สตาร์ท daemon โดยอัตโนมัติ | /etc/security/pscexpert/bin/cominetdconf |
| **PCI เวอร์ชัน 2**<br>1.1.5<br>2.2.2<br>**PCI เวอร์ชัน 3**<br>2.2.2 | ปิดใช้งานเซอร์วิสที่ไม่ปลอดภัย และเซอร์วิสที่ไม่จำเป็น ซึ่งรวมถึง rwalld daemon | หยุดและปิดใช้งานอินสแตนซ์ทั้งหมดของ rwalld daemon ยูทิลิตี้ AIX Security Expert ยังคอมเม้นต์รายการที่เกี่ยวข้อง ในไฟล์ /etc/inetd.conf ที่สตาร์ท daemon โดยอัตโนมัติ | /etc/security/pscexpert/bin/cominetdconf |
| **PCI เวอร์ชัน 2**<br>1.1.5<br>2.2.2<br>**PCI เวอร์ชัน 3**<br>2.2.2 | ปิดใช้งานเซอร์วิสที่ไม่จำเป็น และที่ไม่ปลอดภัย ซึ่งรวมถึง sprayd daemon | หยุดและปิดใช้งานอินสแตนซ์ทั้งหมดของ sprayd daemon ยูทิลิตี้ AIX Security Expert ยังคอมเม้นต์รายการที่เกี่ยวข้อง ในไฟล์ /etc/inetd.conf ที่สตาร์ท daemon โดยอัตโนมัติ | /etc/security/pscexpert/bin/cominetdconf |
| **PCI เวอร์ชัน 2**<br>1.1.5<br>2.2.2<br>**PCI เวอร์ชัน 3**<br>2.2.2 | ปิดใช้งานเซอร์วิสที่ไม่ปลอดภัย และเซอร์วิสที่ไม่จำเป็น ซึ่งรวมถึง pcnfsd daemon | หยุดและปิดใช้งานอินสแตนซ์ทั้งหมดของ pcnfsd daemon ยูทิลิตี้ AIX Security Expert ยังคอมเม้นต์รายการที่เกี่ยวข้อง ในไฟล์ /etc/inetd.conf ที่สตาร์ท daemon โดยอัตโนมัติ | /etc/security/pscexpert/bin/cominetdconf |
| **PCI เวอร์ชัน 2**<br>1.1.5<br>2.2.2<br>**PCI เวอร์ชัน 3**<br>2.2.2 | ปิดใช้งานเซอร์วิสที่ไม่ปลอดภัย และเซอร์วิสที่ไม่จำเป็น ซึ่งรวมถึงเซอร์วิส TCP echo | หยุดและปิดใช้งานอินสแตนซ์ทั้งหมดของเซอร์วิส echo(tcp) ยูทิลิตี้ AIX Security Expert ยังคอมเม้นต์รายการที่เกี่ยวข้อง ในไฟล์ /etc/inetd.conf ที่สตาร์ท เซอร์วิสโดยอัตโนมัติ | /etc/security/pscexpert/bin/cominetdconf |

*ตารางที่ 7. การตั้งค่าที่เกี่ยวข้องกับมาตรฐานการปฏิบัติตามข้อกำหนด PCI DSS เวอร์ชัน 2.0 และเวอร์ชัน 3.0 (ต่อ)*

| การปรับใช้มาตรฐาน PCI DSS เหล่านี้ | ข้อมูลจำเพาะการนำไปปฏิบัติ | การปรับใช้ AIX Security Expert | ตำแหน่งของสคริปต์ที่แก้ไขค่า |
|---|---|---|---|
| **PCI เวอร์ชัน 2**<br>1.1.5<br>2.2.2<br>**PCI เวอร์ชัน 3**<br>2.2.2 | ปิดใช้งานเซอร์วิสที่ไม่ปลอดภัย และเซอร์วิสที่ไม่จำเป็น ซึ่งรวมถึงเซอร์วิส TCP discard | หยุดและปิดใช้งานอินสแตนซ์ทั้งหมดของเซอร์วิส discard(tcp) ยูทิลิตี้ AIX Security Expert ยังคอมเม้นต์รายการที่เกี่ยวข้อง ในไฟล์ /etc/inetd.conf ที่สตาร์ท เซอร์วิสโดยอัตโนมัติ | /etc/security/pscexpert/bin/cominetdconf |
| **PCI เวอร์ชัน 2**<br>1.1.5<br>2.2.2<br>**PCI เวอร์ชัน 3**<br>2.2.2 | ปิดใช้งานเซอร์วิสที่ไม่ปลอดภัย และเซอร์วิสที่ไม่จำเป็น ซึ่งรวมถึงเซอร์วิส TCP chargen | หยุดและปิดใช้งานอินสแตนซ์ทั้งหมดของเซอร์วิส chargen(tcp) ยูทิลิตี้ AIX Security Expert ยังคอมเม้นต์รายการที่เกี่ยวข้อง ในไฟล์ /etc/inetd.conf ที่สตาร์ท เซอร์วิสโดยอัตโนมัติ | /etc/security/pscexpert/bin/cominetdconf |
| **PCI เวอร์ชัน 2**<br>1.1.5<br>2.2.2<br>**PCI เวอร์ชัน 3**<br>2.2.2 | ปิดใช้งานเซอร์วิสที่ไม่ปลอดภัย และเซอร์วิสที่ไม่จำเป็น ซึ่งรวมถึงเซอร์วิส TCP daytime | หยุดและปิดใช้งานอินสแตนซ์ทั้งหมดของเซอร์วิส daytime(tcp) ยูทิลิตี้ AIX Security Expert ยังคอมเม้นต์รายการที่เกี่ยวข้อง ในไฟล์ /etc/inetd.conf ที่สตาร์ท เซอร์วิสโดยอัตโนมัติ | /etc/security/pscexpert/bin/cominetdconf |
| **PCI เวอร์ชัน 2**<br>1.1.5<br>2.2.2<br>**PCI เวอร์ชัน 3**<br>2.2.2 | ปิดใช้งานเซอร์วิสที่ไม่ปลอดภัย และเซอร์วิสที่ไม่จำเป็น ซึ่งรวมถึงเซอร์วิส TCP time | หยุดและปิดใช้งานอินสแตนซ์ทั้งหมดของเซอร์วิส timed(tcp) ยูทิลิตี้ AIX Security Expert ยังคอมเม้นต์รายการที่เกี่ยวข้อง ในไฟล์ /etc/inetd.conf ที่สตาร์ท เซอร์วิสโดยอัตโนมัติ | /etc/security/pscexpert/bin/cominetdconf |
| **PCI เวอร์ชัน 2**<br>1.1.5<br>2.2.2<br>**PCI เวอร์ชัน 3**<br>2.2.2 | ปิดใช้งานเซอร์วิสที่ไม่ปลอดภัย และเซอร์วิสที่ไม่จำเป็น ซึ่งรวมถึงเซอร์วิส UDP echo | หยุดและปิดใช้งานอินสแตนซ์ทั้งหมดของเซอร์วิส echo(udp) ยูทิลิตี้ AIX Security Expert ยังคอมเม้นต์รายการที่เกี่ยวข้อง ในไฟล์ /etc/inetd.conf ที่สตาร์ท เซอร์วิสโดยอัตโนมัติ | /etc/security/pscexpert/bin/cominetdconf |
| **PCI เวอร์ชัน 2**<br>1.1.5<br>2.2.2<br>**PCI เวอร์ชัน 3**<br>2.2.2 | ปิดใช้งานเซอร์วิสที่ไม่ปลอดภัย และเซอร์วิสที่ไม่จำเป็น ซึ่งรวมถึงเซอร์วิส UDP discard | หยุดและปิดใช้งานอินสแตนซ์ทั้งหมดของเซอร์วิส discard(udp) ยูทิลิตี้ AIX Security Expert ยังคอมเม้นต์รายการที่เกี่ยวข้อง ในไฟล์ /etc/inetd.conf ที่สตาร์ท เซอร์วิสโดยอัตโนมัติ | /etc/security/pscexpert/bin/cominetdconf |

*ตารางที่ 7. การตั้งค่าที่เกี่ยวข้องกับมาตรฐานการปฏิบัติตามข้อกำหนด PCI DSS เวอร์ชัน 2.0 และเวอร์ชัน 3.0 (ต่อ)*

| การปรับใช้มาตรฐาน PCI DSS เหล่านี้ | ข้อมูลจำเพาะการนำไปปฏิบัติ | การปรับใช้ AIX Security Expert | ตำแหน่งของสคริปต์ที่แก้ไขค่า |
|---|---|---|---|
| **PCI เวอร์ชัน 2**<br>1.1.5<br>2.2.2<br>**PCI เวอร์ชัน 3**<br>2.2.2 | ปิดใช้งานเซอร์วิสที่ไม่ปลอดภัย และเซอร์วิสที่ไม่จำเป็น ซึ่งรวมถึงเซอร์วิส UDP chargen | หยุดและปิดใช้งานอินสแตนซ์ทั้งหมดของเซอร์วิส chargen(udp) ยูทิลิตี้ AIX Security Expert ยังคอมเม้นต์รายการที่เกี่ยวข้อง ในไฟล์ /etc/inetd.conf ที่สตาร์ท เซอร์วิสโดยอัตโนมัติ | /etc/security/pscexpert/bin/cominetdconf |
| **PCI เวอร์ชัน 2**<br>1.1.5<br>2.2.2<br>**PCI เวอร์ชัน 3**<br>2.2.2 | ปิดใช้งานเซอร์วิสที่ไม่ปลอดภัย และเซอร์วิสที่ไม่จำเป็น ซึ่งรวมถึงเซอร์วิส UDP daytime | หยุดและปิดใช้งานอินสแตนซ์ทั้งหมดของเซอร์วิส daytime(udp) ยูทิลิตี้ AIX Security Expert ยังคอมเม้นต์รายการที่เกี่ยวข้อง ในไฟล์ /etc/inetd.conf ที่สตาร์ท เซอร์วิสโดยอัตโนมัติ | /etc/security/pscexpert/bin/cominetdconf |
| **PCI เวอร์ชัน 2**<br>1.1.5<br>2.2.2<br>**PCI เวอร์ชัน 3**<br>2.2.2 | ปิดใช้งานเซอร์วิสที่ไม่ปลอดภัย และเซอร์วิสที่ไม่จำเป็น ซึ่งรวมถึงเซอร์วิส UDP time | หยุดและปิดใช้งานอินสแตนซ์ทั้งหมดของเซอร์วิส timed(udp) ยูทิลิตี้ AIX Security Expert ยังคอมเม้นต์รายการที่เกี่ยวข้อง ในไฟล์ /etc/inetd.conf ที่สตาร์ท เซอร์วิสโดยอัตโนมัติ | /etc/security/pscexpert/bin/cominetdconf |
| **PCI เวอร์ชัน 2**<br>1.1.5<br>2.2.2<br>**PCI เวอร์ชัน 3**<br>2.2.3 | ปิดใช้งานเซอร์วิสที่ไม่ปลอดภัย และเซอร์วิสที่ไม่จำเป็น ซึ่งรวมถึงเซอร์วิส FTP | หยุดและปิดใช้งานอินสแตนซ์ทั้งหมดของ ftpd daemon ยูทิลิตี้ AIX Security Expert ยังคอมเม้นต์รายการที่เกี่ยวข้อง ในไฟล์ /etc/inetd.conf ที่สตาร์ท daemon โดยอัตโนมัติ | /etc/security/pscexpert/bin/cominetdconf |
| **PCI เวอร์ชัน 2**<br>1.1.5<br>2.2.2<br>**PCI เวอร์ชัน 3**<br>2.2.3 | ปิดใช้งานเซอร์วิสที่ไม่ปลอดภัย และเซอร์วิสที่ไม่จำเป็น ซึ่งรวมถึงเซอร์วิส telnet | หยุดและปิดใช้งานอินสแตนซ์ทั้งหมดของ telnetd daemon ยูทิลิตี้ AIX Security Expert ยังคอมเม้นต์รายการที่เกี่ยวข้อง ในไฟล์ /etc/inetd.conf ที่สตาร์ท daemon โดยอัตโนมัติ | /etc/security/pscexpert/bin/cominetdconf |
| **PCI เวอร์ชัน 2**<br>1.1.5<br>2.2.2<br>**PCI เวอร์ชัน 3**<br>2.2.2 | ปิดใช้งานเซอร์วิสที่ไม่ปลอดภัย และเซอร์วิสที่ไม่จำเป็น ซึ่งรวมถึง dtspc | หยุดและปิดใช้งานอินสแตนซ์ทั้งหมดของ dtspc daemon ยูทิลิตี้ AIX Security Expert ยังคอมเม้นต์รายการที่เกี่ยวข้องในไฟล์ /etc/inittab ที่สตาร์ท daemon โดยอัตโนมัติ เมื่อ LFT ไม่ถูกกำหนดค่าคอนฟิกไว้ และ CDE ถูกปิดใช้งานในไฟล์ /etc/inittab | /etc/security/pscexpert/bin/cominetdconf |

*ตารางที่ 7. การตั้งค่าที่เกี่ยวข้องกับมาตรฐานการปฏิบัติตามข้อกำหนด PCI DSS เวอร์ชัน 2.0 และเวอร์ชัน 3.0 (ต่อ)*

| การปรับใช้มาตรฐาน PCI DSS เหล่านี้ | ข้อมูลจำเพาะการนำไปปฏิบัติ | การปรับใช้ AIX Security Expert | ตำแหน่งของสคริปต์ที่แก้ไขค่า |
|---|---|---|---|
| **PCI เวอร์ชัน 2**<br>1.1.5<br>2.2.2<br>**PCI เวอร์ชัน 3**<br>2.2.2 | ปิดใช้งานเซอร์วิสที่ไม่ปลอดภัย และเซอร์วิสที่ไม่จำเป็น ซึ่งรวมถึงเซอร์วิส `ttdbserver` | หยุดและปิดใช้งานอินสแตนซ์ทั้งหมดของเซอร์วิส `ttdbserver` ยูทิลิตี้ AIX Security Expert ยังคอมเม้นต์รายการที่เกี่ยวข้อง ในไฟล์ `/etc/inetd.conf` ที่สตาร์ท เซอร์วิสโดยอัตโนมัติ | `/etc/security/pscexpert/bin/cominetdconf` |
| **PCI เวอร์ชัน 2**<br>1.1.5<br>2.2.2<br>**PCI เวอร์ชัน 3**<br>2.2.2 | ปิดใช้งานเซอร์วิสที่ไม่ปลอดภัย และเซอร์วิสที่ไม่จำเป็น ซึ่งรวมถึงเซอร์วิส `cmsd` | หยุดและปิดใช้งานอินสแตนซ์ทั้งหมดของเซอร์วิส `cmsd` ยูทิลิตี้ AIX Security Expert ยังคอมเม้นต์รายการที่เกี่ยวข้อง ในไฟล์ `/etc/inetd.conf` ที่สตาร์ท เซอร์วิสโดยอัตโนมัติ | `/etc/security/pscexpert/bin/cominetdconf` |
| **PCI เวอร์ชัน 2**<br>2.2.3<br>**PCI เวอร์ชัน 3**<br>2.2.4 | กำหนดค่าคอนฟิกพารามิเตอร์การรักษาความปลอดภัยของระบบเพื่อป้องกัน ความผิดพลาด | ลบคำสั่ง Set User ID (SUID) โดยการใส่เครื่องหมายข้อคิดเห็นรายการที่เกี่ยวข้องในไฟล์ `/etc/inetd.conf` ที่เปิดดใช้งานคำสั่ง โดยอัตโนมัติ | `/etc/security/pscexpert/bin/rmsuidfrmrcmds` |
| **PCI เวอร์ชัน 2**<br>2.2.3<br>**PCI เวอร์ชัน 3**<br>2.2.4 | กำหนดค่าคอนฟิกพารามิเตอร์การรักษาความปลอดภัยของระบบเพื่อป้องกัน ความผิดพลาด | เปิดใช้ระดับการรักษาความปลอดภัยต่ำสุดสำหรับ File Permissions Manager | `/etc/security/pscexpert/bin/filepermgr` |
| **PCI เวอร์ชัน 2**<br>2.2.3<br>**PCI เวอร์ชัน 3**<br>2.2.4 | กำหนดค่าคอนฟิกพารามิเตอร์การรักษาความปลอดภัยของระบบเพื่อป้องกัน ความผิดพลาด | ปรับเปลี่ยนโปรโตคอล Network File System ด้วยค่าติดตั้งที่จำกัดซึ่งสอดคล้องกับข้อกำหนดด้านความปลอดภัย PCI ค่าติดตั้งที่จำกัดเหล่านี้ประกอบด้วยการปิดใช้งานการเข้าถึงแบบ roote แบบรีโมต และการเข้าถึง UID และ GID แบบไม่ระบุชื่อ | `/etc/security/pscexpert/bin/nfsconfig` |
| **PCI เวอร์ชัน 2**<br>2.2.2<br>**PCI เวอร์ชัน 3**<br>2.2.3 | เปิดใช้เฉพาะเซอร์วิสการรักษาความปลอดภัย และเซอร์วิสที่จำเป็น, โปรโตคอล, daemons และอื่นๆ ตามที่จำเป็นสำหรับการทำงานที่ถูกต้องของระบบ ปรับใช้คุณลักษณะการรักษาความปลอดภัยสำหรับเซอร์วิสที่จำเป็น โปรโตคอล หรือ daemons ที่ถือว่าไม่ปลอดภัย | ปิดใช้งาน `rlogind`, `rshd` และ `tftpd` daemons ซึ่งไม่ ปลอดภัย | `/etc/security/pscexpert/bin/disrmtdmns` |

*ตารางที่ 7. การตั้งค่าที่เกี่ยวข้องกับมาตรฐานการปฏิบัติตามข้อกำหนด PCI DSS เวอร์ชัน 2.0 และเวอร์ชัน 3.0 (ต่อ)*

| การปรับใช้มาตรฐาน PCI DSS เหล่านี้ | ข้อมูลจำเพาะการนำไปปฏิบัติ | การปรับใช้ AIX Security Expert | ตำแหน่งของสคริปต์ที่แก้ไขค่า |
|---|---|---|---|
| **PCI เวอร์ชัน 2**<br>2.2.2<br>**PCI เวอร์ชัน 3**<br>2.2.3 | เปิดใช้เฉพาะเซอร์วิสการรักษาความปลอดภัย และเซอร์วิสที่จำเป็น, โปรโตคอล, daemons และอื่นๆ ตามที่จำเป็นสำหรับการทำงานที่ถูกต้องของระบบ ปรับใช้คุณลักษณะการรักษาความปลอดภัยสำหรับเซอร์วิสที่จำเป็น โปรโตคอล หรือ daemons ที่ถือว่าไม่ปลอดภัย | ปิดใช้งาน `rlogind`, `rshd` และ `tftpd` daemons ซึ่งไม่ ปลอดภัย | `/etc/security/pscexpert/bin/rmrhostsnetrc` |
| **PCI เวอร์ชัน 2**<br>2.2.2<br>**PCI เวอร์ชัน 3**<br>2.2.3 | เปิดใช้เฉพาะเซอร์วิสการรักษาความปลอดภัย และเซอร์วิสที่จำเป็น, โปรโตคอล, daemons และอื่นๆ ตามที่จำเป็นสำหรับการทำงานที่ถูกต้องของระบบ ปรับใช้คุณลักษณะการรักษาความปลอดภัยสำหรับเซอร์วิสที่จำเป็น โปรโตคอล หรือ daemons ที่ถือว่าไม่ปลอดภัย | ปิดใช้งาน `logind`, `rshd` และ `tftpdpci_rmetchostsequiv` daemons, ซึ่งไม่ปลอดภัย | `/etc/security/pscexpert/bin/rmetchostsequiv` |
| **PCI เวอร์ชัน 2**<br>1.3.6<br>**PCI เวอร์ชัน 3**<br>2.2.3 | ใช้การตรวจสอบสถานะสัมพันธ์ หรือการกรองแพ็กเกจซึ่งมีเฉพาะการเชื่อมต่อที่สร้างขึ้นที่ได้รับอนุญาตบนเครือข่าย | เปิดใช้อ็อพชัน `clean_partial_conns` บนเครือข่ายโดยการตั้งค่าเป็น 1 | `/etc/security/pscexpert/bin/ntwkopts` |
| **PCI เวอร์ชัน 2**<br>2.2.2<br>**PCI เวอร์ชัน 3**<br>2.2.3 | ใช้การตรวจสอบสถานะสัมพันธ์ หรือการกรองแพ็กเกจซึ่งมีเฉพาะการเชื่อมต่อที่สร้างขึ้นที่ได้รับอนุญาตบนเครือข่าย | เปิดใช้การรักษาความปลอดภัย TCP โดยการตั้งค่าอ็อพชัน `tcp_tcpsecure` บนเครือข่ายให้มีค่าเท่ากับ 7 การตั้งค่านี้จะ ช่วยป้องกันการโจมตีข้อมูล, รีเซ็ต (RST), และคำขอการเชื่อมต่อ TCP (SYN) | `/etc/security/pscexpert/bin/ntwkopts` |
| 1.2 | ปกป้องการเข้าถึงที่ไม่ได้รับอนุญาตไปยังพอร์ตที่ไม่ได้ใช้งาน | กำหนดคอนฟิกระบบเพื่อหลบหลีกโฮสต์เป็นเวลา 5 นาทีเพื่อป้องกันระบบอื่นๆ ไม่ให้เข้าถึงพอร์ตที่ไม่ได้ใช้งาน | `/etc/security/pscexpert/bin/ipsecshunhosthls`<br>**หมายเหตุ:** คุณสามารถป้อนกฎการกรองเพิ่มเติมใน ไฟล์ `/etc/security/aixpert/bin/filter.txt` กฎนี้ถูกรวมไว้โดยสคริปต์ `ipsecshunhosthls.sh` เมื่อคุณใช้กับโปรไฟล์ รายการต่างๆ ควรอยู่ในรูปแบบ ต่อไปนี้:<br>*`port_number`*`:`*`ip_address`*`:`<br>*`action (การดำเนินการ)`*<br><br>โดยที่ ค่าที่อาจเกิดขึ้นได้สำหรับ *action* คือ `Allow` หรือ `Deny` |

*ตารางที่ 7. การตั้งค่าที่เกี่ยวข้องกับมาตรฐานการปฏิบัติตามข้อกำหนด PCI DSS เวอร์ชัน 2.0 และเวอร์ชัน 3.0 (ต่อ)*

| การปรับใช้มาตรฐาน PCI DSS เหล่านี้ | ข้อมูลจำเพาะการนำไปปฏิบัติ | การปรับใช้ AIX Security Expert | ตำแหน่งของสคริปต์ที่แก้ไขค่า |
|---|---|---|---|
| 1.2 | ปกป้องโฮสต์จากการสแกนพอร์ต | กำหนดคอนฟิกระบบเพื่อหลบหลีกพอร์ตที่มีช่องโหว่เป็นเวลา 5 นาที ซึ่งจะป้องกัน การสแกนพอร์ต | `/etc/security/pscexpert/bin/ipsecshunports`<br>**หมายเหตุ:** คุณสามารถป้อนกฎการกรองเพิ่มเติมใน ไฟล์ `/etc/security/aixpert/bin/filter.txt` กฎนี้ถูกรวมไว้โดยสคริปต์ `ipsecshunhosthls.sh` เมื่อคุณใช้กับโปรไฟล์ รายการต่างๆ ควรอยู่ในรูปแบบ ต่อไปนี้:<br>*port_number*:*ip_address*:*action (การดำเนินการ)*<br>โดยที่ ค่าที่อาจเกิดขึ้นได้สำหรับ *action* คือ `Allow` หรือ `Deny` |
| 1.2 | จำกัดสิทธิ์การสร้างอ็อบเจ็กต์ | ตั้งค่าสิทธิ์การสร้างอ็อบเจ็กต์ดีฟอลต์เป็น 22 โดยการตั้งค่า พารามิเตอร์ `umask` เป็นค่า 22 | `/etc/security/pscexpert/bin/chusrattr` |
| 1.2 | จำกัดการเข้าถึงระบบ | ตรวจสอบให้แน่ใจว่ามีเฉพาะ ID รูทที่แสดงใน ไฟล์ `cron.allow` และลบไฟล์ `cron.deny` ออกจาก ระบบ | `/etc/security/pscexpert/bin/limitsysacc` |
| 6.5.8 | ลบจุดออกจากพาธรูท | ลบจุดออกจากตัวแปรสภาพแวดล้อม PATH ในไฟล์ต่อไปนี้ที่อยู่ในโฮมไดเร็กทอรีรูท:<br>• .cshrc<br>• .kshrc<br>• .login<br>• .profile | `/etc/security/pscexpert/bin/rmdotfrmpathroot` |
| 6.5.8 | ลบจุดออกจากพาธที่ไม่ใช่รูท | ลบจุดออกจากตัวแปรสภาพแวดล้อม *PATH* ในไฟล์ต่อไปนี้ที่อยู่ในโฮมไดเร็กทอรี ของผู้ใช้:<br>• .cshrc<br>• .kshrc<br>• .login<br>• .profile | `/etc/security/pscexpert/bin/rmdotfrmpathnroot` |
| 2.2.3 | จำกัดการเข้าถึงระบบ | เพิ่มความสามารถของผู้ใช้รูท และชื่อผู้ใช้ในไฟล์ `/etc/ftpusers` | `/etc/security/pscexpert/bin/chetcftpusers` |
| 2.1 | ลบบัญชีเกสต์ | ลบบัญชีเกสต์ และไฟล์ออก | `/etc/security/pscexpert/bin/execmds` |
| 6.5.2 | ป้องการเรียกโปรแกรมในพื้นที่เนื้อหา | เปิดใช้คุณลักษณะปิดใช้งานการดำเนินการสแต็ก (SED) | `/etc/security/pscexpert/bin/sedconfig` |
| 8.2 | ตรวจสอบให้แน่ใจว่ารหัสผ่านสำหรับรูทมีความปลอดภัย | เริ่มต้นการตรวจสอบความสมบูรณ์รหัสผ่านรูท เพื่อให้แน่ใจว่ารหัสผ่านรูทมีความปลอดภัย | `/etc/security/pscexpert/bin/chuserstanza` |

*ตารางที่ 7. การตั้งค่าที่เกี่ยวข้องกับมาตรฐานการปฏิบัติตามข้อกำหนด PCI DSS เวอร์ชัน 2.0 และเวอร์ชัน 3.0 (ต่อ)*

| การปรับใช้มาตรฐาน PCI DSS เหล่านี้ | ข้อมูลจำเพาะการนำไปปฏิบัติ | การปรับใช้ AIX Security Expert | ตำแหน่งของสคริปต์ที่แก้ไขค่า |
|---|---|---|---|
| **PCI เวอร์ชัน 2**<br>8.5.15<br>**PCI เวอร์ชัน 3**<br>8.1.8 | จำกัดการเข้าถึงระบบโดยการตั้งค่าเวลาที่ไม่มีการทำงานเซสชัน | ตั้งค่าจำกัดเวลาที่ไม่ทำงานเท่ากับ 15 นาที หาก เซสชันไม่ทำงานนานมากกว่า 15 นาที คุณต้องป้อนรหัสผ่านใหม่อีกครั้ง | `/etc/security/pscexpert/bin/autologoff` |
| 1.3.5 | จำกัดทราฟฟิกการเข้าถึงข้อมูลผู้ถือบัตร | ตั้งค่าข้อบังคับด้านทราฟฟิกของ TCP ไปที่การตั้งค่า สูงสุด ซึ่งจะแก้ไขผลกระทบจากการโจมตี DDoS บนพอร์ต | `/etc/security/pscexpert/bin/tcptr_pscexpert` |
| 1.3.5 | รักษาการเชื่อมต่อที่ปลอดภัยเมื่อโอนย้าย ข้อมูล | เปิดใช้การสร้างทันเนลของ IP Security (IPSec) โดยอัตโนมัติระหว่าง Virtual I/O Servers ขณะโอนย้ายพาร์ติชันที่ใช้งานอยู่ | `/etc/security/pscexpert/bin/cfgsecmig` |
| 1.3.5 | จำกัดแพ็กเกจจากแหล่งที่ไม่รู้จัก | อนุญาตแพ็กเกจจาก Hardware Management Console | `/etc/security/pscexpert/bin/ipsecpermithostorport` |
| 5.1.1 | บำรุงรักษาซอฟต์แวร์ป้องกันไวรัส | บำรุงรักษาความสมบูรณ์ของระบบโดยการตรวจจับ การลบ และการป้องกันประเภทของซอฟต์แวร์ที่เป็นอันตรายที่ไม่รู้จัก | `/etc/security/pscexpert/bin/manageITsecurity` |
| **PCI เวอร์ชัน 2**<br>ส่วน 7<br>**PCI เวอร์ชัน 3**<br>ส่วน 7 | รักษาการเข้าถึงตามพื้นฐานที่จำเป็น | เปิดใช้การควบคุมการเข้าถึงตามบทบาท (RBAC) โดยการสร้างโอเปอเรเตอร์ของระบบ, ผู้ดูแลระบบ และบทบาทของผู้ใช้ที่เป็นเจ้าหน้าที่รักษาความปลอดภัย ระบบข้อมูลที่มีสิทธิ์ที่จำเป็น | `/etc/security/pscexpert/bin/EnableRbac` |
| **PCI เวอร์ชัน 2**<br>ไม่รวมในโปรไฟล์เวอร์ชัน 2 เพิ่มในเวอร์ชัน 3<br>**PCI เวอร์ชัน 3**<br>2.3 | ปรับใช้คุณลักษณะการรักษาความปลอดภัยเพิ่มเติมสำหรับเซอร์วิสที่จำเป็น โปรโตคอล หรือ daemons ที่ถือว่าไม่ปลอดภัย | ใช้เทคโนโลยีที่มีการรักษาความปลอดภัยเช่น Secure Shell (SSH), SSH File Transfer Protocol (S-FTP), Secure Sockets Layer (SSL) หรือ Internet Protocol Security Virtual Private Network (IPsec VPN) เพื่อปกป้องเซอร์วิสที่ไม่มีการรักษาความปลอดภัย เช่น NetBIOS, การแบ่งปันไฟล์, Telnet และ FTP รวมทั้ง กำหนดคอนฟิก SSH daemon เพื่อใช้โปรโตคอล SSHv2 เท่านั้น | `/etc/security/pscexpert/bin/sshPCIconfig` |
| **PCI เวอร์ชัน 2**<br>ไม่รวมในโปรไฟล์เวอร์ชัน 2 เพิ่มในเวอร์ชัน 3<br>**PCI เวอร์ชัน 3**<br>2.3 | SSH Client ต้องถูกกำหนดคอนฟิกให้ใช้โปรโตคอล SSHv2 เท่านั้น | กำหนดคอนฟิกไคลเอ็นต์ SSH เพื่อใช้โปรโตคอล SSHv2 | `/etc/security/pscexpert/bin/sshPCIconfig` |

*ตารางที่ 7. การตั้งค่าที่เกี่ยวข้องกับมาตรฐานการปฏิบัติตามข้อกำหนด PCI DSS เวอร์ชัน 2.0 และเวอร์ชัน 3.0 (ต่อ)*

| การปรับใช้มาตรฐาน PCI DSS เหล่านี้ | ข้อมูลจำเพาะการนำไปปฏิบัติ | การปรับใช้ AIX Security Expert | ตำแหน่งของสคริปต์ที่แก้ไขค่า |
|---|---|---|---|
| **PCI เวอร์ชัน 2**<br>ไม่รวมในโปรไฟล์เวอร์ชัน 2 เพิ่มในเวอร์ชัน 3<br>**PCI เวอร์ชัน 3**<br>2.3 | SSH daemon ต้อง listen บนแอดเดรสเครือข่ายการจัดการเท่านั้น ยกเว้น ได้รับอนุญาตสำหรับใช้การจัดการอื่น | ตรวจสอบให้แน่ใจว่าติดตั้ง SSH daemon เพื่อให้ listen เท่านั้น | `/etc/security/pscexpert/bin/sshPCIconfig` |
| **PCI เวอร์ชัน 2**<br>ไม่รวมในโปรไฟล์เวอร์ชัน 2 เพิ่มในเวอร์ชัน 3<br>**PCI เวอร์ชัน 3**<br>2.3 | SSH daemon ต้องถูกกำหนดคอนฟิกให้ใช้การเข้ารหัส FIPS 140-2 ที่อนุญาต เท่านั้น | ตรวจสอบให้แน่ใจว่า SSH daemon ใช้การเข้ารหัส FIPS 140-2 เท่านั้น | `/etc/security/pscexpert/bin/sshPCIconfig` |
| **PCI เวอร์ชัน 2**<br>ไม่รวมในโปรไฟล์เวอร์ชัน 2 เพิ่มในเวอร์ชัน 3<br>**PCI เวอร์ชัน 3**<br>2.3 | SSH daemon ต้องถูกกำหนดคอนฟิกเพื่อใช้ Message Authentication Codes (MACs) เท่านั้นที่พยายามปรับใช้แฮชเข้ารหัสที่อนุญาต | ตรวจสอบให้แน่ใจว่า MACs กำลังรันอัลกอริทึม ที่อนุมัติ | `/etc/security/pscexpert/bin/sshPCIconfig` |
| **PCI เวอร์ชัน 2**<br>ไม่รวมในโปรไฟล์เวอร์ชัน 2 เพิ่มในเวอร์ชัน 3<br>**PCI เวอร์ชัน 3**<br>2.3 | SSH daemon ต้องจำกัดความสามารถในการล้อกอินแก่ผู้ใช้หรือ ล็อกอินที่เจาะจง | จำกัดการล็อกอินบนระบบแก่ผู้ใช้หรือกลุ่ม ที่เจาะจง | `/etc/security/pscexpert/bin/sshPCIconfig` |
| **PCI เวอร์ชัน 2**<br>ไม่รวมในโปรไฟล์เวอร์ชัน 2 เพิ่มในเวอร์ชัน 3<br>**PCI เวอร์ชัน 3**<br>2.3 | ระบบต้องแสดงวันที่ และเวลาของการล็อกอินดด้วยแอคเคาต์สำเร็จล่าสุด ในแต่ละครั้งที่ล้อกอิน | เก็บรักษาข้อมูลจากการล็อกอินที่สำเร็จล่าสุด และแสดง หลังการล็อกอินสำเร็จครั้งหน้า | `/etc/security/pscexpert/bin/sshPCIconfig` |
| **PCI เวอร์ชัน 2**<br>ไม่รวมในโปรไฟล์เวอร์ชัน 2 เพิ่มในเวอร์ชัน 3<br>**PCI เวอร์ชัน 3**<br>2.3 | SSH daemon ต้องดำเนินการตรวจสอบโหมดแบบจำกัดของไฟล์คอนฟิกูเรชัน โฮมไดเร็กทอรี | ตรวจสอบให้แน่ใจว่าไฟล์คอนฟิกูเรชันโฮมไดเร็กทอรีถูกตั้งค่าเน โหมดที่ถูกต้อง | `/etc/security/pscexpert/bin/sshPCIconfig` |

*ตารางที่ 7. การตั้งค่าที่เกี่ยวข้องกับมาตรฐานการปฏิบัติตามข้อกำหนด PCI DSS เวอร์ชัน 2.0 และเวอร์ชัน 3.0 (ต่อ)*

| การปรับใช้มาตรฐาน PCI DSS เหล่านี้ | ข้อมูลจำเพาะการนำไปปฏิบัติ | การปรับใช้ AIX Security Expert | ตำแหน่งของสคริปต์ที่แก้ไขค่า |
|---|---|---|---|
| **PCI เวอร์ชัน 2**<br>ไม่รวมในโปรไฟล์เวอร์ชัน 2<br>เพิ่มในเวอร์ชัน 3<br>**PCI เวอร์ชัน 3**<br>2.3 | SSH daemon ต้องใช้การแยกสิทธิพิเศษ | ตรวจสอบให้แน่ใจว่า SSH daemon มีจำนวนการแยกของสิทธิพิเศษ ที่ถูกต้อง | `/etc/security/pscexpert/bin/sshPCIconfig` |
| **PCI เวอร์ชัน 2**<br>ไม่รวมในโปรไฟล์เวอร์ชัน 2<br>เพิ่มในเวอร์ชัน 3<br>**PCI เวอร์ชัน 3**<br>2.3 | SSH daemon ต้องไม่อนุญาตให้ rhosts มีการพิสูจน์ตัวตน RSA | ปิดใช้งานการพิสูจน์ตัวตน RSA สำหรับ rhosts เมื่อคุณกำลังใช้ SSH daemon | `/etc/security/pscexpert/bin/sshPCIconfig` |
| **PCI เวอร์ชัน 2**<br>ไม่รวมในโปรไฟล์เวอร์ชัน 2<br>เพิ่มในเวอร์ชัน 3<br>**PCI เวอร์ชัน 3**<br>2.3 | จำกัดจำนวนเซสชันการล็อกอินสูงสุดเป็น 2 ต่อหนึ่งผู้ใช้ | ตั้งค่าจำนวนเซสชันการล็อกอินสูงสุดเป็น 2 ต่อหนึ่ง ผู้ใช้ | `/etc/security/pscexpert/bin/sshPCIconfig` |
| **PCI เวอร์ชัน 2**<br>1.1.5<br>2.2.2<br>**PCI เวอร์ชัน 3**<br>10.4 | ตรวจสอบมาตรฐานการกำหนดคอนฟิก และกระบวนการเพื่อยืนยันว่า เทคโนโลยีการซิงโครไนซ์เวลาได้รับการประยุกต์ใช้ และทำให้เป็นปัจจุบันตามข้อกำหนด PCI DSS 6.1 และ 6.2 | เปิดใช้งาน ntp daemon | `/etc/security/pscexpert/bin/rctcpip` |
| **PCI เวอร์ชัน 2**<br>ไม่รวมในโปรไฟล์เวอร์ชัน 2<br>เพิ่มในเวอร์ชัน 3<br>**PCI เวอร์ชัน 3**<br>8.1.5 | ปิดใช้งานแอคเคาต์ผู้ใช้เมื่อไม่ใช้งาน | ปิดใช้งานแอคเคาต์หลังจากไม่มีการใช้งาน 35 วัน | `/etc/security/pscexpert/bin/disableacctpci` |
| **PCI เวอร์ชัน 2**<br>ไม่รวมในโปรไฟล์เวอร์ชัน 2<br>เพิ่มในเวอร์ชัน 3<br>**PCI เวอร์ชัน 3**<br>8.2 | จำกัดจำนวนเซสชันการล็อกอินสูงสุดเป็น 2 ต่อหนึ่งผู้ใช้ | ตั้งค่าจำนวนเซสชันแอ็คทีฟสูงสุดสำหรับผู้ใช้เป็น 2 โดยการตั้งค่า พารามิเตอร์ `maxulogs` เป็นค่า 2 | `/etc/security/pscexpert/bin/chusrattr` |

## ความเข้ากันได้กับ Sarbanes-Oxley Act และ COBIT

Sarbanes-Oxley (SOX) Act of 2002 ที่เป็นพื้นฐานของ 107th congress ของประเทศสหรัฐอเมริกาตรวจสอบ บริษัทมหาชน ในเรื่องกฎหมายหลักทรัพย์ และเรื่องที่ เกี่ยวข้อง เพื่อป้องกันผลประโยชน์ของผู้ลงทุน

SOX ส่วน 404 มอบอำนาจการจัดการประเมินผ่านการควบคุมภายใน สำหรับองค์กรส่วนใหญ่ การควบคุมภายในขยาย ระบบสารสนเทศ ซึ่งประมวลผลและรายงาน ข้อมูลการเงินของบริษัท SOX Act จัดให้มีรายละเอียดเฉพาะเจาะจง เกี่ยวกับ IT และการรักษาความปลอดภัย IT ผู้ตรวจสอบ SOX จำนวนมากยึดตามมาตรฐาน เช่น COBIT เป็นวิธีการประเมินและตรวจสอบการกำกับดูแลและควบคุม IT ที่เหมาะสม อ็อพชันการกำหนดคอนฟิก PowerSC Standard Edition SOX/COBIT XML จัดให้มีการกำหนดค่าการรักษาความปลอดภัยของระบบ AIX และ Virtual I/O Server (VIOS ที่จำเป็นต้องมีเพื่อให้เป็นไปตามแนวทางความเข้ากันได้กับ COBIT

IBM Compliance Expert Express Edition รันบนระบบปฏิบัติการ AIX เวอร์ชันต่อไปนี้:

- AIX 6.1
- AIX 7.1
- AIX 7.2

ความเข้ากันได้ กับมาตรฐานภายนอกถือเป็นความรับผิดชอบของเวิร์กโหลดของผู้ดูแลระบบ AIX IBM Compliance Expert Express Edition ได้รับการออกแบบมาเพื่อให้ง่ายต่อการจัดการ การตั้งค่าระบบปฏิบัติการ และรายการที่จำเป็นสำหรับ ความเข้ากันได้มาตรฐาน

โปรไฟล์ความเข้ากันได้ที่กำหนดค่าที่กำหนดล่วงหน้า ที่มากับ IBM Compliance Expert Express Edition ช่วยลด เวิร์กโหลดการดูแลระบบของการแปลความหมายเอกสารคู่มือความเข้ากันได้ และการประยุกต์ใช้มาตรฐานเหล่านี้ตามพารามิเตอร์การกำหนดค่า ระบบที่ระบุ

ความสามารถของ IBM Compliance Expert Express Edition ถูกออกแบบเพื่อช่วยไคลเอ็นต์ จัดการข้อกำหนดระบบได้อย่างมีประสิทธิภาพ ซึ่งเชื่อมโยงกับ ความเข้ากันได้กับมาตรฐานภายนอกที่สามารถลดค่าใช้จ่ายได้ ขณะปรับปรุงความเข้ากันได้มาตรฐาน ความปลอดภัยภายนอกรวมถึงด้านอื่นๆ ที่ไม่ใช่ค่าติดตั้งคอนฟิกูเรชัน การใช้งานของ IBM Compliance Expert Express Edition ไม่ได้รับประกันความเข้ากันได้กับมาตรฐาน Compliance Expert ออกแบบมาเพื่อช่วย ให้จัดการค่าติดตั้งคอนฟิกูเรชันระบบได้ง่าย ซึ่งทำให้ผู้ดูแลระบบ สามารถใส่ใจกับประเด็นอื่นๆ ที่ไม่ใช่ความเข้ากันได้

**ข้อมูลที่เกี่ยวข้อง**:

มาตรฐาน COBIT

## Health Insurance Portability and Accountability Act (HIPAA)

Health Insurance Portability and Accountability Act (HIPAA) คือโปรไฟล์การรักษาความปลอดภัยที่โฟกัสที่การป้องกัน Electronically Protected Health Information (EPHI)

กฎการรักษาความปลอดภัย HIPAA มุ่งเน้นเฉพาะที่การป้องกันของ EPHI และเฉพาะเซ็ตย่อยของเอเจนซีที่เป็นไปตามกฎการรักษาความปลอดภัย HIPAA ตามฟังก์ชัน และการใช้งาน EPHI

HIPAA ทั้งหมดที่ครอบคลุม เอนทิตี คล้ายกับ federal agencies บางส่วน ต้องเป็นไปตาม กฎการรักษาความปลอดภัย HIPAA

กฎการรักษาความปลอดภัย HIPAA มุ่งเน้นที่ การป้องกันการเก็บรักษาความลับ, ความสมบูรณ์ และความพร้อมใช้งานของ EPHI ตามที่กำหนดในกฎการรักษาความปลอดภัย

EPHI ที่เอนทิตีครอบคลุม สร้าง ได้รับ ดูแลรักษา หรือส่งต้องได้รับการป้องกันจาก เธรด อันตราย และการใช้งานที่ไม่ถูกต้อง และการเปิดเผยที่คาดการณ์อย่าง มีเหตุผล

ข้อกำหนด มาตรฐาน และการประยุกต์ใช้ ข้อมูลจำเพาะของกฎการรักษาความปลอดภัย HIPAA ใช้กับเอนทิตีที่ครอบคลุม ต่อไปนี้:

- ผู้ให้บริการด้านบริการสุขภาพ
- แผนสุขภาพ
- ศูนย์การบริการด้านสุขภาพ
- ใบสั่งยาโครงการประกันสุขภาพ และผู้สนับสนุนบัตรยา

ตารางต่อไปนี้มีรายละเอียดเกี่ยวกับหลายๆ ส่วนของ กฎการรักษาความปลอดภัย HIPAA และแต่ละส่วนได้แก่มาตรฐาน หลายๆ อย่างและ ข้อมูลจำเพาะการนำไปปฏิบัติ

**หมายเหตุ:** ไฟล์สคริปต์ที่กำหนดเอง ทั้งหมดที่มีไว้เพื่อบำรุงรักษา HIPAA Compliance จะอยู่ใน ไดเร็กทอรี `/etc/security/pscexpert/bin`

*ตารางที่ 8. กฎ HIPAA และรายละเอียด การนำไปปฏิบัติ*

| ส่วนของกฎการรักษาความปลอดภัย HIPAA | ข้อมูลจำเพาะการนำไปปฏิบัติ | การนำไปปฏิบัติ aixpert | คำสั่ง และค่าส่งคืน |
|---|---|---|---|
| 164.308 (a) (1) (ii) (D)<br><br>164.308 (a) (5) (ii) (C)<br><br>164.312 (b) | ประยุกต์ใช้โพรซีเดอร์เพื่อตรวจทานเร็กคอร์ด ทั่วไปของกิจกรรมระบบข้อมูล เช่นล็อกการตรวจสอบ รายงานการเข้าถึง และรายการการรักษาความปลอดภัยที่เกิดขึ้น | พิจารณาว่าการตรวจสอบถูกเปิดใช้งานในระบบ หรือไม่ | **คำสั่ง:**<br><br>**#audit query**<br><br>**ค่าส่งคืน:** ถ้าสำเร็จ คำสั่งนี้ออกโดยมีค่าเป็น 0 ถ้าไม่สำเร็จ คำสั่ง ออกโดยมีค่า 1 |
| 164.308 (a) (1) (ii) (D)<br><br>164.308 (a) (5) (ii) (C)<br><br>166.312 (b) | ประยุกต์ใช้โพรซีเดอร์เพื่อตรวจทานเร็กคอร์ด ทั่วไปของกิจกรรมระบบข้อมูล เช่นล็อกการตรวจสอบ รายงานการเข้าถึง และรายการการรักษาความปลอดภัยที่เกิดขึ้น | เปิดใช้การตรวจสอบในระบบ รวมถึงกำหนดคอนฟิก เหตุการณ์ที่จะถูกบันทึก | **คำสั่ง:**<br><br>**# audit start >/dev/null 2>&1.**<br><br>**ค่าส่งคืน:** ถ้าสำเร็จ คำสั่งนี้ออกโดยมีค่าเป็น 0 ถ้าไม่สำเร็จ คำสั่ง ออกโดยมีค่า 1<br><br>เหตุการณ์ต่อไปนี้ถูกตรวจสอบ:<br><br>**FILE_Mknod, FILE_Open, FS_Mkdir, PROC_Execute, DEV_Create, FILE_Acl, FILE_Chpriv, FILE_Fchpriv, FILE_Mode, INIT_Start, PASSWORD_Change, PASSWORD_Check, PROC_Adjtime, PROC_Kill, PROC_Privilege, PROC_Setpgid, USER_SU, USER_Change, USER_Create, USER_Login, USER_Logout, USER_Reboot, USER_Remove, USER_SetEnv, USER_SU, FILE_Acl, FILE_Fchmod,FILE_Fchown** |

*ตารางที่ 8. กฎ HIPAA และรายละเอียด การนำไปปฏิบัติ (ต่อ)*

| ส่วนของกฎการรักษาความปลอดภัย HIPAA | ข้อมูลจำเพาะการนำไปปฏิบัติ | การนำไปปฏิบัติ aixpert | คำสั่ง และค่าส่งคืน |
|---|---|---|---|
| 164.312 (a) (2) (iV) | การเข้ารหัสและการถอดรหัส (A):ประยุกต์ใช้ กลไกเพื่อเข้ารหัส และถอดรหัส EPHI | พิจารณาว่า encrypted file system (EFS) ถูกเปิดใช้งานบนระบบหรือไม่ | **คำสั่ง:**<br>**# efskeymgr -V >/dev/null 2>&1.**<br>**ค่าส่งคืน:** ถ้า EFS ยังไม่เปิดใช้าน คำสั่งนี้ออกโดยมีค่าเป็น 0 ถ้า EFS ไม่ ถูกเปิดใช้งาน คำสั่งนี้ออกโดยมีค่า 1 |
| 164.312 (a) (2) (iii) | ล็อกออฟอัตโนมัติ (A): ประยุกต์ใช้ อิเล็กทรอนิกส์โพรซีเดอร์เพื่อสิ้นสุดอิเล็กทรอนิกส์เซสชัน หลังจากช่วงเวลา ที่กำหนดไว้ล่วงหน้าของกิจกรรม | กำหนดค่าระบบเพื่อล็อกเอาต์ออกจากการประมวลผลแบบโต้ตอบ หลังจากไม่มีการดำเนินกิจกรรมใดๆ นานเกิน 15 | **คำสั่ง:**<br>**grep TMOUT= /etc/security /.profile > /dev/null 2>&1**<br>**echo "TMOUT=900 ; TIMEOUT=900; export TMOUT TIMEOUT.**<br>**ค่า ส่งคืน:** ถ้าคำสั่งไม่พบค่า **TMOUT=15** และสคริปต์ออกโดยมีค่า 1 มิฉะนั้นคำสั่งจะออกโดยมี ค่าเป็น 0 |
| 164.308 (a) (5) (ii) (D)<br>164.312 (a) (2) (i) | การจัดการรหัสผ่าน (A) :ประยุกต์ใช้ กระบวนการสำหรับการสร้าง การเปลี่ยนแปลง และการป้องกันรหัสผ่าน | ให้แน่ใจว่ารหัสผ่านทั้งหมดที่นั้นยาว 14 อักขระ | **คำสั่ง:**<br>**chsec -f /etc/security/user -s user -a minlen=8**<br>**ค่า ส่งคืน:** ถ้าสำเร็จ สคริปต์นี้ออกโดยมีค่าเป็น 0 ถ้าไม่สำเร็จ สคริปต์ออกโดยมีโค้ดระบุความผิดพลาดเป็น 1 |
| 164.308 (a) (5) (ii) (D)<br>164.312 (a) (2) (i) | การจัดการรหัสผ่าน (A) :ประยุกต์ใช้ กระบวนการสำหรับการสร้าง การเปลี่ยนแปลง และการป้องกันรหัสผ่าน | ให้แน่ใจว่ารหัสผ่านทั้งหมดประกอบด้วยอักขระแบบตัวอักษรอย่างน้อยสองตัวอักษร หนึ่งในนั้นต้องเป็นตัวพิมพ์ใหญ่ | **คำสั่ง:**<br>**chsec -f /etc/security/user -s user -a minalpha=4**<br>**ค่า ส่งคืน:** ถ้าสำเร็จ สคริปต์นี้ออกโดยมีค่าเป็น 0 ถ้าไม่สำเร็จ คำสั่งออกโดยมีโค้ดระบุความผิดพลาดเป็น 1 |
| 164.308 (a) (5) (ii) (D)<br>164.312 (a) (2) (i) | การจัดการรหัสผ่าน (A) :ประยุกต์ใช้ กระบวนการสำหรับการสร้าง การเปลี่ยนแปลง และการป้องกันรหัสผ่าน | ระบุจำนวนอักขระที่ไม่ใช่ตัวอักษรผสมตัวเลขขั้นต่ำ 2 ตัว | **คำสั่ง:**<br>**#chsec -f /etc/security/user -s user -a minother=2**<br>**ค่า ส่งคืน:** ถ้าสำเร็จ สคริปต์นี้ออกโดยมีค่าเป็น 0 ถ้าไม่สำเร็จ คำสั่งออกโดยมีโค้ดระบุความผิดพลาดเป็น 1 |
| 164.308 (a) (5) (ii) (D)<br>164.312 (a) (2) (i) | การจัดการรหัสผ่าน (A) :ประยุกต์ใช้ กระบวนการสำหรับการสร้าง การเปลี่ยนแปลง และการป้องกันรหัสผ่าน | ให้แน่ใจว่ารหัสผ่านทั้งหมดไม่มีอักขระ ซ้ำกัน | **คำสั่ง:**<br>**#chsec -f /etc/security/user -s user -a maxrepeats=1**<br>**ค่า ส่งคืน:** ถ้าสำเร็จ สคริปต์นี้ออกโดยมีค่าเป็น 0 ถ้าไม่สำเร็จ คำสั่งออกโดยมีโค้ดระบุความผิดพลาดเป็น 1 |

*ตารางที่ 8. กฎ HIPAA และรายละเอียด การนำไปปฏิบัติ (ต่อ)*

| ส่วนของกฎการรักษาความปลอดภัย HIPAA | ข้อมูลจำเพาะการนำไปปฏิบัติ | การนำไปปฏิบัติ aixpert | คำสั่ง และค่าส่งคืน |
|---|---|---|---|
| 164.308 (a) (5) (ii) (D)<br><br>164.312 (a) (2) (i) | การจัดการรหัสผ่าน (A) :ประยุกต์ใช้ กระบวนการสำหรับการสร้าง การเปลี่ยนแปลง และการป้องกันรหัสผ่าน | ให้แน่ใจว่ารหัสผ่านไม่ถูกนำมาใช้ซ้ำภายใน การเปลี่ยนแปลงอย่างน้อยห้าครั้ง | **คำสั่ง:**<br><br>**#chsec -f /etc/security/user -s user -a histsize=5**<br><br>**ค่า ส่งคืน:** ถ้าสำเร็จ สคริปต์นี้ออกโดยมีค่าเป็น 0 ถ้าไม่สำเร็จ คำสั่งออกโดยมีโค้ดระบุความผิดพลาดเป็น 1 |
| 164.308 (a) (5) (ii) (D)<br><br>164.312 (a) (2) (i) | การจัดการรหัสผ่าน (A) :ประยุกต์ใช้ กระบวนการสำหรับการสร้าง การเปลี่ยนแปลง และการป้องกันรหัสผ่าน | ระบุจำนวนสัปดาห์สูงสุดถือ 13 สัปดาห์ เพื่อที่รหัสผ่านจะยังคงถูกต้อง | **คำสั่ง:**<br><br>**#chsec -f /etc/security/user -s user -a maxage=8**<br><br>**ค่า ส่งคืน:** ถ้าสำเร็จ สคริปต์นี้ออกโดยมีค่าเป็น 0 ถ้าไม่สำเร็จ คำสั่งออกโดยมีโค้ดระบุความผิดพลาดเป็น 1 |
| 164.308 (a) (5) (ii) (D)<br><br>164.312 (a) (2) (i) | การจัดการรหัสผ่าน (A) :ประยุกต์ใช้ กระบวนการสำหรับการสร้าง การเปลี่ยนแปลง และการป้องกันรหัสผ่าน | นำจำนวนต่ำสุดของข้อกำหนดจำนวนสัปดาห์ ก่อนที่รหัสผ่านจะสามารถเปลี่ยนการเปลี่ยนแปลง | **คำสั่ง:**<br><br>**#chsec -f /etc/security/user -s user -a minage=2**<br><br>**ค่า ส่งคืน:** ถ้าสำเร็จ สคริปต์นี้ออกโดยมีค่าเป็น 0 ถ้าไม่สำเร็จ คำสั่งออกโดยมีโค้ดระบุความผิดพลาดเป็น 1 |
| 164.308 (a) (5) (ii) (D)<br><br>164.312 (a) (2) (i) | การจัดการรหัสผ่าน (A) :ประยุกต์ใช้ กระบวนการสำหรับการสร้าง การเปลี่ยนแปลง และการป้องกันรหัสผ่าน | ระบุจำนวนสัปดาห์สูงสุดเป็น 4 สัปดาห์ เพื่อเปลี่ยนแปลงรหัสผ่านที่หมดอายุ หลังจากค่าของพารามิเตอร์ **maxage** ถูกตั้งค่าโดยผู้ใช้ที่หมดอายุ | **คำสั่ง:**<br><br>**#chsec -f /etc/security/user -s user -a maxexpired=4**<br><br>**ค่า ส่งคืน:** ถ้าสำเร็จ สคริปต์นี้ออกโดยมีค่าเป็น 0 ถ้าไม่สำเร็จ คำสั่งออกโดยมีโค้ดระบุความผิดพลาดเป็น 1 |
| 164.308 (a) (5) (ii) (D)<br><br>164.312 (a) (2) (i) | การจัดการรหัสผ่าน (A) :ประยุกต์ใช้ กระบวนการสำหรับการสร้าง การเปลี่ยนแปลง และการป้องกันรหัสผ่าน | ระบุจำนวนอักขระขั้นต่ำที่ไม่สามารถมีซ้ำจากรหัสผ่านคือ 4 อักขระ | **คำสั่ง:**<br><br>**#chsec -f /etc/security/user -s user -a mindiff=4**<br><br>**ค่า ส่งคืน:** ถ้าสำเร็จ สคริปต์นี้ออกโดยมีค่าเป็น 0 ถ้าไม่สำเร็จ คำสั่งออกโดยมีโค้ดระบุความผิดพลาดเป็น 1 |
| 164.308 (a) (5) (ii) (D)<br><br>164.312 (a) (2) (i) | การจัดการรหัสผ่าน (A) :ประยุกต์ใช้ กระบวนการสำหรับการสร้าง การเปลี่ยนแปลง และการป้องกันรหัสผ่าน | ระบุว่าจำนวนวันคือ 5 เพื่อรอ ก่อนที่ระบบจะออกคำเตือนว่าจำเป็นต้องมีการเปลี่ยนแปลงรหัสผ่าน | **คำสั่ง:**<br><br>**#chsec -f /etc/security/user -s user -a pwdwarntime = 5**<br><br>**ค่า ส่งคืน:** ถ้าสำเร็จ สคริปต์นี้ออกโดยมีค่าเป็น 0 ถ้าไม่สำเร็จ คำสั่งออกโดยมีโค้ดระบุความผิดพลาดเป็น 1 |

*ตารางที่ 8. กฎ HIPAA และรายละเอียด การนำไปปฏิบัติ (ต่อ)*

| ส่วนของกฎการรักษาความปลอดภัย HIPAA | ข้อมูลจำเพาะการนำไปปฏิบัติ | การนำไปปฏิบัติ aixpert | คำสั่ง และค่าส่งคืน |
|---|---|---|---|
| 164.308 (a) (5) (ii) (D)<br><br>164.312 (a) (2) (i) | การจัดการรหัสผ่าน (A) :ประยุกต์ใช้ กระบวนการสำหรับการสร้าง การเปลี่ยนแปลง และการป้องกันรหัสผ่าน | ตรวจสอบความถูกต้องของนิยามผู้ใช้ และแก้ไขข้อผิดพลาด | **คำสั่ง:**<br><br>**/usr/bin/usrck -y ALL**<br><br>**/usr/bin/usrck -n ALL.**<br><br>**ค่า ส่งคืน:** คำสั่งไม่ส่งคืนค่า คำสั่งตรวจสอบ และแก้ไขข้อผิดพลาดถ้ามี |
| 164.308 (a) (5) (ii) (D)<br><br>164.312 (a) (2) (i) | การจัดการรหัสผ่าน (A) :ประยุกต์ใช้ กระบวนการสำหรับการสร้าง การเปลี่ยนแปลง และการป้องกันรหัสผ่าน | ล็อกแอคเคาต์หลังจากพยายามล็อกอินแล้วล้มเหลว ติดต่อกันสามครั้ง | **คำสั่ง:**<br><br>**#chsec -f /etc/security/user -s user -a loginretries=3**<br><br>**ค่า ส่งคืน:** ถ้าสำเร็จ สคริปต์นี้ออกโดยมีค่าเป็น 0 ถ้าไม่สำเร็จ คำสั่งออกโดยมีโค้ดระบุความผิดพลาดเป็น 1 |
| 164.308 (a) (5) (ii) (D)<br><br>164.312 (a) (2) (i) | การจัดการรหัสผ่าน (A) :ประยุกต์ใช้ กระบวนการสำหรับการสร้าง การเปลี่ยนแปลง และการป้องกันรหัสผ่าน | ระบุการหน่วงเวลาระหว่างการล็อกอิน ที่ไม่สำเร็จหนึ่งครั้งกับการล็อกอินอื่นๆ เป็น 5 วินาที | **คำสั่ง:**<br><br>**chsec -f /etc/security/login.cfg -s default -a logindelay=5**<br><br>**ค่า ส่งคืน:** ถ้าสำเร็จ สคริปต์นี้ออกโดยมีค่าเป็น 0 ถ้าไม่สำเร็จ คำสั่งออกโดยมีโค้ดระบุความผิดพลาดเป็น 1 |
| 164.308 (a) (5) (ii) (D)<br><br>164.312 (a) (2) (i) | การจัดการรหัสผ่าน (A) :ประยุกต์ใช้ กระบวนการสำหรับการสร้าง การเปลี่ยนแปลง และการป้องกันรหัสผ่าน | ระบุจำนวนครั้งที่พยายามล็อกอินแล้วไม่สำเร็จ บนพอร์ต ก่อนที่พอร์ตถูกล็อกเป็น 10 | **คำสั่ง:**<br><br>**chsec -f /etc/security/lastlog -s username -a \ unsuccessful_login_count=10**<br><br>**ค่า ส่งคืน:** ถ้าสำเร็จ สคริปต์นี้ออกโดยมีค่าเป็น 0 ถ้าไม่สำเร็จ คำสั่งออกโดยมีโค้ดระบุความผิดพลาดเป็น 1 |
| 164.308 (a) (5) (ii) (D)<br><br>164.312 (a) (2) (i) | การจัดการรหัสผ่าน (A) :ประยุกต์ใช้ กระบวนการสำหรับการสร้าง การเปลี่ยนแปลง และการป้องกันรหัสผ่าน | ระบุช่วงเวลาในพอร์ตสำหรับความพยายามล็อกอินที่ไม่สำเร็จก่อนพอร์ตถูกปิดใช้งานเป็น 60 วินาที | **คำสั่ง:**<br><br>**#chsec -f /etc/security/lastlog -s user -a time_last_unsuccessful_login=60**<br><br>**ค่า ส่งคืน:** ถ้าสำเร็จ สคริปต์นี้ออกโดยมีค่าเป็น 0 ถ้าไม่สำเร็จ คำสั่งออกโดยมีโค้ดระบุความผิดพลาดเป็น 1 |
| 164.308 (a) (5) (ii) (D)<br><br>164.312 (a) (2) (i) | การจัดการรหัสผ่าน (A) :ประยุกต์ใช้ กระบวนการสำหรับการสร้าง การเปลี่ยนแปลง และการป้องกันรหัสผ่าน | ระบุช่วงเวลาหลังจากพอร์ต ถูกล็อก และหลังจากถูกปิดใช้งาน เป็น 30 นาที | **คำสั่ง:**<br><br>**#chsec -f /etc/security/login.cfg -s default -a loginreenable = 30**<br><br>**ค่า ส่งคืน:** ถ้าสำเร็จ สคริปต์นี้ออกโดยมีค่าเป็น 0 ถ้าไม่สำเร็จ คำสั่งออกโดยมีโค้ดระบุความผิดพลาดเป็น 1 |

*ตารางที่ 8. กฎ HIPAA และรายละเอียด การนำไปปฏิบัติ (ต่อ)*

| ส่วนของกฎการรักษาความปลอดภัย HIPAA | ข้อมูลจำเพาะการนำไปปฏิบัติ | การนำไปปฏิบัติ aixpert | คำสั่ง และค่าส่งคืน |
|---|---|---|---|
| 164.308 (a) (5) (ii) (D)<br><br>164.312 (a) (2) (i) | การจัดการรหัสผ่าน (A) :ประยุกต์ใช้ กระบวนการสำหรับการสร้าง การเปลี่ยนแปลง และการป้องกันรหัสผ่าน | ระบุช่วงเวลาเพื่อพิมพ์รหัสผ่านเป็น 30 วินาที | **คำสั่ง:**<br><br>**chsec -f /etc/security/login.cfg -s usw -a logintimeout=30**<br><br>**ค่า ส่งคืน:** ถ้าสำเร็จ สคริปต์นี้ออกโดยมีค่าเป็น 0 ถ้าไม่สำเร็จ คำสั่งออกโดยมีโค้ดระบุความผิดพลาดเป็น 1 |
| 164.308 (a) (5) (ii) (D)<br><br>164.312 (a) (2) (i) | การจัดการรหัสผ่าน (A) :ประยุกต์ใช้ กระบวนการสำหรับการสร้าง การเปลี่ยนแปลง และการป้องกันรหัสผ่าน | ให้แน่ใจว่าแอคเคาต์ถูกล็อกหลังไม่ได้ใช้งาน 35 วัน | **คำสั่ง:**<br><br>**grep TMOUT= /etc/security /.profile > /dev/null 2>&1if TMOUT = (35x24x60x60){#chsec -f /etc/security/user -s user -aaccount_locked = true}**<br><br>**ค่าส่งคืน:** ถ้าคำสั่งไม่สามารถตั้งค่า **account_locked** เป็น **true** สคริปต์ออกโดยมีค่า 1 มิฉะนั้นคำสั่งออกโดยมี ค่า 0 |
| 164.312 (c) (1) | ประยุกต์ใช้นโยบายและโพรซีเดอร์เพื่อป้องกัน EPHI จากการยืนยัน หรือการทำลายที่ไม่ถูกต้อง | ตั้งค่านโยบาย trusted execution (TE) เป็น ON | **คำสั่ง:**<br><br>เปิด **CHKEXEC, CHKSHLIB, CHKSCRIPT, CHKKERNEXT, STOP_ON_CHKFAIL,TE=ON**<br>**ตัวอย่างเช่น trustchk -p TE=ON CHKEXEC = ON, CHKSHLIB, =ON, CHKSCRIPT=ON, CHKKERNEXT = ON**<br><br>**ค่าส่งคืน:** เมื่อล้มเหลว สคริปต์ ออกโดยมีค่าเป็น 1 |
| 164.312 (e) (1) | ประยุกต์ใช้การวัดการรักษาความปลอดภัยด้านเทคนิคเพื่อป้องกันการเข้าถึงที่ไม่ได้รับอนุญาตใน EPHI ที่กำลังถูกส่งผ่านเครือข่ายการสื่อสารอิเล็กทรอนิกส์ | พิจารณาว่า **ssh** filesets ถูก ติดตั้งหรือไม่ ถ้าไม่ ให้แสดงข้อความแสดงข้อผิดพลาด | **คำสั่ง:**<br><br>**# lslpp -l \| grep openssh > /dev/null 2>&1**<br><br>**ค่าส่งคืน:** ถ้าค่าส่งคืนสำหรับคำสั่งนี้คือ 0 สคริปต์ออกโดยมีค่า เป็น 0 ถ้า ssh filesets ไม่ถูกติดตั้ง สคริปต์ออกด้วยค่า 1 และแสดงข้อความแสดงข้อผิดพลาด `Install ssh filesets for secure transmission` |

ตารางต่อไปนี้มีรายละเอียดเกี่ยวกับหลายๆ ฟังก์ชันของ กฎการรักษาความปลอดภัย HIPAA และแต่ละฟังก์ชันได้แก่มาตรฐานหลายๆ อย่างและ ข้อมูลจำเพาะการนำไปปฏิบัติ

*ตารางที่ 9. ฟังก์ชัน HIPAA และรายละเอียด การนำไปปฏิบัติ*

| ฟังก์ชัน HIPAA | ข้อมูลจำเพาะการนำไปปฏิบัติ | การนำไปปฏิบัติ aixpert | คำสั่ง และค่าส่งคืน |
|---|---|---|---|
| การล็อกข้อผิดพลาด | รวบรวมข้อผิดพลาดจากล็อกต่างๆ และ ส่งอีเมลถึงผู้ดูแลระบบ | พิจารณาว่ามีข้อผิดพลาดฮาร์ดแวร์อยู่หรือไม่<br><br>พิจารณา ว่ามีข้อผิดพลาดที่ไม่สามารถแก้ไขได้ จากไฟล์ **trcfile** ในตำแหน่ง `/var/adm/ras/trcfile` หรือไม่<br><br>ส่ง ข้อผิดพลาดไปยัง **root@<hostname>** | **คำสั่ง:**<br><br>**errpt -d H**<br><br>**ค่าส่งคืน:** ถ้าสำเร็จ คำสั่งนี้ออกโดยมีค่าเป็น 0 ถ้าไม่สำเร็จ คำสั่ง ออกโดยมีค่า 1 |
| การเปิดใช้งาน FPM | เปลี่ยนแปลงสิทธิ์ไฟล์ | เปลี่ยนแปลงสิทธิของไฟล์จากรายการ สิทธิ์ และไฟล์โดยใช้คำสั่ง **fpm** | **คำสั่ง:**<br><br>**# fpm -l <level> -f <commands file>**<br><br>**ค่าส่งคืน:** ถ้าสำเร็จ คำสั่งนี้ออกโดยมีค่าเป็น 0 ถ้าไม่สำเร็จ คำสั่ง ออกโดยมีค่า 1 |
| การเปิดใช้งาน RBAC | สร้างผู้ใช้ **isso, so** และ **sa** และกำหนดบทบาทที่เหมาะสมให้กับผู้ใช้ | แนะนำให้คุณสร้างผู้ใช้ **isso, so** และ **sa**<br><br>กำหนดค่า บทบาทที่เหมาะสมให้แก่ผู้ใช้ | **คำสั่ง:**<br><br>**/etc/security/pscexpert/bin/RbacEnablement** |

## ความเชื่อถือได้กับ North American Electric Reliability Corporation

North American Electric Reliability Corporation (NERC) คือองค์กรที่ไม่แสวงผลกำไร ที่พัฒนามาตรฐานสำหรับอุตสาหกรรมระบบไฟฟ้ากำลัง PowerSC Standard Edition มีโปรไฟล์ NERC ที่กำหนดคอนฟิกล่วงหน้าซึ่ง มีมาตรฐานการรักษาความปลอดภัยที่คุณสามารถใช้เพื่อปกป้องระบบไฟฟ้ากำลังสำคัญ

โปรไฟล์ NERC เป็นไปตามมาตรฐาน Critical Infrastructure Protection (CIP)

โปรไฟล์ NERC อยู่ที่ `/etc/security/aixpert/custom/NERC.xml` คุณ สามารถรีเซ็ตข้อกำหนด CIP ที่ใช้กับโปรไฟล์ NERC ให้เป็นสภาวะดีฟอลต์ได้โดยการใช้ โปรไฟล์ NERC_to_AIXDefault.xml ที่อยู่ใน ไดเร็กทอรี `/etc/security/aixpert/custom` กระบวนการนี้ไม่เหมือนกับ การดำเนินการ เลิกทำ ของโปรไฟล์ NERC

ตารางต่อไปนี้ให้ข้อมูลเกี่ยวกับมาตรฐาน CIP ที่ใช้กับระบบปฏิบัติการ AIX และวิธีที่ PowerSC Standard Edition จัดการกับมาตรฐาน CIP:

*ตารางที่ 10. มาตรฐาน CIP สำหรับ PowerSC Standard Edition*

| มาตรฐาน CIP | การปรับใช้ AIX Security Expert | ตำแหน่งของสคริปต์ที่แก้ไขค่า |
|---|---|---|
| CIP-003-3 R5.1 | กำหนดคอนฟิกพารามิเตอร์การรักษาความปลอดภัยระบบเพื่อป้องกันปัญหาโดยการลบแอ็ตทริบิวต์ set-user identification (SUID) และ set-group identification (SGID) ออกจากไบนารีไฟล์ | • `/etc/security/pscexpert/bin/filepermgr`<br>• `/etc/security/pscexpert/bin/rmsuidfrmrcmds` |
| CIP-003-3 R5.1.1 | เปิดใช้การควบคุมการเข้าถึงตามบทบาท (RBAC) โดยการสร้างโอเปอเรเตอร์ของระบบ, ผู้ดูแลระบบ และบทบาทของผู้ใช้ที่เป็นเจ้าหน้าที่รักษาความปลอดภัยระบบข้อมูลที่มีสิทธิ์ที่จำเป็น | `/etc/security/pscexpert/bin/EnableRbac` |
| CIP-005-3a R2.1-R2.4 | เปิดใช้งาน Secure Shell (SSH) สำหรับเข้าถึงการรักษาความปลอดภัย | `/etc/security/pscexpert/bin/sshstart` |
| CIP-005-3a R2.5 | ปิดใช้งานเซอร์วิสที่ไม่จำเป็นและไม่มีการรักษาความปลอดภัยต่อไปนี้:<br>• **lpd** daemon<br>• Common Desktop Environment (CDE) | `/etc/security/pscexpert/bin/comntrows` |
| CIP-005-3a R2.5 | ปิดใช้งานเซอร์วิสที่ไม่จำเป็นและไม่มีการรักษาความปลอดภัยต่อไปนี้:<br>• **timed** daemon<br>• **NTP** daemon<br>• **rwhod** daemon<br>• **DPID2** daemon<br>• เอเจนต์ DHCP | `/etc/security/pscexpert/bin/rctcpip` |

*ตารางที่ 10. มาตรฐาน CIP สำหรับ PowerSC Standard Edition (ต่อ)*

| มาตรฐาน CIP | การปรับใช้ AIX Security Expert | ตำแหน่งของสคริปต์ที่แก้ไขค่า |
|---|---|---|
| CIP-005-3a R2.5 | ปิดใช้งานเซอร์วิสที่ไม่จำเป็นและไม่มีการรักษาความปลอดภัยต่อไปนี้:<br>• **comsat** daemon<br>• **dtspcd** daemon<br>• **fingerd** daemon<br>• **ftpd** daemon<br>• **rshd** daemon<br>• **rlogind** daemon<br>• **rexecd** daemon<br>• **systat** daemon<br>• **tfptd** daemon<br>• **talkd** daemon<br>• **rquotad** daemon<br>• **rstatd** daemon<br>• **rusersd** daemon<br>• **rwalld** daemon<br>• **sprayd** daemon<br>• **pcnfsd** daemon<br>• **telnet** daemon<br>• เซอร์วิส cmsd<br>• เซอร์วิส ttdbserver<br>• เซอร์วิส TCP echo<br>• เซอร์วิส TCP discard<br>• เซอร์วิส TCP chargen<br>• เซอร์วิส TCP daytime<br>• เวลา TCP time<br>• เซอร์วิส UDP echo<br>• เซอร์วิส UDP discard<br>• เซอร์วิส UDP chargen<br>• เซอร์วิส UDP daytime<br>• เวลา UDP time | `/etc/security/pscexpert/bin/cominetdconf` |
| CIP-005-3a R2.5 | บังคับใช้การร้องขอการโจมตีโดยการปฏิเสธการให้บริการสำหรับพอร์ตการผ่อนปรน | `/etc/security/pscexpert/bin/tcptr_aixpert` |
| CIP-005-3a R3 CIP-007-3a R5, R6.5 | เปิดใช้งานการตรวจสอบไฟล์ไลบรารีบน ระบบ | `/etc/security/pscexpert/bin/pciaudit` |
| CIP-005-3a R3 | อัพเดตคอนฟิกไฟล์การตรวจสอบด้วยผู้ใช้ บท บาท และเหตุการณ์ที่สร้างใหม่ | `/etc/security/pscexpert/bin/auditconfig` |

*ตารางที่ 10. มาตรฐาน CIP สำหรับ PowerSC Standard Edition (ต่อ)*

| มาตรฐาน CIP | การปรับใช้ AIX Security Expert | ตำแหน่งของสคริปต์ที่แก้ไขค่า |
|---|---|---|
| CIP-007-3a R3 | แสดงข้อความเพื่อเปิดใช้งาน Trusted Network Connect (TNC) | /etc/security/pscexpert/bin/GeneralMsg |
| CIP-007-3a R4 | บำรุงรักษาความสมบูรณ์ของระบบโดยการตรวจจับ การลบ และการป้องกันประเภทของซอฟต์แวร์ที่เป็นอันตรายที่ไม่รู้จัก | /etc/security/pscexpert/bin/manageITsecurity |
| CIP-007-3a R5.2.1 | เปิดใช้งานรหัสผ่านที่จะเปลี่ยนแปลงในการล็อกอินครั้งแรกสำหรับแอคเคาต์ผู้ใช้ดีฟอลต์ทั้งหมดที่ ไม่ถูกล็อก | /etc/security/pscexpert/bin/pwdchg |
| CIP-007-3a R5.2.2-R5.2.3 | ล็อกแอคเคาต์ผู้ใช้ดีฟอลต์ทั้งหมด | /etc/security/pscexpert/dodv2/lockacc_rlogin |
| CIP-007-3a R5.3.1 | ตั้งค่ารหัสผ่านแต่ละค่าเป็นขั้นต่ำ 6 อักขระ | /etc/security/pscexpert/bin/chusrattr |
| CIP-007-3a R5.3.2 | ตั้งค่ารหัสผ่านแต่ละค่าเป็นค่าที่มีอักขระตัวอักษร ตัวเลข และอักขระพิเศษรวมกัน | /etc/security/pscexpert/bin/chusrattr |
| CIP-007-3a R5.3.3 | เปลี่ยนแปลงรหัสผ่านแต่ละค่าทุกปี | /etc/security/pscexpert/bin/chusrattr |
| CIP-007-3a R7 | แสดงข้อความเพื่อเปิดใช้งาน Encrypted File System (EFS) | /etc/security/pscexpert/bin/GeneralMsg |
| CIP-010-1 | แสดงข้อความเพื่อเปิดใช้งาน Real Time Compliance (RTC) | /etc/security/pscexpert/bin/GeneralMsg |

รายการต่อไปนี้แสดงข้อมูลเกี่ยวกับมาตรฐาน CIP ที่ใช้กับระบบปฏิบัติการ AIX:

**Standard CIP-003-3 — Cyber Security — Security Management Controls**

**R5 ค่าควบคุมการเข้าถึง**

เอกสาร Responsible Entity และประยุกต์ใช้โปรแกรมสำหรับการจัดการการเข้าถึงข้อมูล Critical Cyber Asset (CCA) ที่มีการป้องกัน

- **R5.1:** Responsible Entity เก็บรักษารายการส่วนบุคคลที่กำหนดให้ที่มีหน้าที่ ในการอนุญาตการเข้าถึงข้อมูลที่ได้รับการปกป้องแบบโลจิคัลหรือฟิสิคัล
- **R5.1.1:** บุคคลถูกระบุด้วยชื่อ ตำแหน่ง และข้อมูลซึ่งบุคคลนั้น มีหน้าที่สำหรับการอนุญาตการเข้าถึง

**Standard CIP-005-3a — Cyber Security — Electronic Security Perimeters**

**R2. Electronic Access Controls**

Responsible Entity ประยุกต์ใช้และจัดทำเอกสารกระบวนการเกี่ยวกับองค์กร และกลไก ด้านขั้นตอนและเทคนิคสำหรับควบคุมการเข้าถึงกระแสไฟฟ้าที่จุดเข้าถึงกระแสไฟฟ้ากับหมดด้วย Electronic Security Perimeters

- **R2.1:** กระบวนการและกลไกเหล่านี้ใช้โมเดลการควบคุมการเข้าถึงที่ปฏิเสธการเข้าถึง โดยดีฟอลต์ โดยสิทธิ์การเข้าถึงโดยชัดแจ้งต้องถูกระบุไว้

- **R2.2:** ที่จุดเข้าถึง Electronic Security Perimeter ทั้งหมด Responsible Entity เปิดให้เฉพาะพอร์ตและเซอร์วิสที่จำเป็นสำหรับการดำเนินการ และการมอนิเตอร์ Cyber Assets ภายใน Electronic Security Perimeter และเอกสารแต่ละรายการ หรือที่ระบุ โดยการจัดกลุ่ม การกำหนดคอนฟิกของพอร์ตและเซอร์วิสเหล่านั้น
- **R2.3:** Responsible Entity ประยุกต์ใช้และดูแลรักษาโพรซีเดอร์ สำหรับการรักษาความปลอดภัยการเข้าถึง ทางสายโทรศัพท์ไปยัง Electronic Security Perimeters
- **R2.4:** เมื่อจุดเข้าถึงที่ติดต่อภายนอกกับ Electronic Security Perimeter ถูก เปิดใช้งาน Responsible Entity จะประยุกต์ใช้การควบคุมที่มีขั้นตอน หรือเทคนิคที่ชัดเจนที่จุด เข้าถึงเพื่อให้แน่ใจในความถูกต้องของผู้ที่เข้าถึง ที่ดำเนินการได้ทางเทคนิค
- **R2.5:** เอกสารคู่มือที่ต้องการโดยขั้นต่ำจะระบุ และอธิบายต่อไปนี้:
  - **R2.5.1:** กระบวนการสำหรับการร้องขอการเข้าถึง และการอนุญาต
  - **R2.5.2:** วิธีการพิสูจน์ตัวตน
  - **R2.5.3:** กระบวนการตรวจทานสำหรับสิทธิ์ในการอนุญาต เป็นไปตาม Standard CIP-004-3 Requirement R4
  - **R2.5.4:** การควบคุมที่ใช้เพื่อรักษาความปลอดภัยการเชื่อมต่อที่เข้าถึงได้ทางโทรศัพท์

**R3. การมอนิเตอร์ Electronic Access**

Responsible Entity ประยุกต์ใช้และจัดทำเอกสารกระบวนการอิเล็กทรอนิกส์ หรือด้วยตนเองสำหรับการมอนิเตอร์ และการล็อกการเข้าถึงที่จุดเข้าถึง Electronic Security Perimeters ตลอดยี่สิบสี่ชั่วโมงต่อวัน เจ็ดวันต่อสัปดาห์

- **R3.1:** สำหรับ Critical Cyber Assets ที่เข้าถึงได้ทางโทรศัพท์ที่ใช้โปรโตคอลที่ไม่สามารถกำหนดเส้นทางได้ Responsible Entity ประยุกต์ใช้และจัดทำเอกสารกระบวนการมอนิเตอร์ที่แต่ละจุดเข้าถึงกับอุปกรณ์โทรศัพท์ ที่เป็นไปได้ด้านเทคนิค
- **R3.2:** ที่เป็นไปได้ด้านเทคนิค กระบวนการมอนิเตอร์ความปลอดภัยตรวจหา และแจ้งเตือน เมื่อมีความพยายาม หรือมีการเข้าถึงที่ไม่ได้รับอนุญาตจริง รวมทั้งยังจัดให้มีการแจ้งเตือนที่เหมาะสมไปยังบุคคลที่มีหน้าที่ตอบสนองที่กำหนด เมื่อการแจ้งเตือนไม่สามารถทำได้ทางเทคนิค Responsible Entity จะทบทวนหรือจัดหาล็อกการเข้าถึงสำหรับความพยายาม หรือการเข้าถึงที่ไม่ได้รับอนุญาตจริงอย่างน้อยทุก 90 วัน

**Standard CIP-007-3a — Cyber Security — Systems Security Management**

**R2. พอร์ตและเซอร์วิส**

Responsible Entity สร้าง จัดทำเอกสาร และประยุกต์ใช้กระบวนการเพื่อให้แน่ใจว่ามีเฉพาะ พอร์ตและเซอร์วิสเหล่านั้นที่จำเป็นสำหรับการดำเนินการปกติ และในกรณีฉุกเฉินที่ถูกเปิดใช้งาน

- **R2.1:** Responsible Entity เปิดใช้งานเฉพาะพอร์ตและเซอร์วิสที่จำเป็นสำหรับ การดำเนินการปกติและกรณีฉุกเฉิน
- **R2.2:** Responsible Entity ปิดใช้งานพอร์ตและเซอร์วิสอื่นๆ รวมถึงพอร์ตที่ ใช้สำหรับวัตถุประสงค์ในการทดสอบ ก่อนการดำเนินงานจริงในการใช้ Cyber Assets ทั้งหมดภายใน Electronic Security Perimeters
- **R2.3:** ในกรณีที่มีพอร์ตและเซอร์วิสซึ่งไม่ถูกใช้งานแต่ไม่สามารถปิดใช้งานได้เนื่องจากข้อจำกัด ด้านเทคนิค Responsible Entity จะจัดทำเอกสารวัดค่าชดเชยที่ใช้เพื่อลด ความเสี่ยงที่จะเปิดเผย

**R3. การจัดการแพตช์การรักษาความปลอดภัย**

Responsible Entity อาจแยก หรือเป็นส่วนประกอบหนึ่งของกระบวนการจัดการการกำหนดคอนฟิก ที่จัดทำเอกสารที่ระบุใน CIP-003-3 Requirement R6 ซึ่งสร้าง จัดทำเอกสาร และ ประยุกต์ใช้โปรแกรมจัดการแพตช์รักษาความปลอดภัยสำหรับการติดตาม การประเมินค่า การทดสอบ และการติดตั้ง แพตช์ซอฟต์แวร์รักษาความปลอดภัยไซเบอร์ที่ปรับใช้ได้สำหรับ Cyber Assets ทั้งหมดภายใน Electronic Security Perimeters

- **R3.1:** Responsible Entity จัดทำเอกสารการประเมินค่าแพตช์การรักษาความปลอดภัย และการอัพเกรด การรักษาความปลอดภัยสำหรับการปรับใช้ได้ภายใน 30 วันที่มีความพร้อมใช้งานแพตช์ หรือการอัพเกรด
- **R3.2:** Responsible Entity จัดทำเอกสารการประยุกต์ใช้แพตช์การรักษาความปลอดภัย ใน กรณีใดๆ ที่แพตช์ไม่ได้รับการติดตั้ง Responsible Entity จัดทำเอกสารการวัดค่าการชดเชย ที่ใช้เพื่อลดความเสี่ยงที่จะเปิดเผย

**R4. การป้องกันซอฟต์แวร์ไม่พึงประสงค์**

Responsible Entity ใช้ซอฟต์แวร์ป้องกันไวรัส และเครื่องมือป้องกันซอฟต์แวร์ ไม่พึงประสงค์ (มัลแวร์) อื่นๆ ที่เป็นไปได้ทางเทคนิคเพื่อตรวจหา ป้องกัน ขัดขวาง และลด การแนะนำ การเปิดเผย และการให้ข้อมูลมัลแวร์บน Cyber Assets ทั้งหมดภายใน Electronic Security Perimeters

- **R4.1:** Responsible Entity จัดทำเอกสารและประยุกต์ใช้เครื่องมือป้องกันไวรัส และมัลแวร์ ในกรณีที่ซอฟต์แวร์ป้องกันไวรัส และเครื่องมือป้องกันมัลแวร์ไม่ถูกติดตั้ง Responsible Entity จะจัดทำเอกสารการวัดค่าการชดเชยเพื่อลดความเสี่ยงที่จะเปิดเผย
- **R4.2:** Responsible Entity จัดทำเอกสารและประยุกต์ใช้กระบวนการในการอัพเดต ลายเซ็นต์ป้องกันไวรัส และการป้องกันมัลแวร์ กระบวนการต้องระบุถึงการทดสอบและการติดตั้ง ลายเซ็นต์

**R5. การจัดการแอคเคาต์**

Responsible Entity สร้าง ประยุกต์ใช้ และจัดทำเอกสารการควบคุมด้านเทคนิค และด้านขั้นตอน เพื่อบังคับใช้การพิสูจน์ตัวตนในการเข้าถึง และความรับผิดชอบต่อกิจกรรมผู้ใช้ทั้งหมด และที่ลด ความเสี่ยงต่อการเข้าถึงระบบที่ไม่ได้รับอนุญาต

- **R5.1:** Responsible Entity ยืนยันว่าบุคคล และแอคเคาต์ระบบที่ใช้ร่วมกัน และ สิทธิ์การเข้าถึงที่ได้รับอนุญาตนั้นสอดคล้องกับแนวคิดที่ ต้องทราบ เกี่ยวกับฟังก์ชันการทำงานที่ดำเนินการ
  - **R5.1.1:** Responsible Entity ตรวจทานแอคเคาต์ผู้ใช้อย่างน้อยปีละครั้งเพื่อยืนยันว่า สิทธิ์ในการเข้าถึงนั้นตรงตาม Standard CIP-003-3
  - **R5.1.2:** Responsible Entity สร้างวิธี กระบวนการ และโพรซีเดอร์ที่ สร้างล็อกที่มีรายละเอียดอย่างเพียงพอต่อการสร้างร่องรอยการตรวจสอบข้อมูลประวัติของกิจกรรมการเข้าถึง ของแอคเคาต์ผู้ใช้แต่ละคนเป็นเวลาอย่างน้อย 90 วัน
  - **R5.1.3:** Responsible Entity ตรวจทานแอคเคาต์ผู้ใช้อย่างน้อยปีละครั้งเพื่อยืนยันว่า สิทธิ์ในการเข้าถึงนั้นตรงตาม Standard CIP-003-3
- **R5.2:** Responsible Entity ประยุกต์ใช้นโยบายเพื่อลดและจัดการขอบเขตและ การใช้งานที่ยอมรับได้ของผู้ดูแลระบบ ที่ใช้ร่วมกัน และสิทธิ์แอคเคาต์ทั่วไปอื่นๆ ที่รวมแอคเคาต์ ดีฟอลต์จากโรงงาน
  - **R5.2.1:** นโยบายประกอบด้วยการลบ การปิดใช้งาน หรือการเปลี่ยนชื่อแอคเคาต์เหล่านั้น ที่เป็นไปได้ สำหรับแอคเคาต์เหล่านั้นที่ยังต้องเปิดใช้งานไว้ รหัสผ่านจะถูกเปลี่ยนก่อนการทำให้ระบบกลับมาให้บริการต่อ

- **R5.2.2:** Responsible Entity ระบุบุคคลเหล่านั้นให้มีการเข้าถึงแอคเคาต์ ที่ใช้ร่วมกัน
- **R5.2.3:** โดยที่แอคเคาต์เหล่านั้นต้องถูกใช้ร่วมกัน Responsible Entity มีนโยบายสำหรับ การจัดการการใช้งานแอคเคาต์เหล่านั้นที่จำกัดการเข้าถึงแก่ผู้ใช้ที่ได้รับอนุญาตเท่านั้น แนวทาง การตรวจสอบการใช้งานแอคเคาต์ (อัตโนมัติหรือด้วยตนเอง) และขั้นตอนสำหรับการรักษาความปลอดภัย แอคเคาต์ถ้ามีการ เปลี่ยนตัวบุคคล (ตัวอย่างเช่น การเปลี่ยนแปลงในการมอบหมาย หรือการสิ้นสุด)

- **R5.3:** อย่างน้อย Responsible Entity จำเป็นต้องใช้รหัสผ่าน กับสิ่งต่อไปนี้ เท่าที่เป็นไปได้ทางเทคนิค:
  - **R5.3.1:** รหัสผ่านแต่ละตัวต้องมีอย่างน้อย 6 อักขระ
  - **R5.3.2:** รหัสผ่านแต่ละตัวต้องประกอบด้วยอักขระตัวอักษร ตัวเลข และอักขระพิเศษ รวมกัน
  - **R5.3.3:** รหัสผ่านแต่ละตัวต้องถูกเปลี่ยนอย่างน้อยปีละครั้ง หรือบ่อยกว่านั้นขึ้นอยู่กับ ความเสี่ยง

**R6. การมอนิเตอร์สถานะการรักษาความปลอดภัย**

Responsible Entity ตรวจสอบให้แน่ใจว่า Cyber Assets ทั้งหมดภายใน Electronic Security Perimeter ที่เป็นไปได้ทางเทคนิค จะประยุกต์ใช้เครื่องมืออัตโนมัติ หรือการควบคุมกระบวนการในองค์กรเพื่อมอนิเตอร์ เหตุการณ์ระบบที่สัมพันธ์กับความปลอดภัยไซเบอร์

- **R6.1:** Responsible Entity ประยุกต์ใช้และจัดทำเอกสารกระบวนการเกี่ยวกับองค์กร และกลไก ด้านขั้นตอนและเทคนิคสำหรับการมอนิเตอร์เหตุการณ์การรักษาความปลอดภัยบน Cyber Assets ทั้งหมดภายใน Electronic Security Perimeter
- **R6.2:** การควบคุมการมอนิเตอร์การรักษาความปลอดภัยสร้างการแจ้งเตือนอัตโนมัติ หรือด้วยตนเองสำหรับเหตุการณ์ความปลอดภัยไซเบอร์ที่ตรวจพบ
- **R6.3:** Responsible Entity เก็บรักษาล็อกของเหตุการณ์ระบบที่เกี่ยวกับความปลอดภัย ไซเบอร์ ที่เป็นไปได้ทางเทคนิคเพื่อสนับสนุนการตอบสนองเหตุการณ์ที่จำเป็นใน Standard CIP-008-3
- **R6.4:** Responsible Entity เก็บรักษาล็อกทั้งหมดที่ระบุใน Requirement R6 เป็นเวลา 90 วัน
- **R6.5:** Responsible Entity ตรวจทานล็อกของเหตุการณ์ระบบที่สัมพันธ์กับความปลอดภัย ไซเบอร์ และเก็บรักษาเร็กคอร์ดที่บันทึกการตรวจสอบของล็อก

**R7. การทำลายหรือการปรับใช้ใหม่**

Responsible Entity สร้างและประยุกต์ใช้เมธอด กระบวนการ และโพรซีเดอร์สำหรับ การทำลายหรือการปรับใช้ใหม่ของ Cyber Assets ภายใน Electronic Security Perimeter ที่ระบุ และบันทึกใน Standard CIP-005-3

- **R7.1:** ก่อนการทำลายทรัพย์สิน Responsible Entity จะกำจัดหรือลบ สื่อบันทึกหน่วยเก็บข้อมูลเพื่อป้องกันการเรียกค้นที่ไม่ได้รับอนุญาตในข้อมูลที่มีความละเอียดอ่อนต่อความปลอดภัยบนไซเบอร์ หรือ ความเชื่อถือได้
- **R7.2:** ก่อนการปรับใช้ทรัพย์สินนั้นใหม่ อย่างน้อย Responsible Entity จะลบ สื่อบันทึกหน่วยเก็บข้อมูลเพื่อป้องกันการเรียกค้นที่ไม่ได้รับอนุญาตในข้อมูลที่มีความละเอียดอ่อนต่อความปลอดภัยบนไซเบอร์ หรือ ความเชื่อถือได

**CIP-010-1 — Cyber Security — Configuration Change Management and Vulnerability Assessments**

**R1:** Responsible Entity ประยุกต์ใช้ในแนวทางที่ระบุ ประเมินค่า และแก้ไข ความขาดแคลนอย่างน้อยหนึ่งกระบวนการที่ระบุที่รวมแต่ละส่วนของข้อกำหนดที่ บังคับใช้ได้เข้าไว้ด้วยกัน

# การจัดการความปลอดภัยและความร่วมมืออัตโนมัติ

ศึกษาเกี่ยวกับขั้นตอนการวางแผนและนำโปรไฟล์ความปลอดภัยและความเข้ากันได้อัตโนมัติของ PowerSC บนกลุ่มระบบตาม ขั้นตอนควบคุมและความเข้ากันได้ด้าน IT ที่ยอมรับ

ส่วนหนึ่งของความเข้ากันได้และการควบคุม IT ระบบที่รันบนเวิร์กโหลดเสมือน และคลาสความปลอดภัยของข้อมูลต้องถูกจัดการ และกำหนดคอนฟิกให้สอดคล้องกัน เมื่อต้องการวางแผนและปรับใช้การปฏิบัติตามระบบ ดำเนิน งานต่อไปนี้:

## การจำแนกกลุ่มทำงานของระบบ

คำแนะนำ ความเข้ากันได้และการควบคุม IT กล่าวว่า ระบบที่รันบนเวิร์กโหลดเสมือน และคลาสความปลอดภัยของข้อมูลต้องถูกจัดการ และกำหนดคอนฟิกให้สอดคล้องกัน ดังนั้น คุณต้องจำแนกระบบทั้งหมด ในเวิร์กกรุ๊ปเดียวกัน

## การใช้ระบบทดสอบที่ไม่ใช้งานจริงสำหรับตการเซ็ตอัพเริ่มต้น

ใช้โปรไฟล์ความเข้ากันได้ที่เหมาะสมของ PowerSC เพื่อทดสอบระบบ

พิจารณาตัวอย่างต่อไปนี้ สำหรับการปรับใช้โปรไฟล์การปฏิบัติตามไปยังระบบปฏิบัติการ AIX

ตัวอย่างที่ 1: ใช้ `DoD.xml`

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

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

ในตัวอย่างนี้ ไม่มีกฎที่ล้มเหลว นั้นคือ `Failedrules=0` นี้หมายความว่ากฎทั้งหมดถูกถูกนำไปใช้เสร็จสมบูรณ์ และเฟส การทดสอบสามารถเริ่มทำงานได้ ถ้ามีความล้มเหลว เอาต์พุตโดยละเอียดถูกสร้าง

ตัวอย่างที่ 2: ใช้ `PCI.xml` ที่มีความล้มเหลว

```
# aixpert -f /etc/security/aixpert/custom/PCI.xml
do_action(): rule(pci_grpck) : failed.
Processedrules=85       Passedrules=84  Failedrules=1   Level=AllRules

Input file=/etc/security/aixpert/custom/PCI.xml
```

ความล้มเหลว ของกฎ `pci_grpck` ต้องได้รับการแก้ไขไข สาเหตุ ที่เป็นไปได้สำหรับความล้มเหลวประกอบด้วยเหตุผลต่อไปนี้:

- กฎไม่สามารถใช้ได้กับสภาวะแวดล้อมและต้องถูกลบออก
- เกิดประเด็นขึ้นบนระบบที่ต้องแก้ไข

# การค้นหาสาเหตุของกฎที่ล้มเหลว

ในกรณีส่วนใหญ่ ไม่มีความล้มเหลวเมื่อใช้โปรไฟล์ความปลอดภัยและความเข้ากันได้ของ PowerSC อย่างไรก็ตาม ระบบอาจมีข้อกำหนดล่วงหน้าที่เกี่ยวข้อง กับการติดตั้ง ซึ่งอาจหายไปหรือประเด็นอื่นที่ต้องการความสนใจจาก ผู้ดูแลระบบ

สาเหตุของความล้มเหลวสามารถตรวจสอบได้โดยใช้ตัวอย่าง ต่อไปนี้:

ดูไฟล์ /etc/security/aixpert/custom/PCI.xml และค้นหากฎที่ล้มเหลว ในตัวอย่างนี้ กฎคือ pci_grpck รันคำสั่ง **fgrep** ค้นหากฎที่ล้มเหลว pci_grpck และดูกฎ XML ที่เกี่ยวข้อง

```
fgrep -p pci_grpck /etc/security/aixpert/custom/PCI.xml
<AIXPertEntry name="pci_grpck" function="grpck"
<AIXPertRuleType type="DLS"/
<AIXPertDescription&gt;Implements portions of PCI Section 8.2,
Check group definitions: Verifies the correctness of group definitions and fixes the errors
</AIXPertDescription
<AIXPertPrereqList&gt;bos.rte.security,bos.rte.date,bos.rte.ILS</AIXPertPrereqList
<AIXPertCommand
/etc/security/aixpert/bin/execmds</AIXPertCommand
<AIXPertArgs
"/usr/sbin/grpck -y ALL; /usr/sbin/grpck -n ALL"</AIXPertArgs
<AIXPertGroup
User Group System and Password Definitions</AIXPertGroup
</AIXPertEntry
```

จากกฎ pci_grpck คำสั่ง /usr/sbin/grpck สามารถเห็นได้

## การอัพเดตกฎที่ล้มเหลว

เมื่อใช้โปรไฟล์ความปลอดภัยและความร่วมมือของ PowerSC คุณสามารถตรวจหาข้อผิดพลาด

ระบบอาจมีสิ่งที่จำเป็นต้องมีในการติดตั้งบางอย่างหายไป หรือปัญหา อื่นๆ ที่จำเป็นต้องได้รับการดูแลจากผู้ดูแลระบบ หลังจากพบคำสั่ง ที่เป็นสาเหตุให้กฎล้มเหลว ให้ตรวจสอบระบบเพื่อทำความเข้าใจ คำสั่งคอนฟิกูเรชันที่ล้มเหลวนั้น ระบบอาจมีประเด็นด้านความปลอดภัย ซึ่งอาจเป็นในกรณีที่กฎเฉพาะไม่เหมาะสม กับสภาวะแวดล้อมของระบบ จากนั้นให้สร้างโปรไฟล์ความปลอดภัย กำหนดเอง

## การสร้างโปรไฟล์คอนฟิกูเรชันความปลอดภัย

ถ้ากฎไม่เหมาะสมกับสภาวะแวดล้อมของระบบที่ระบุ องค์กรความเข้ากันได้ส่วนใหญ่อนุญาตข้อยกเว้นที่มีเอกสารประกอบ

เมื่อต้องการลบกฎ และสร้างนโยบายการรักษาความปลอดภัยแบบกำหนดเอง และ ไฟล์คอนฟิกูเรชัน ดำเนินขั้นตอนต่อไปนี้:

1. คัดลอกเนื้อหาของไฟล์ต่อไปี้ลงในไฟล์เดียวชื่อ /etc/security/aixpert/custom/*<my_security_policy>*.xml:
   /etc/security/aixpert/custom/[PCI.xml|DoD.xml|SOX-COBIT.xml]
2. แก้ไขไฟล์ *<my_security_policy>*.xml โดยลบบทบาทที่ไม่สามารถเรียกทำงานได้จากแท็ก XML ที่เปิด <AIXPertEntry name... จนถึงแท็ก XML ที่ปิด </AIXPertEntry

คุณสามารถแทรกกฎคอนฟิกูเรชันเพิ่มเติมเพื่อความปลอดภัยได้ แทรก กฎเพิ่มเติมไปยังสกีมา XML AIXPertSecurityHardening คุณไม่สามารถเปลี่ยนแปลงโปรไฟล์ PowerSC ได้โดยตรง แต่คุณสามารถกำหนดลักษณะโปรไฟล์ได้เอง

สำหรับสภาวะแวดล้อมส่วนใหญ่ คุณต้องสร้างนโยบาย XML กำหนดเอง เมื่อต้องการ แจกจ่ายโปรไฟล์ลูกค้าไปยังอีกระบบ คุณต้องคัดลอก นโยบาย XML กำหนดเองอย่างปลอดภัยไปยังระบบที่ต้องการคอนฟิกูเรชัน เดียวกัน โปรโตคอลแบบปลอดภัย เช่น secure file transfer protocol (SFTP) ใช้เพื่อแจกจ่ายนโยบาย XML แบบกำหนดเองไปยังอีกระบบ และโปรไฟล์ถูกเก็บในตำแหน่งที่ปลอดภัย /etc/security/aixpert/custom/*<my_security_policy.xml>*/etc/security/aixpert/custom/

ล็อกออนเข้าสู่ระบบที่สร้างโปรไฟล์กำหนดเองไว้ และรันคำสั่งต่อไปนี้:

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

## การทดสอบแอ็พพลิเคชันด้วย AIX Profile Manager

กำหนดคอนฟิกความปลอดภัยสามารถมีผลกระทบกับแอ็พพลิเคชัน และวิธีการเข้าถึงและจัดการระบบ ซึ่งเป็นสิ่งสำคัญที่จะทดสอบ แอ็พพลิเคชันและวิธีการจัดการที่คาดไว้ของระบบ ก่อนที่จะนำระบบเข้าสู่สภาวะแวดล้อมการใช้งานจริง

มาตรฐานความเข้ากันเพื่อควบคุมกำหนดการกำหนดคอนฟิก ที่มีความเข้มงวดมากยิ่งขึ้นกว่าการกำหนดคอนฟิกที่มีดั้งเดิม เมื่อต้องการทดสอบระบบ ให้ปฏิบัติตามขั้นตอนต่อไปนี้:

1. เลือก **ดูและจัดการโปรไฟล์** จากหน้าต่างย่อยด้านขวาของ หน้ายินดีต้อนรับ AIX Profile Manager
2. เลือกโปรไฟล์ที่ใช้โดยเท็มเพลตเพื่อนำไปใช้กับ ระบบที่จะติดตาม
3. คลิก **เปรียบเทียบ**
4. เลือกกลุ่มที่ถูกจัดการ หรือเลือกแต่ละระบบภายใน กลุ่ม และคลิก **เพิ่ม** เพื่อเพิ่มกลุ่มใน กล่องที่เลือก
5. คลิก **ตกลง**

การดำเนินการเปรียบเทียบเริ่มทำงาน

## การมอนิเตอร์ระบบสำหรับการปฏิบัติตามมาตรฐานอย่างต่อเนื่องด้วย AIX Profile Manager

กำหนดคอนฟิกความปลอดภัยสามารถมีผลกระทบกับแอ็พพลิเคชัน และวิธีการเข้าถึงและจัดการระบบ สิ่งสำคัญคือมอนิเตอร์ แอ็พพลิเคชัน และเมธอดการจัดการที่ควรมีของระบบ เมื่อปรับใช้ระบบในสภาวะแวดล้อมการใช้งานจริง

เมื่อต้องการใช้ AIX Profile Manager เพื่อมอนิเตอร์ระบบ AIX ดำเนิน ขั้นตอนต่อไปนี้:

1. เลือก **ดูและจัดการโปรไฟล์** จากหน้าต่างย่อยด้านขวาของ หน้ายินดีต้อนรับ AIX Profile Manager
2. เลือกโปรไฟล์ที่ใช้โดยเท็มเพลตเพื่อนำไปใช้กับ ระบบที่จะติดตาม
3. คลิก **เปรียบเทียบ**
4. เลือกกลุ่มที่ถูกจัดการ หรือเลือกระบบเฉพาะภายใน กลุ่ม และเพิ่มไปยังกลุ่มที่เลือก
5. คลิก **ตกลง**

การดำเนินการเปรียบเทียบเริ่มทำงาน

---

## การกำหนดคอนฟิกความปลอดภัยและความร่วมมืออัตโนมัติของ PowerSC

ศึกษาขั้นตอนเพื่อกำหนดค่าคอนฟิก PowerSC สำหรับ Security and Compliance Automation จากบรรทัดคำสั่งโดยใช้ AIX Profile Manager

## การกำหนดคอนฟิกค่าติดตั้งอ็อพชันความร่วมมือ PowerSC

เรียนรู้พื้นฐานของคุณลักษณะการทำให้การรักษาความปลอดภัย และ ความเข้ากันได้กับ PowerSC เป็นอัตโนมัติ ทดสอบการกำหนด คอนฟิก บนระบบทดสอบที่ไม่ใช่การใช้งาน จริง และวางแผน และปรับใช้การตั้งค่า เมื่อคุณนำคอนฟิกูเรชันความร่วมมือ ไปใช้ ค่าติดตั้งจะเปลี่ยนแปลงค่าติดตั้งคอนฟิกูเรชันจำนวนมาก บนระบบปฏิบัติการ

**หมายเหตุ:** มาตรฐานความเข้ากันได้และโปรไฟล์บางอย่างปิดการใช้งาน Telnet เนื่องจาก Telnet ใช้ข้อความรหัสผ่านโดยตรง ดังนั้น คุณต้องติดตั้ง, กำหนดคอนฟิก และใช้งาน Open SSH คุณสามารถใช้สื่อของความปลอดภัยอื่นๆ การสื่อสารกับระบบที่ถูกกำหนดคอนฟิก ความเข้ากันได้มาตรฐานเหล่านี้ จำเป็นต้องใช้ล็อกอิน `root` เพื่อปิดการใช้งาน กำหนดคอนฟิกผู้ใช้ที่ไม่ใช่ root หนึ่งรายหรือมากกว่าก่อนที่คุณจะดำเนินการใช้ คอนฟิกูเรชันที่เปลี่ยนแปลง คอนฟิกูเรชันนี้ไม่ได้ปิดใช้งาน root, และคุณสามารถล็อกอินเป็นผู้ใช้ที่ไม่ใช่ root และรันคำสั่ง **su** กับ root ทดสอบว่าคุณสามารถสร้างการเชื่อมต่อ SSH ไปยังระบบล็อกอินเป็นผู้ใช้ที่ไม่ใช่ root และรันคำสั่ง `root`

เมื่อต้องการเข้าถึงโปรไฟล์การกำหนดคอนฟิก DoD, PCI, SOX หรือ COBIT ใช้ไดเร็กทอรีต่อไปนี้:

- โปรไฟล์ในระบบปฏิบัติการ AIX อยู่ในไดเร็กทอรี `/etc/security/aixpert/custom`
- โปรไฟล์ใน Virtual I/O Server (VIOS) อยู่ในไดเร็กทอรี `/etc/security/aixpert/core`

## การกำหนดคอนฟิกความเข้ากันได้ PowerSC จากบรรทัดรับคำสั่ง

นำไปใช้หรือตรวจสอบโปรไฟล์ความเข้ากันได้โดยใช้คำสั่ง **pscxpert** บนระบบ AIX และคำสั่ง **viosecure** บน Virtual I/O Server (VIOS)

เพื่อปรับใช้โปรไฟล์ความเข้ากันได้ PowerSC บนระบบ AIX ให้ป้อนหนึ่งในคำสั่งต่อไปนี้ ซึ่งจะขึ้นอยู่กับ ระดับมาตรฐานความปลอดภัยที่คุณต้องการปรับใช้

*ตารางที่ 11. คำสั่ง PowerSC สำหรับ AIX*

| คำสั่ง | มาตรฐานความเข้ากันได้ |
|---|---|
| **% pscxpert -f /etc/security/aixpert/custom/DoD.xml** | *คู่มือการประยุกต์ใช้ด้านเทคนิคของการรักษาความปลอดภัย US Department of Defense UNIX* |
| **% pscxpert -f /etc/security/aixpert/custom/Hipaa.xml** | *Heath Insurance Portability and Accountability Act* |
| **% pscxpert -f /etc/security/aixpert/custom/PCI.xml** | *มาตรฐานความปลอดภัยข้อมูลของ Payment card industry* |
| **% pscxpert -f /etc/security/aixpert/custom/SOX-COBIT.xml** | *Sarbanes-Oxley Act ประจำปี 2002 – COBIT IT Governance* |

เมื่อต้องการใช้โปรไฟล์ความเข้ากันได้ PowerSC บนระบบ VIOS ป้อนหนึ่งในคำสั่งต่อไปนี้สำหรับระดับความเข้ากันได้ของการรักษาความปลอดภัย ที่คุณต้องการใช้

*ตารางที่ 12. คำสั่ง PowerSC สำหรับ Virtual I/O Server*

| คำสั่ง | มาตรฐานความเข้ากันได้ |
|---|---|
| **% viosecure -file /etc/security/aixpert/custom/DoD.xml** | *คู่มือการประยุกต์ใช้ด้านเทคนิคของการรักษาความปลอดภัย US Department of Defense UNIX* |
| **% viosecure -file /etc/security/aixpert/custom/Hipaa.xml** | *Heath Insurance Portability and Accountability Act* |
| **% viosecure -file /etc/security/aixpert/custom/PCI.xml** | *มาตรฐานความปลอดภัยข้อมูลของ Payment card industry* |
| **% viosecure -file /etc/security/aixpert/custom/SOX-COBIT.xml** | *Sarbanes-Oxley Act ประจำปี 2002 – COBIT IT Governance* |

คำสั่ง **pscxpert** บนระบบ AIX และคำสั่ง **viosecure** ใน VIOS อาจใช้เวลาในการรันเนื่องจากกำลังตรวจสอบหรือตั้งค่าระบบทั้งหมด และทำการเปลี่ยนแปลงคอนฟิกูเรชันที่เกี่ยวข้องกับความปลอดภัย เอาต์พุตจะคล้ายกับที่แสดง ตามตัวอย่างต่อไปนี้:

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

อย่างไรก็ตาม กฎบางข้อล้มเหลวขึ้นอยู่กับสภาวะแวดล้อม AIX ชุดการติดตั้ง และการกำหนดคอนฟิกก่อนหน้านี้

ตัวอย่าง กฎเบื้องต้นสามารถล้มเหลว เนื่องจากระบบไม่มี fileset การติดตั้งที่ต้องการ ซึ่งจำเป็นต้องเข้าใจแต่ละ ความล้มเหลว และการแก้ไขก่อนนำโปรไฟล์ความเข้ากันได้ไปใช้ ผ่านศูนย์ข้อมูล

**หลักการที่เกี่ยวข้อง:**

"การจัดการความปลอดภัยและความร่วมมืออัตโนมัติ" ในหน้า 123
ศึกษาเกี่ยวกับขั้นตอนการวางแผนและนำโปรไฟล์ความปลอดภัยและความเข้ากันได้อัตโนมัติของ PowerSC บนกลุ่มระบบ ตาม ขั้นตอนควบคุมและความเข้ากันได้ด้าน IT ที่ยอมรับ

## การกำหนดคอนฟิกความร่วมมือของ PowerSC กับตัวจัดการโปรไฟล์ AIX

ศึกษาขั้นตอนการกำหนดคอนฟิกด้านความปลอดภัยและโปรไฟล์ความร่วมมือ PowerSC และนำคอนฟิกูเรชันไปใช้กับระบบที่ถูกจัดการของ AIX โดยใช้ตัวจัดการโปรไฟล์ AIX

เมื่อต้องการกำหนดคอนฟิกโปรไฟล์ความปลอดภัยและความร่วมมือ PowerSC โดยใช้ตัวจัดการโปรไฟล์ AIX ให้ปฏิบัติตามขั้นตอนต่อไปนี้:

1. ล็อกอินเข้าสู่ IBM Systems Director และเลือกตัวจัดการโปรไฟล์ AIX
2. สร้างเท็มเพลตตามหนึ่งในโปรไฟล์ความปลอดภัยและความร่วมมือของ PowerSC โดยปฏิบัติตามขั้นตอนต่อไปนี้:
   a. คลิก **ดูและจัดการเท็มเพลต** จากบานหน้าต่างด้านขวาของ หน้ายินดีต้อนรับตัวจัดการโปรไฟล์ AIX
   b. คลิก **สร้าง**
   c. คลิก **ระบบปฏิบัติการ** จากรายการ **ชนิดเท็มเพลต**
   d. ตั้งชื่อเท็มเพลตในฟิลด์ **ชื่อเท็มเพลตคอนฟิกูเรชัน**
   e. คลิก **ทำต่อ** > **บันทึก**
3. เลือกโปรไฟล์ที่จะใช้กับเท็มเพลตโดยเลือก **เรียกดู** ภายใต้อ็อพชัน **เลือกโปรไฟล์ที่จะใช้สำหรับเท็มเพลตนี้** โปรไฟล์จะแสดงผลไอเท็มต่อไปนี้:
   - `ice_DLS.xml` คือระดับการรักษาความปลอดภัยดีฟอลต์ของ ระบบปฏิบัติการ AIX
   - `ice_DoD.xml` คือ Department of Defense Security and Implementation Guide สำหรับการตั้งค่า UNIX
   - `ice_HLS.xml` คือความปลอดภัยระดับสูงทั่วไป สำหรับค่าติดตั้ง AIX
   - `ice_LLS.xml` คือความปลอดภัยระดับต่ำสำหรับค่าติดตั้ง AIX
   - `ice_MLS.xml` คือความปลอดภัยระดับกลาง สำหรับค่าติดตั้ง AIX
   - `ice_PCI.xml` คือการตั้งค่า Payment Card Industry สำหรับระบบปฏิบัติการ AIX
   - `ice_SOX.xml` คือการตั้งค่า SOX หรือ COBIT สำหรับระบบปฏิบัติการ AIX
4. ลบโปรไฟล์ใดๆ ออกจากกล่องที่เลือก
5. เลือก **เพิ่ม** เพื่อย้ายโปรไฟล์ที่ร้องขอไปไว้ใน กล่องที่เลือก
6. คลิก **บันทึก**

เมื่อต้องการปรับใช้การกำหนดคอนฟิกบนระบบที่ถูกจัดการ AIX ดำเนินขั้นตอนต่อไปนี้:

1. เลือก **ดูและจัดการเท็มเพลต** จากบานหน้าต่างด้านขวาของ หน้ายินดีต้อนรับของตัวจัดการโปรไฟล์ AIX
2. เลือกเท็มเพลตที่ต้องการนำไปใช้

3. คลิก **นำไปใช้**
4. เลือกระบบเพื่อปรับใช้โปรไฟล์ และคลิก **เพิ่ม** เพื่อ ย้ายโปรไฟล์ที่จำเป็นไปยังกล่องที่เลือก
5. คลิก **ตกลง** เพื่อนำเท็มเพลตคอนฟิกูเรชันไปใช้ ระบบ จะถูกกำหนดคอนฟิกตามเท็มเพลตที่เลือกของโปรไฟล์

เพื่อให้การปรับใช้สำเร็จสำหรับ DoD, PCI หรือ SOX นั้น PowerSC Standard Edition ต้องติดตั้งที่จุดปลายของระบบ AIX ถ้าระบบที่กำลังถูกปรับใช้ไม่มี PowerSC ติดตั้งอยู่ การปรับใช้จะล้มเหลว IBM Systems Director นำเท็มเพลตคอนฟิกูเรชันไปใช้กับจุดปลายของระบบ AIX ที่เลือก และกำหนดคอนฟิกตามข้อกำหนดความเข้ากันได้

**ข้อมูลที่เกี่ยวข้อง**:

ตัวจัดการโปรไฟล์ AIX

IBM Systems Director

# PowerSC Real Time Compliance

คุณลักษณะ PowerSC Real Time Compliance มอนิเตอร์ระบบ AIX ที่เปิดใช้งานอย่างต่อเนื่องเพื่อให้แน่ใจว่าถูกกำหนด สอดคล้องกันและมีความปลอดภัย

คุณลักษณะ PowerSC Real Time Compliance จะทำงานร่วมกับนโยบาย PowerSC Compliance Automation และ AIX Security Expert เพื่อให้มีการแจ้งเตือนเมื่อเกิดการละเมิดมาตรฐาน หรือเมื่อไฟล์ที่มอนิเตอร์มีการเปลี่ยนแปลง เมื่อนโยบายการกำหนดคอนฟิกการรักษาความปลอดภัยของระบบ ถูกละเมิด คุณลักษณะ PowerSC Real Time Compliance จะส่งอีเมลหรือข้อความตัวอักษรเพื่อแจ้งเตือน ผู้ดูแลระบบ

คุณลักษณะ PowerSC Real Time Compliance เป็นคุณลักษณะการรักษาความปลอดภัยแบบป้องกันที่สนับสนุนโปรไฟล์ ความเข้ากันได้ที่กำหนดไว้ล่วงหน้า หรือเปลี่ยนแปลง ที่รวมความเข้ากันได้ของ Department of Defense Security Technical Implementation Guide, Payment Card Industry Data Security Standard, Sarbanes-Oxley Act และ COBIT ซึ่งจะมีรายการไฟล์ดีฟอลต์เพื่อมอนิเตอร์การเปลี่ยนแปลง แต่คุณ สามารถเพิ่มไฟล์ในรายการได้

## การติดตั้ง PowerSC Real Time Compliance

คุณลักษณะ PowerSC Real Time Compliance ถูกติดตั้ง กับ PowerSC Standard Edition เวอร์ชัน 1.1.4 หรือใหม่กว่า และไม่เป็น ส่วนหนึ่งของระบบปฏิบัติการ AIX ฐาน

เมื่อต้องการติดตั้ง PowerSC Real Time Compliance ดำเนินขั้นตอนต่อไปนี้:

1. ให้แน่ใจว่าคุณกำลังรันหนึ่งในระบบปฏิบัติการ AIX ต่อไปนี้บนระบบที่คุณ กำลังติดตั้งคุณลักษณะ PowerSC Real Time Compliance:
   - IBM AIX 6 ที่มีเทคโนโลยีระดับ 7 หรือใหม่กว่า ที่มี AIX Event Infrastructure สำหรับ AIX และ AIX Clusters (bos.ahafs 6.1.7.0) หรือใหม่กว่า
   - IBM AIX 7 ที่มีเทคโนโลยีระดับ 1 หรือใหม่กว่า ที่มี AIX Event Infrastructure สำหรับ AIX และ AIX Clusters (bos.ahafs 7.1.1.0) หรือใหม่กว่า
   - AIX เวอร์ชัน 7.2 หรือใหม่กว่า ที่มี AIX Event Infrastructure สำหรับ AIX และ AIX Clusters (bos.ahafs 7.2.0.0) หรือใหม่กว่า
2. เมื่อต้องการอัพเดตหรือติดตั้งชุดไฟล์คุณลักษณะ PowerSC Real Time Compliance ให้ติดตั้งชุดไฟล์ `powerscStd.rtc` จากแพ็กเกจการติดตั้งสำหรับ PowerSC Standard Edition เวอร์ชัน 1.1.4 หรือใหม่กว่า

## การกำหนดค่า PowerSC Real Time Compliance

คุณสามารถกำหนดค่า PowerSC Real Time Compliance ให้ส่ง การแจ้งเตือนเมื่อมีการละเมิดโปรไฟล์ความเข้ากันได้ หรือการเปลี่ยนแปลงไปยังไฟล์ที่ มอนิเตอร์เกิดขึ้น บางตัวอย่างของโปรไฟล์ได้แก่ Department of Defense Security Technical Implementation Guide, Payment Card Industry Data Security Standard, Sarbanes-Oxley Act และ COBIT

คุณสามารถกำหนดค่า PowerSC Real Time Compliance โดยใช้ หนึ่งในเมธอดต่อไปนี้:

- ป้อนคำสั่ง **mkrtc**
- รันเครื่องมือ SMIT โดยป้อนคำสั่งต่อไปนี้:

  ```
  smit RTC
  ```

## การระบุไฟล์ที่มอนิเตอร์โดยคุณลักษณะ PowerSC Real Time Compliance

คุณลักษณะ PowerSC Real Time Compliance มอนิเตอร์รายการไฟล์ดีฟอลต์จากการตั้งค่าการรักษาความปลอดภัย ระดับสูง เพื่อทำการเปลี่ยนแปลง ซึ่งสามารถกำหนดเองโดยการเพิ่มหรือ ลบไฟล์ออกจากรายการไฟล์ในไฟล์ `/etc/security/rtc/rtcd_policy.conf`

มีสองเมธอดของการระบุเท็มเพลตความเข้ากันได้ที่ ถูกนำใช้บนระบบ หนึ่งเมธอดคือ ใช้คำสั่ง **pscxpert** และอีกหนึ่งเมธอดคือ ใช้ AIX Profile Manager กับ IBM Systems Director

เมื่อโปรไฟล์ความเข้ากันได้ถูกระบุ คุณสามารถเพิ่มไฟล์ เพิ่มเติมในรายการไฟล์เพื่อมอนิเตอร์โดยการรวมไฟล์ เพิ่มเติมใน ไฟล์ `/etc/security/rtc/rtcd_policy.conf` หลังจากไฟล์ถูกบันทึก รายการใหม่จะถูกนำใช้ทันที เป็นบรรทัดฐาน และมอนิเตอร์การเปลี่ยนแปลงโดยไม่ต้องรีสตาร์ทระบบ

## การตั้งค่าการแจ้งเตือนสำหรับ PowerSC Real Time Compliance

คุณต้องกำหนดค่าการแจ้งเตือนของคุณลักษณะ PowerSC Real Time Compliance โดยการระบุชนิดการแจ้งเตือน หรือผู้รับการแจ้งเตือน

สำหรับ rtcd daemon ซึ่งเป็นคอมโพเนนต์หลักของคุณลักษณะ PowerSC Real Time Compliance จัดหาข้อมูลเกี่ยวกับชนิดของการแจ้งเตือน และผู้รับจาก ไฟล์คอนฟิกูเรชัน `/etc/security/rtc/rtcd.conf` คุณสามารถแก้ไขไฟล์นี้เพื่ออัพเดตข้อมูลโดยใช้ เอดิเตอร์ข้อความ

**ข้อมูลที่เกี่ยวข้อง**:

รูปแบบไฟล์ /etc/security/rtc/rtcd.conf สำหรับ ความเข้ากันได้แบบเรียลไทม์

# 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

คุณสามารถกำหนดค่าคอนฟิกโลจิคัลพาร์ติชันทีเปิดใช้ 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 136
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 หากคุณไม่ได้สำเนาไฟล์นี้ไว้ 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 คุณจะใช้การดำเนินการ ใด (ข้อเสนอแนะประกอบด้วยการรวบรวมล็อก การตรวจสอบ การยกเลิกการเชื่อมต่อ ระบบออกจากเครือข่าย การปิดทำงานระบบ และการแจ้งผู้ใช้)
- มีระบบอื่นๆ ที่ถูกบุกรุกที่ต้องถูกตรวจสอบหรือไม่

**หลักการที่เกี่ยวข้อง:**

"การแก้ไขปัญหา Trusted Boot" ในหน้า 136
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 1.1.4" ในหน้า 7
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 13. การแก้ไขปัญหาสถานการณ์จำลองบางอย่างสำหรับความล้มเหลว*

| สาเหตุของความล้มเหลว | สาเหตุที่เป็นไปได้ของความล้มเหลว | การแก้ไขที่แนะนำ |
|---|---|---|
| การยืนยันไม่สมบูรณ์ | • ชื่อโฮสต์ไม่ถูกต้อง<br>• ไม่มีเส้นทางเครือข่ายระหว่างต้นทางและปลายทาง<br>• ข้อมูลประจำตัวการรักษาความปลอดภัยไม่ถูกต้อง | ตรวจสอบการเชื่อม Secure Shell (SSH) โดยใช้ คำสั่งต่อไปนี้:<br>`ssh ptsc@hostname`<br>หาก การเชื่อมต่อ SSH ประสบสำเร็จ ให้ตรวจสอบสาเหตุต่อไปนี้ สำหรับการยืนยันที่ล้มเหลว:<br>• ระบบที่กำลังถูกยืนยันไม่ได้รัน **tcsd** daemon<br>• ระบบที่กำลังถูกยืนยันไม่ได้เริ่มต้นด้วยคำสั่ง **ptsc** กระบวนการนี้ควรเกิดขึ้นโดยอัตโนมัติระหว่าง การเริ่มต้นระบบแต่จะตรวจสอบการมีอยู่ของไดเร็กทอรี `/var/ptsc/` บนตัวรวบรวม หากไดเร็กทอรี `/var/ptsc/` ไม่มีอยู่ ให้รันคำสั่งต่อไปนี้บนตัวรวบรวม:<br>`ptsc -i` |
| เฟิร์มแวร์ CEC มีการเปลี่ยนแปลง | • ใช้เฟิร์มแวร์ที่อัพเกรด<br>• LPAR ถูกโอนย้ายไปยังระบบที่รันเวอร์ชันที่แตกต่าง ของเฟิร์มแวร์ | ตรวจสอบระดับเฟิร์มแวร์ของระบบที่โฮสต์ LPAR |
| รีซอร์สที่จัดสรรให้กับ LPAR มีการเปลี่ยนแปลง | CPU หรือหน่วยความจำที่จัดสรรให้กับ LPAR มีการเปลี่ยนแปลง | ตรวจสอบโปรไฟล์ของพาร์ติชันใน HMC |

*ตารางที่ 13. การแก้ไขปัญหาสถานการณ์จำลองบางอย่างสำหรับความล้มเหลว (ต่อ)*

| สาเหตุของความล้มเหลว | สาเหตุที่เป็นไปได้ของความล้มเหลว | การแก้ไขที่แนะนำ |
|---|---|---|
| เฟิร์มแวร์มีการเปลี่ยนแปลงสำหรับอะแด็ปเตอร์ที่มีอยู่ใน LPAR | อุปกรณ์ฮาร์ดแวร์ถูกเพิ่มหรือลบออกจาก LPAR | ตรวจสอบโปรไฟล์พาร์ติชันใน HMC |
| รายการอุปกรณ์ที่ต่อพ่วงกับ LPAR มีการเปลี่ยนแปลง | อุปกรณ์ฮาร์ดแวร์ถูกเพิ่มหรือลบออกจาก LPAR | ตรวจสอบโปรไฟล์พาร์ติชันใน HMC |
| อิมเมจการบูตมีการเปลี่ยนแปลง ซึ่งรวมถึงเคอร์เนลของ ระบบปฏิบัติการ | • ใช้การอัพเดต AIX และตัวตรวจสอบไม่ได้รับรู้ถึงการอัพเดต<br>• คำสั่ง **bosboot** รันอยู่ | • ตรวจสอบกับผู้ดูแลระบบว่ามีการดำเนินการบำรุงรักษาใดๆ หรือไม่ ก่อนดำเนินการรีบูตครั้งล่าสุด<br>• ตรวจสอบล็อกบนตัวรวบรวมสำหรับกิจกรรมการบำรุงรักษา |
| LPAR ถูกบูตจากอุปกรณ์อื่น | • การลงทะเบียนถูกดำเนินการทันทีหลังจากการติดตั้งเครือข่าย<br>• ระบบถูกบูตจากอุปกรณ์การบำรุงรักษา | สามารถตรวจสอบแฟล็ก และอุปกรณ์การบูตโดยใช้คำสั่ง **bootinfo** หากการลงทะเบียนถูกดำเนินการทันที หลังจากการติดตั้ง Network Installation Management (NIM) และก่อน ทำการรีบูต รายละเอียดที่ลงทะเบียนไว้จะเกี่ยวข้องกับการติดตั้งเครือข่าย และไม่ใช่การบูตด้วยดิสก์ในครั้งถัดไป การลงทะเบียนนี้สามารถ แก้ไขโดยการลบการลงทะเบียน และทำการลงทะเบียนโลจิคัลพาร์ติชันใหม่ |
| เมนูบูต System Management Services (SMS) แบบโต้ตอบถูกเรียกใช้ | | กระบวนการบูตจะต้องรันอย่างต่อเนื่องโดยไม่ต้องมีการโต้ตอบของผู้ใช้ สำหรับระบบที่ไว้วางใจได้ การเข้าสู่เมนูการบูต SMS จะทำให้ การบูตไม่ถูกต้อง |
| ฐานข้อมูล Trusted Execution (TE) ถูกแก้ไข | • ไฟล์ไบนารีจะถูกเพิ่ม หรือลบออกจากฐานข้อมูล TE<br>• ไฟล์ไบนารีในฐานข้อมูลถูกอัพเดต | รันคำสั่ง **trustchk** เพื่อตรวจสอบฐานข้อมูล |

**หลักการที่เกี่ยวข้อง:**

"การจัดเตรียมสำหรับการแก้ไข" ในหน้า 132
ข้อมูล Trusted Boot ที่อธิบายไว้ในที่นี้จะทำหน้าที่เป็น แนวทางในการระบุสถานการณ์ที่อาจต้องแก้ไข ซึ่งไม่มีผลกับกระบวนการบูต

"แนวคิด Trusted Boot" ในหน้า 131
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

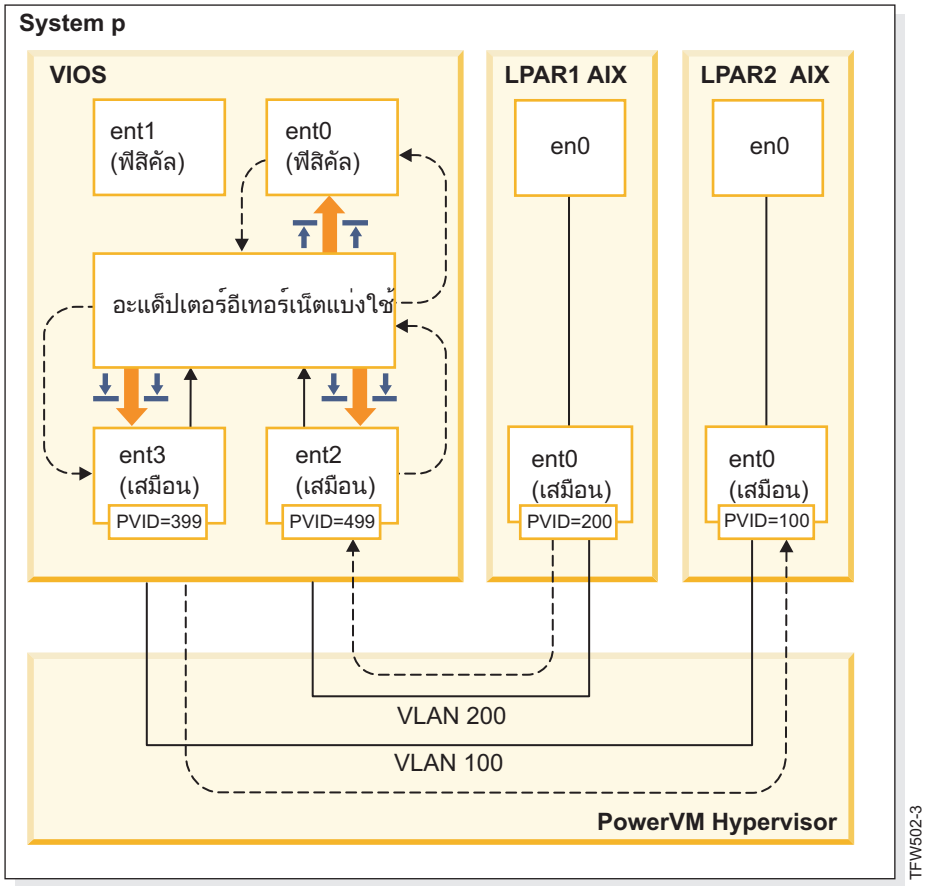
## แนวคิด Trusted Firewall

มีแนวคิดพื้นฐานบางอย่างที่ต้องเข้าใจเมื่อใช้ Trusted Firewall

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

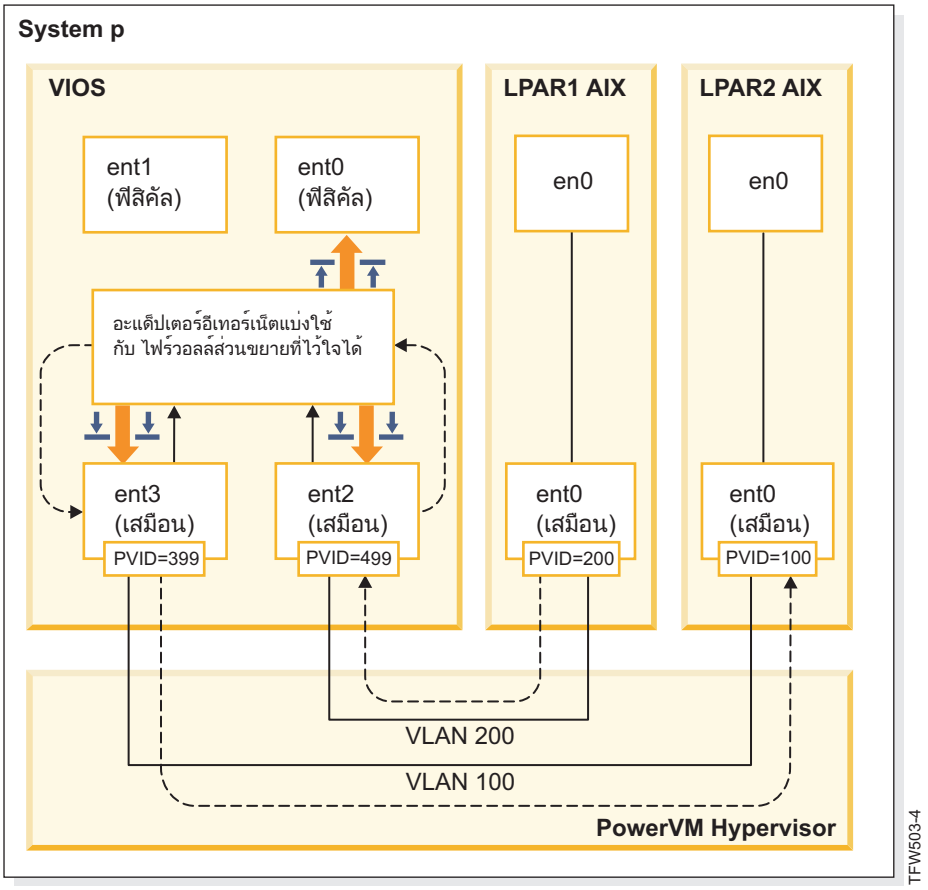
ด้วย Trusted Firewall คุณสามารถกำหนดค่าคอนฟิกกฎเพื่ออนุญาตให้ทราฟฟิก บางชนิดถ่ายโอนโดยตรงจากหนึ่ง VLAN บน Virtual I/O Server (VIOS) ไปยัง VLAN อื่นบน VIOS เดียวกัน ขณะที่ยังคงรักษาระดับการรักษาความปลอดภัยที่สูงโดยการจำกัด ทราฟฟิกชนิดอื่นๆ ซึ่งเป็นไฟล์วอลล์ที่สามารถกำหนดค่าคอนฟิกได้ภายในเวอร์ชวลไลเซชันเลเยอร์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

การใช้ตัวอย่างใน รูปที่ 1 ในหน้า 140 เป้าหมายคือสามารถถ่ายโอน 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 141




*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 1.1.4" ในหน้า 7
คุณต้องติดตั้ง fileset สำหรับแต่ละฟังก์ชันเฉพาะของ PowerSC Standard Edition

---

## การกำหนดค่าคอนฟิก Trusted Firewall

ต้องมีการตั้งค่าคอนฟิกูเรชันเพิ่มเติมสำหรับ คุณลักษณะ Trusted Firewall หลังจากที่มีการติดตั้ง

### Trusted Firewall Advisor

Trusted Firewall Advisor จะวิเคราะห์ทราฟฟิก ของระบบจากโลจิคัลพาร์ติชัน (LPARs) ที่แตกต่างกันเพื่อระบุข้อมูล เพื่อตรวจสอบว่าการรัน Trusted Firewall ช่วยให้มีประสิทธิภาพของระบบที่ดีขึ้นหรือไม่

หากฟังก์ชัน Trusted Firewall Advisor บันทึกปริมาณที่สำคัญ ของทราฟฟิกจาก LANs เสมือน (VLANs) ที่ต่างกันที่อยู่บนคอมเพล็กซ์อิเล็กทรอนิกส์กลางเดียวกัน การเปิดใช้ Trusted Firewall ควร จะมีประโยชน์กับระบบของคุณ

เมื่อต้องการเปิดใช้งาน Trusted Firewall Advisor ป้อนคำสั่ง ต่อไปนี้:

```
vlantfw -m
```

เมื่อต้องการแสดงผลลัพธ์ของ Trusted Firewall Advisor ป้อนคำสั่งต่อไปนี้:

```
vlantfw -D
```

เมื่อต้องการปิดใช้งาน Trusted Firewall Advisor ป้อน คำสั่งต่อไปนี้:

```
vlantfw -M
```

## การบันทึกล็อก Trusted Firewall

การบันทึกล็อก Trusted Firewall จะรวบรวมรายการเส้นทางทราฟฟิกเครือข่าย ภายในคอมเพล็กซ์อิเล็กทรอนิกส์กลาง รายการจะแสดงตัวกรอง ที่ Trusted Firewall ใช้เพื่อกำหนดเส้นทางทราฟฟิก

เมื่อ Trusted Firewall Advisor ระบุว่าเส้นทางทราฟฟิก ภายในทำให้มีประสิทธิภาพที่ดีขึ้น การบันทึกล็อก Trusted Firewall จะเก็บรักษา รายการเส้นทางไว้ในไฟล์ `svm.log` ขนาดของไฟล์ `svm.log` จำกัดอยู่ที่ 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`

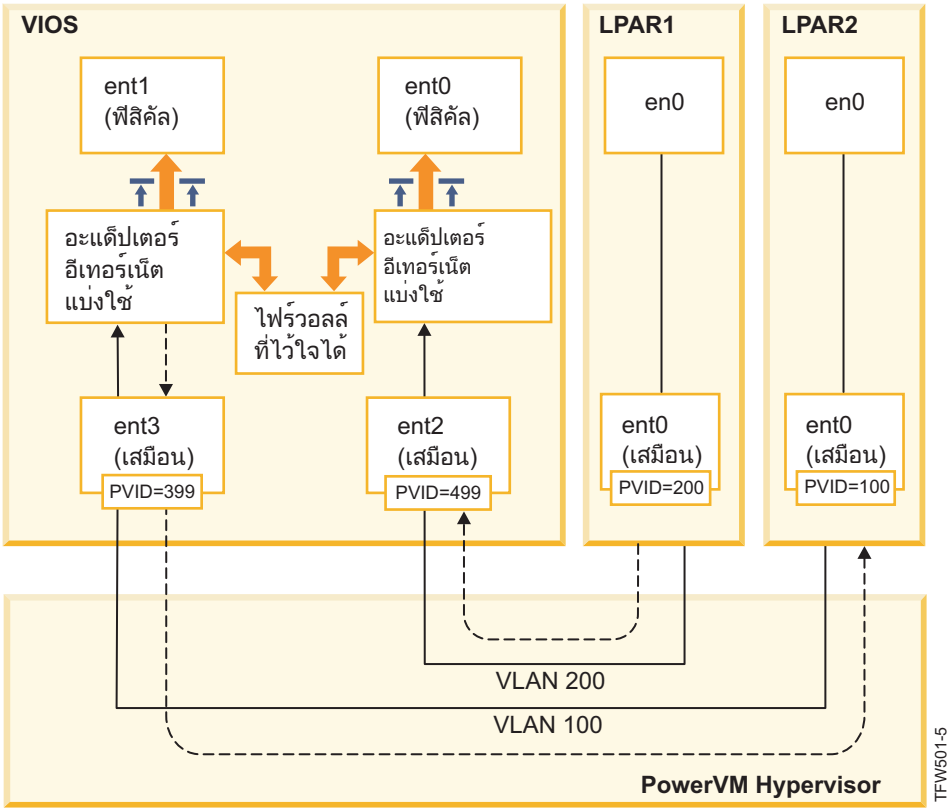
**หมายเหตุ:** คุณสามารถรันคำสั่งเพื่อเริ่มและหยุดทำงานการล็อก Trusted Firewall เมื่อคุณได้รับอนุญาตให้เป็นผู้ใช้ root เท่านั้น

## 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 3 ในหน้า 144 แสดง 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 โดยดีฟอลต์ ขึ้นอยู่กับรายการพอร์ตและโปรโตคอล 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 168

"คำสั่ง mkvfilt" ในหน้า 171

"คำสั่ง vlantfw" ในหน้า 187

**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 145

คุณสามารถสร้างกฎเพื่อเปิดใช้การกำหนดเส้นทาง Trusted Firewall ข้าม VLAN

**สิ่งอ้างอิงที่เกี่ยวข้อง:**

"คำสั่ง lsvfilt" ในหน้า 170

"คำสั่ง rmvfilt" ในหน้า 186

# Trusted Logging

PowerVM® Trusted Logging จะทำให้โลจิคัลพาร์ติชัน AIX (LPARs) เขียนลงล็อกไฟล์ที่เก็บบน 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 ทำให้ข้อมูลล็อกจากหลาย LPARs ไคลเอ็นต์ถูกรวบรวม เข้าไว้ในระบบไฟล์เดียว ซึ่งเข้าถึงได้จาก 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

ชื่อของสองคอมโพเนนต์สามารถตั้งค่าโดยผู้ดูแลระบบ VIOS เป็นค่าใดๆ แต่ชื่อไคลเอ็นต์โดยทั่วไปจะเหมือนกันสำหรับล็อกเสมือน ทั้งหมดที่เชื่อมต่อกับ LPAR ที่กำหนด (ตัวอย่างเช่น ชื่อ โฮสต์ของ 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 ที่มีเทคโนโลยีระดับ 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 1.1.4" ในหน้า 7
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 150

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 150

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 ข้อมูลไปยังล็อกเสมือนไฟล์ในระบบไฟล์ /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>
```

เพื่ออิมพอร์ตใบรับรองจากไคลเอ็นต์ ให้ป้อน คำสั่งต่อไปนี้:

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

## โปรโตคอล Trusted Network Connect

โปรโตคอล Trusted Network Connect (TNC) จะถูกใช้กับ เฟรมเวิร์ก TNC เพื่อรักษาบูรณภาพของเครือข่าย

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 175

---

## 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 160

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 175

**ข้อมูลที่เกี่ยวข้อง:**

"การติดตั้ง PowerSC Standard Edition 1.1.4" ในหน้า 7

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 175

## 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 175

## 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` เพื่อยอมรับข้อตกลงการใช้ซอฟต์แวร์ทั้งหมดเมื่อรันการอัพ

เดตไคลเอ็นต์โดยดีฟอลต์ 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 และการอัพเดต ไคลเอ็นต์ แฟซิลิตี้คือ `user` และลำดับความสำคัญคือ `info` ตัวอย่างนี้คือ `user.info`

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

**สิ่งอ้างอิงที่เกี่ยวข้อง:**

"คำสั่ง psconf" ในหน้า 175

**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 175

## 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 175

---

## การบริหารจัดการ Trusted Network Connect และ Patch

ศึกษาวิธีจัดการ Trusted Network Connect (TNC) เพื่อใช้งานต่างๆ 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 175

## การสร้างนโยบายสำหรับไคลเอ็นต์ Trusted Network Connect

ศึกษาวิธีการตั้งค่านโยบายที่เชื่อมโยงกับไคลเอ็นต์ Trusted Network Connect (TNC)

คอนโซล `psconf` จะมี อินเตอร์เฟสที่จำเป็นในการจัดการนโยบาย TNC แต่ละไคลเอ็นต์หรือกลุ่ม ของไคลเอ็นต์สามารถเชื่อมโยงกับนโยบาย

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 ตัวอย่างเช่น หากไคลเอ็นต์ อยู่บน 6100-02-01 และคุณระบุนโยบาย fileset เป็น 7100-03-04 และ 6100-02-03 ดังนั้น 6100-02-03 จะถูกบังคับใช้บนไคลเอ็นต์

**สิ่งอ้างอิงที่เกี่ยวข้อง**:

"คำสั่ง psconf" ในหน้า 175

## 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 175

## 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 175

## 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 175

## การจัดการนโยบายการจัดการแพตช์

คำสั่ง **pmconf** จะถูกใช้เพื่อกำหนดค่าคอนฟิกนโยบายการจัดการแพตช์

นโยบายการจัดการแพตช์จะมีข้อมูล เช่น IP แอดเดรสของเซิร์ฟเวอร์ TNC และช่วงเวลาในการเริ่มต้นการอัพเดต SUMA

เพื่อจัดการนโยบายการจัดการแพตช์ ให้ป้อนคำสั่งต่อไปนี้:

```
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 171

## 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 จะได้รับการรับรอง และปลอดภัย แต่ละระบบจะมีคีย์และใบรับรองของตัวเอง ที่สร้างขึ้นเมื่อรันคำสั่งเริ่มต้นสำหรับ คอมโพเนนต์ กระบวนการนี้จะโปร่งใสต่อผู้ดูแลระบบ และต้องการ ความเกี่ยวข้องที่น้อยลงจากผู้ดูแลระบบ เมื่อไคลเอ็นต์ถูกตรวจสอบในครั้งแรก ใบรับรองของไคลเอ็นต์จะถูกอิมพอร์ตไปยังฐานข้อมูล ของเซิร์ฟเวอร์ ใบรับรองจะถูกทำเครื่องหมายเป็นไม่ไว้วางใจในตอนเริ่มแรก และ ผู้ดูแลระบบจะใช้คำสั่ง **psconf** เพื่อ ดู และทำเครื่องหมายใบรับรองเป็นไว้วางใจโดยการป้อนคำสั่งต่อไปนี้:

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

หากผู้ดูแลระบบต้องการใช้คีย์ และใบรับรองที่แตกต่าง คำสั่ง **psconf** จะมีคุณลักษณะเพื่อ อิมพอร์ตคีย์และใบรับรอง

เพื่ออิมพอร์ตใบรับรองจากเซิร์ฟเวอร์ ให้ป้อน คำสั่งต่อไปนี้:

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

เพื่ออิมพอร์ตใบรับรองจากไคลเอ็นต์ ให้ป้อน คำสั่งต่อไปนี้:

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

**สิ่งอ้างอิงที่เกี่ยวข้อง:**

"คำสั่ง psconf" ในหน้า 175

## 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 175

# การแก้ไขปัญหาการจัดการ Trusted Network Connect และ Patch

ศึกษาสาเหตุที่เป็นไปได้สำหรับความล้มเหลว และขั้นตอนเพื่อ แก้ไขปัญหาระบบการจัดการ TNC และแพตช์

เพื่อแก้ไขปัญหา TNC และระบบการจัดการแพตช์ให้ตรวจสอบ การตั้งค่าคอนฟิกูเรชันที่แสดงในตารางต่อไปนี้

*ตารางที่ 14. การแก้ไขปัญหาการตั้งค่าคอนฟิกูเรชัน ระบบการจัดการ TNC และ Patch*

| ปัญหา | วิธีแก้ไข |
|---|---|
| เซิร์ฟเวอร์ TNC ไม่สตาร์ท หรือตอบสนอง | ดำเนินการขั้นตอนต่อไปนี้:<br>1. ตรวจสอบว่า daemon ของเซิร์ฟเวอร์ TNC รันอยู่หรือไม่โดยการป้อนคำสั่ง:<br>`ps -eaf \| grep tnccsd`<br>2. หากไม่ถูกรันอยู่ ให้ลบไฟล์ `/var/tnc/.tncsock`<br>3. รีสตาร์ทเซิร์ฟเวอร์<br>หากไม่สามารถแก้ไขปัญหา ให้ตรวจสอบไฟล์คอนฟิกูเรชัน `/etc/tnccs.conf` สำหรับรายการ `component = SERVER` บนเซิร์ฟเวอร์ TNC |
| เซิร์ฟเวอร์การจัดการแพตช์ TNC ไม่สตาร์ท หรือตอบสนอง | • ตรวจสอบว่า daemon ของเซิร์ฟเวอร์การจัดการแพตช์ TNC รันอยู่โดยการป้อนคำสั่งต่อไปนี้หรือไม่:<br>`ps -eaf \| grep tncpmd`<br>• ตรวจสอบไฟล์คอนฟิกูเรชัน `/etc/tnccs.conf` สำหรับรายการ `component = TNCPM` บนเซิร์ฟเวอร์การจัดการ แพตช์ TNC |
| ไคลเอ็นต์ TNC ไม่สตาร์ทหรือตอบสนอง | • ตรวจสอบว่า daemon ของไคลเอ็นต์ TNC รันอยู่โดยการป้อน คำสั่งต่อไปนี้:<br>`ps -eaf \| grep tnccsd`<br>• 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:<br>`ps -eaf \| grep tnccsd`<br>• 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" ในหน้า 171

"คำสั่ง vlantfw" ในหน้า 187

---

## 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 146

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 168

---

## 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 ที่มีโปรแกรมแก้ไขล่าสุด 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 เซอร์วิสแพ็คใหม่สำหรับระดับเทคโนโลยีที่ลงทะเบียนไว้ช่วงเวลาจะเป็นค่าจำนวนเต็มที่แสดงเป็นนาที หรือ ในรูปแบบต่อไปนี้: **d** (จำนวนวัน): **h** (ชั่วโมง): **m** (นาที) ช่วง ที่สนับสนุนสำหรับ *download_interval* คือ 30 - 525600 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 |
| **-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:<br>`# name: attribute1: attribute2: ...`<br>`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 ช่วงที่สนับสนุนสำหรับ *<ifix interval>* คือ 30 - 525600 นาที |

## 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. เพื่อสตาร์ทเซิร์ฟเวอร์ให้ป้อนคำสั่งต่อไปนี้:

```
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*> ] [**default_policy=**<*yes* | *no* > ] [**clientData_interval=**<*time in mins* > | **d** (days) : **h** (hours) : **m** (minutes) ] [ **clientDataPath=**<*Full_path* >]

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

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

**psconf chserver** attribute = *value*

**psconf clientData -i** *host* **[-l | -g]**

**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**<br>**หมายเหตุ:** แอ็ตทริบิวต์ **dbpath** ไม่สามารถเปลี่ยนแปลงโดยใช้คำสั่ง **chserver** ซึ่งสามารถ ตั้งค่าได้ขณะรัน **mkserver** |
| **clientData** | สร้างสแน็ปช็อตข้อมูล (ระดับระบบปฏิบัติการระดับ และชุดไฟล์ ที่ติดตั้ง) เกี่ยวกับไคลเอ็นต์ TNC<br><br>พาธ *clientDataPath* ระบุตำแหน่งที่เก็บข้อมูล การรวบรวมสแน็ปช็อต ตำแหน่งดีฟอลต์อยู่ใน ไดเร็กทอรี `/var/tnc/clientData/` บนเซิร์ฟเวอร์ TNC คุณสามารถเปลี่ยนแปลงหรือตั้งค่า พาธ *clientDataPath* โดยใช้คำสั่ง **chserver** หรือ **mkserver**<br><br>คุณสามารถ เริ่มต้นการรวบรวมสแน็ปช็อตไคลเอ็นต์ TNC จากบรรทัดรับคำสั่งโดยการรันคำสั่งย่อย **clientData** จากเซิร์ฟเวอร์ TNC คำสั่งย่อย **clientData** ที่รันจากบรรทัดรับคำสั่ง ไม่ขึ้นกับช่วงเวลา **clientData_interval** |
| **clientData_interval** | คุณสามารถใช้คำสั่งย่อย **chserver** หรือ **mkserver** เพื่อกำหนดคอนฟิกการรวบรวม สแน็ปช็อตให้เกิดขึ้นในช่วงเวลาปกติโดยการระบุค่าสำหรับช่วงเวลา **clientData_interval** การรวบรวมสแน็ปช็อตเริ่มต้นโดยอัตโนมัติเมื่อช่วงเวลา **clientData_interval** มีค่าที่ไม่ใช่ 0 (ศูนย์)<br><br>โดยดีฟอลต์ การรวบรวมสแน็ปช็อตถูกปิดใช้งานโดยตัวกำหนดตารางเวลา เมื่อต้องการเปิดใช้งาน ตัวกำหนดตารางเวลาระบุค่า **clientData_interval** ที่มากกว่าหรือเท่ากับ 30 เมื่อต้องการ ปิดใช้งานตัวกำหนดตารางเวลา ระบุค่า **clientData_interval** เป็น 0 (ศูนย์) ช่วงที่สนับสนุน สำหรับช่วงเวลา **clientData_interval** คือ 30 - 525600 นาที |
| **dbpath** | ระบุตำแหน่งฐานข้อมูล TNC ค่าดีฟอลต์ คือ `/var/tnc` |
| **default_policy** | เปิดใช้งานหรือปิดใช้งานการตรวจสอบอัตโนมัติของไคลเอ็นต์ TNC สำหรับ intern fix (ifix) และ APARs ที่ระดับเดียวกับไคลเอ็นต์ ระบุ *yes* เพื่อเปิดใช้งานการตรวจสอบ อัตโนมัติ ระบุ *no* เพื่อปิดใช้งานการตรวจสอบอัตโนมัติ สำหรับข้อมูลเพิ่มเติมเกี่ยวกับ คำสั่งย่อย **default_policy** ดูที่ ตาราง default_policy |
| **delete** | ลบนโยบายหรือข้อมูลไคลเอ็นต์ |
| **export** | เอ็กซ์พอร์ตใบรับรองไคลเอ็นต์หรือเซิร์ฟเวอร์ หรือ ฐานข้อมูลบนเซิร์ฟเวอร์ TNC |
| **fspolicy** | ระบุนโยบายการตั้งค่าไฟล์ของรีลีส, ระดับเทคโนโลยี และเซอร์วิสแพ็คที่ใช้สำหรับการตรวจสอบ ไคลเอ็นต์ TNC |
| **import** | อิมพอร์ตใบรับรองบนไคลเอ็นต์ หรือเซิร์ฟเวอร์ หรือ ฐานข้อมูลบนเซิร์ฟเวอร์ TNC |

| รายการ | คำอธิบาย |
|---|---|
| **ipgroup** | ระบุกลุ่ม Internet Protocol (IP) ที่ มีหลาย IP แอดเดรสของไคลเอ็นต์ หรือชื่อโอสต์ |
| **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 ช่วงที่สนับสนุนสำหรับ ช่วงเวลา **recheck_interval** คือ 30 – 525600 นาที<br>**หมายเหตุ:** ค่า ของ **recheck_interval=0** หมายความว่าตัวกำหนดเวลาไม่ได้เริ่มต้นการตรวจสอบไคลเอ็นต์ ที่ช่วงเวลาปกติ และไคลเอ็นต์ที่ลงทะเบียนไว้จะถูกตรวจสอบโดยอัตโนมัติเริ่มต้นทำงาน ในกรณีเช่นนี้ สามารถตรวจสอบไคลเอ็นต์ ด้วยตัวเอง |
| **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 |

ตารางต่อไปนี้แสดงผลลัพธ์การกำหนดคอนฟิกคำสั่งย่อย **default_policy** เป็นค่า *yes* หรือ *no*:

*ตารางที่ 15. ผลลัพธ์ของคำสั่งย่อย default_policy*

| **FSpolicy (Fileset policy)** | **default policy=***yes* | **default policy=***no* |
|---|---|---|
| ไคลเอ็นต์ TNC เป็นของนโยบายชุดไฟล์ที่มีกลุ่ม interim fix (iFix) และ APARs กำหนด | นโยบายดีฟอลต์ถูกลบล้างโดย iFix และ APARs ที่มีให้ในนโยบายชุดไฟล์ | ไม่ใช้นโยบายดีฟอลต์ iFix และ APARs ที่มีให้ในนโยบายชุดไฟล์ถูก พิจารณาระหว่างกระบวนการการตรวจสอบสำหรับไคลเอ็นต์ TNC |
| ไคลเอ็นต์ TNC เป้นของนโยบายชุดไฟล์ที่ไม่มีกลุ่ม iFix และ APARs ถูกกำหนด | นโยบายดีฟอลต์ถูกใช้กับ iFix และ APARs ระหว่างกระบวนการตรวจสอบสำหรับ ไคลเอ็นต์ TNC iFix และ APARs เท่านั้นที่ตรงกับระดับของไคลเอ็นต์ TNC ถูกใช้ระหว่าง กระบวนการตรวจสอบ | ไม่ใช้นโยบายดีฟอลต์ |

## แฟล็ก

| รายการ | คำอธิบาย |
| --- | --- |
| **-A <advisoryName>** | ระบุชื่อแอดไวเซอร์สำหรับรายงาน |
| **-B <buildinfo>** | ระบุข้อมูลบิลด์เพื่อจัดเตรียม รายงานแพตช์ |
| **-c** | แสดงแอ็ตทริบิวต์ผู้ใช้ในเร็กคอร์ด ที่คั่นด้วยเครื่องหมายโคลอนดังนี้:<br>`# name: attribute1: attribute2: ...`<br>`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 อีเมลตามด้วยรายชื่อกลุ่ม IP ที่คั่นด้วยเครื่องหมายจุลภาค |
| **-E \| FAIL \| COMPLIANT \| ALL \|** | ระบุเหตุการณ์ที่อีเมลต้อง ถูกส่งไปยัง id อีเมลที่กำหนดค่าคอนฟิกไว้<br>FAIL- Mails จะถูกส่งเมื่อ สถานะการตรวจสอบของไคลเอ็นต์คือ FAILED<br>COMPLIANT- Mails จะถูกส่งเมื่อสถานะการตรวจสอบของไคลเอ็นต์คือ COMPLAINT<br>ALL - Mails จะถูกส่งสำหรับสถานะทั้งหมดของการตรวจสอบไคลเอ็นต์ |
| **-f** *filename* | ระบุไฟล์ที่ใบรับรอง ต้องอ่านในกรณีของการอิมพอร์ต หรือระบุตำแหน่ง ที่ใบรับรองต้องถูกเขียนทับในกรณีของการเอ็กซ์พอร์ต |
| **-F** *fspolicy buildinfo* | ระบุชื่อนโยบายของระบบไฟล์ ตามด้วย ข้อมูลบิลด์ ข้อมูลบิดล์สามารถอยู่ในรูปแบบต่อไปนี้:<br>`6100-04-01` โดย `6100` หมายถึงเวอร์ชัน 6.1, `04` คือ ระดับการบำรุงรักษา และ `01` คือเซอร์วิสแพ็ค |
| **-g** | รันคำสั่งย่อย **clientData** บนไคลเอ็นต์ TNC ที่ระบุ แฟล็กนี้ใช้กับคำสั่งย่อย **clientData** เท่านั้น |
| **-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 |
| **-l** | แสดงรายละเอียดสแน็ปช็อตบนเซิร์ฟเวอร์ TNC สำหรับไคลเอ็นต์ TNC ที่ระบุ แฟล็กนี้ใช้กับคำสั่งย่อย **clientData** เท่านั้น |
| **-p** | แสดงตัวอย่างการอัพเดตไคลเอ็นต์ TNC |
| **-P <policyName>** | ระบุชื่อนโยบายเพื่อจัดเตรียมรายงานนโยบาย ของไคลเอ็นต์ |
| **-q** | ยกเลิกข้อมูลส่วนหัว |
| **-r** *buildinfo* | สร้างรายงานตามข้อมูลบิลด์ ข้อมูลบิดล์สามารถอยู่ในรูปแบบต่อไปนี้:<br>`6100-04-01` โดย `6100` หมายถึงเวอร์ชัน 6.1, `04` คือ ระดับการบำรุงรักษา และ `01` คือเซอร์วิสแพ็ค |
| **-R** | ระบุว่าการดำเนินการมีไว้สำหรับคอมโพเนนต์ IPRef |
| **-s COMPLIANT \| IGNORE \| FAILED \| ALL** | แสดงไคลเอ็นต์ตามสถานะดังนี้:<br>**COMPLIANT**<br>แสดงไคลเอ็นต์ที่ทำงานอยู่<br>**IGNORE** แสดงไคลเอ็นต์ที่ถูกยกเว้นจากการตรวจสอบใดๆ<br>**FAILED** แสดงไคลเอ็นต์ที่มีการตรวจสอบที่ล้มเหลวตาม นโยบายที่กำหนดค่าคอนฟิกไว้<br>**ALL** แสดงไคลเอ็นต์ทั้งหมดโดยไม่คำนึงถึงสถานะ |
| **-S <host>** | ระบุชื่อโฮสต์เพื่อจัดเตรียมรายงานการแก้ไข ที่ปลอดภัยของไคลเอ็นต์ |
| **-t TRUSTED \| UNTRUSTED** | ทำเครื่องหมายไคลเอ็นต์ที่ระบุเป็นไว้วางใจได้หรือไม่ไว้วางใจ<br>**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
```

18. เมื่อต้องการแสดงข้อมูลสแน็ปช็อตที่รวบรวมด้วยคำสั่งย่อย **clientData** ป้อนคำสั่งต่อไปนี้:

```
psconf clientData -l [ip|host]
```

19. เมื่อต้องการแสดงประวัติสำหรับไคลเอ็นต์ TNC ป้อนคำสั่งต่อไปนี้:

```
psconf list -H -i [ip|ALL]
```

## 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 pscxpert

## วัตถุประสงค์

ช่วยผู้ดูแลระบบใน การตั้งค่าการกำหนดค่าคอนฟิกการรักษาความปลอดภัย

## ไวยากรณ์

**pscxpert -l** {high|medium|low|default|sox-cobit} [ **-p** ]

**pscxpert -l** {h|m|l|d|s} [ **-p** ]

**pscxpert -f** Profile [ **-p** ]

**pscxpert -u** [ **-p** ]

**pscxpert -c** [ **-p** ] [**-r**|**-R**] [**-P** Profile] [**-l** Level]

**pscxpert -t**

**pscxpert -l** <Level> [ **-p** ] <**-a** *File1* | **-n** *File2* | **-a** *File3* **-n** *File4*>

**pscxpert -f** Profile **-a** File [ **-p** ]

**pscxpert -d**

## คำอธิบาย

คำสั่ง **pscxpert** ตั้งค่าการกำหนดคอนฟิกระบบต่างๆ เพื่อเปิดใช้งาน ระดับการรักษาความปลอดภัยที่ระบุ

การรันคำสั่ง **pscxpert** ที่มีเฉพาะชุดแฟล็ก **-l** จะใช้การตั้งค่าการรักษาความปลอดภัยโดย ไม่อนุญาตให้ผู้ใช้กำหนดค่าคอนฟิกการตั้งค่า ตัวอย่างเช่น การรัน คำสั่ง **pscxpert -l high** จะใช้การตั้งค่า การรักษาความปลอดภัยระดับสูงทั้งหมดกับระบบโดยอัตโนมัติ อย่างไรก็ตามการรันคำสั่ง **pscxpert -l** ด้วยแฟล็ก **-n** และ **-a** บันทึก การตั้งค่าการรักษาความปลอดภัยเป็นไฟล์ที่ระบุโดยพารามิเตอร์ *File* แฟล็ก **-f** จะใช้การกำหนดค่าคอนฟิกใหม่

หลังการเลือกเริ่มแรก เมนูถูกแสดงแยกรายการอ็อพชันการตั้งค่าการรักษาความปลอดภัยทั้งหมด ที่สัมพันธ์กับระดับความปลอดภัยที่เลือก สามารถยอมรับอ็อพชันเหล่านี้ทั้งหมดหรือสลับเปิดหรือปิด แต่ละรายการ หลังจากการเปลี่ยนแปลงครั้งที่สอง คำสั่ง **pscxpert** จะยังคงใช้การตั้งค่าการรักษาความปลอดภัยกับ ระบบคอมพิวเตอร์

รันคำสั่ง **pscxpert** ในฐานะผู้ใช้ root ของ Virtual I/O Server เป้าหมาย เมื่อคุณไม่ได้ล็อกอินในฐานะผู้ใช้ root ของ Virtual I/O Server เป้าหมาย ให้รันคำสั่ง **oem_setup_env** ก่อนคุณรันคำสั่ง

| ถ้าคุณรันคำสั่ง **pscxpert** เมื่ออีกอินสแตนซ์ของ คำสั่ง **pscxpert** กำลังรันอยู่แล้ว คำสั่ง **pscxpert** จะออกจากการทำงานพร้อมข้อ
| ความแสดงข้อผิดพลาด

**หมายเหตุ:** รันคำสั่ง **pscxpert** อีกครั้งหลังจากการเปลี่ยนแปลงระบบหลักใดๆ เช่น การติดตั้ง หรือ อัพเดตซอฟต์แวร์ หากรายการคอนฟิกูเรชันการรักษาความปลอดภัยเฉพาะ ไม่ถูกเลือกเมื่อรันคำสั่ง **pscxpert** อีกครั้ง รายการคอนฟิกูเรชันนั้นจะถูกข้าม

## แฟล็ก

| รายการ | คำอธิบาย |
|---|---|
| **-a** | การตั้งค่าด้วยอ็อพชันระดับการรักษาความปลอดภัยที่สัมพันธ์กัน ถูกเขียนไปยังไฟล์ที่ระบุในรูปแบบย่อ |
| **-c** | ตรวจสอบการตั้งค่าการรักษาความปลอดภัยกับชุดของกฎ ที่ปรับใช้ก่อนหน้านี้ หากการตรวจสอบกฎล้มเหลว เวอร์ชันก่อนหน้า ของกฎจะถูกตรวจสอบ กระบวนการนี้ยังคงทำต่อไปจนกระทั่ง การตรวจสอบผ่านหรือจนกระทั่งอินสแตนซ์ทั้งหมดของกฎที่ล้มเหลว ในไฟล์ `/etc/security/aixpert/core/appliedaixpert.xml` ถูกตรวจสอบ คุณสามารถรัน การตรวจสอบนี้เทียบกับโปรไฟล์ดีฟอลต์ หรือโปรไฟล์แบบกำหนดเองใดๆ |
| **-d** | แสดงนิยามของชนิดเอกสาร (DTD) |

| รายการ | คำอธิบาย |
| --- | --- |
| **-f** | ใช้การตั้งค่าการรักษาความปลอดภัยที่มีให้ในไฟล์ *Profile* ที่ระบุ โปรไฟล์อยู่ใน ไดเร็กทอรี `/etc/security/aixpert/custom` โปรไฟล์ที่มีจะมีโปรไฟล์มาตรฐาน ต่อไปนี้:<br>**DataBase.xml**<br>ไฟล์นี้จะมีข้อกำหนดสำหรับการตั้งค่าฐานข้อมูลดีฟอลต์<br>**DoD.xml** ไฟล์นี้จะมีข้อกำหนดสำหรับการตั้งค่า Department of Defense Security Technical Implementation Guide (STIG)<br>**DoD_to_AIXDefault.xml**<br>เปลี่ยนแปลงค่าติดตั้งไปเป็นค่าติดตั้งดีฟอลต์ของ AIX<br>**DoDv2.xml**<br>ไฟล์นี้มาข้อกำหนดสำหรับเวอร์ชัน 2 ของค่าติดตั้ง Department of Defense Security Technical Implementation Guide (STIG)<br>**DoDv2_to_AIXDefault.xml**<br>เปลี่ยนแปลงค่าติดตั้งไปเป็นค่าติดตั้งดีฟอลต์ของ AIX<br>**Hipaa.xml**<br>ไฟล์นี้จะมีข้อกำหนดสำหรับการตั้งค่า Health Insurance Portability and Accountability Act (HIPAA)<br>**NERC.xml**<br>ไฟล์นี้มีข้อกำหนดสำหรับการตั้งค่า North American Electric Reliability Corporation (NERC)<br>**NERC_to_AIXDefault.xml**<br>ไฟล์นี้เปลี่ยนแปลงการตั้งค่า NERC เป็นการตั้งค่า AIX ดีฟอลต์<br>**PCI.xml** ไฟล์นี้จะมีข้อกำหนดสำหรับการตั้งค่า Payment card industry Data Security Standard<br>**PCIv3.xml**<br>ไฟล์นี้มีข้อกำหนดสำหรับค่าติดตั้ง Payment card industry Data Security Standard Version 3<br>**PCI_to_AIXDefault.xml**<br>ไฟล์นี้เปลี่ยนแปลงการตั้งค่าเป็นการตั้งค่า AIX ดีฟอลต์<br>**PCIv3_to_AIXDefault.xml**<br>ไฟล์นี้เปลี่ยนแปลงการตั้งค่าเป็นการตั้งค่า AIX ดีฟอลต์<br>**SOX-COBIT.xml**<br>ไฟล์นี้จะมีข้อกำหนดสำหรับการตั้งค่า Sarbanes-Oxley Act and COBIT<br>คุณยังสามารถสร้างโปรไฟล์ที่กำหนดเองในไดเร็กทอรี เดียวกัน และใช้กับการตั้งค่าของคุณโดยการเปลี่ยนชื่อและแก้ไข ไฟล์ XML ที่มีอยู่<br>ตัวอย่างเช่น คำสั่งต่อไปนี้จะปรับใช้โปรไฟล์ HIPAA กับระบบของคุณ:<br>`pscxpert -f /etc/security/aixpert/custom/Hipaa.xml`<br>เมื่อคุณระบุแฟล็ก **-f** ค่าติดตั้งการรักษาความปลอดภัยจะถูกใช้อย่างสอดคล้องกันจากระบบ ไปยังอีกระบบโดยการถ่ายโอนอย่างปลอดภัย และการปรับใช้ไฟล์ **appliedaixpert.xml** จากระบบหนึ่งสู่อีกระบบหนึ่ง<br>กฎที่ปรับใช้สำเร็จทั้งหมดจะถูกเขียนไปยังไฟล์ `/etc/security/aixpert/core/appliedaixpert.xml` และกฎการดำเนินการ `undo` ที่เกี่ยวข้อง จะถูกเขียนไปยังไฟล์ `/etc/security/aixpert/core/undo.xml` |

| รายการ | คำอธิบาย |
| --- | --- |
| **-l** | กำหนดการตั้งค่าการรักษาความปลอดภัยระบบไปยังระดับ ที่ระบุ แฟล็กนี้จะมีอ็อพชันต่อไปนี้:<br>**h\|high** ระบุอ็อพชันการรักษาความปลอดภัยระดับสูง<br>**m\|medium** ระบุอ็อพชันการรักษาความปลอดภัยระดับปานกลาง<br>**l\|low** ระบุอ็อพชันการรักษาความปลอดภัยระดับล่าง<br>**d\|default** ระบุอ็อพชันการรักษาความปลอดภัยระดับมาตรฐาน AIX<br>**s\|sox-cobit** ระบุอ็อพชันการรักษาความปลอดภัย Sarbanes-Oxley Act และ COBIT<br>ถ้าคุณระบุแฟล็ก **-l** และ **-n** การตั้งค่าการรักษาความปลอดภัยจะไม่ถูก นำไปใช้บนระบบ อย่างไรก็ตาม จะถูกเขียนลงในไฟล์ที่ระบุเท่านั้น<br><br>กฎที่ปรับใช้สำเร็จทั้งหมดจะถูกเขียนไปยังไฟล์ `/etc/security/aixpert/core/appliedaixpert.xml` และกฎการดำเนินการที่สอดคล้องกัน จะถูกเขียนไปยังไฟล์ `/etc/security/aixpert/core/undo.xml`<br><br>**ข้อควรสนใจ:** เมื่อคุณใช้แฟล็ก **d\|default** ดีฟอลต์สามารถเขียนทับการตั้งค่า การรักษาความปลอดภัยที่กำหนดที่คุณตั้งค่าไว้ก่อนหน้าโดยใช้คำสั่ง **pscxpert** หรือ ด้วยตนเอง และเรียกคืนระบบให้เป็นการกำหนดคอนฟิกแบบเปิดเริ่มแรก |
| **-n** | เขียนการตั้งค่าด้วยอ็อพชันระดับการรักษาความปลอดภัยที่สัมพันธ์กันกับ ไฟล์ที่ระบุ |
| **-p** | ระบุว่าเอาท์พุทของ กฎการรักษาความปลอดภัยจะแสดงขึ้นโดยใช้เอาท์พุท Verbose แฟล็ก The **-p** ล็อกกฎที่ถูกดำเนินการเพื่อตรวจสอบระบบย่อยการตรวจสอบถ้า อ็อพชัน **auditing** ถูกเปิดใช้งาน อ็อพชันนี้สามารถใช้กับแฟล็ก **-l, -u, -c** และ **-f** ใดๆ |
| **-P** | ยอมรับชื่อโปรไฟล์เป็นอินพุท อ็อพชันนี้ใช้ควบคู่ กับแฟล็ก **-c** แฟล็ก **-c** และ **-P** ถูกใช้เพื่อตรวจสอบความเข้ากันได้ของ ระบบที่มีโปรไฟล์ที่ส่งผ่าน |
| **-r** | เขียนการตั้งค่าที่มีอยู่ ของระบบไปยังไฟล์ `/etc/security/aixpert/check_report.txt` คุณสามารถใช้เอาท์พุทในรายงานการตรวจสอบการปฏิบัติตามมาตรฐานและการรักษาความปลอดภัย รายงานจะอธิบายแต่ละการตั้งค่า และมีความเกี่ยวข้องกับข้อกำหนดของการปฏิบัติตาม ข้อบังคับอย่างไร และไม่ว่าการตรวจสอบจะผ่านหรือล้มเหลว |
| **-R** | จะให้เอาท์พุทเช่นเดียวกับแฟล็ก **-r** แต่แฟล็กนี้จะมีคำอธิบายเพิ่มเติมเกี่ยวกับแต่ละสคริปต์และโปรแกรมที่ใช้เพื่อปรับใช้ การตั้งค่าคอนฟิกูเรชัน |
| **-t** | แสดงชนิดของโปรไฟล์ที่ปรับใช้บนระบบ |
| **-u** | ยกเลิกการตั้งค่าการรักษาความปลอดภัยที่ปรับใช้<br>**หมายเหตุ:** คุณไม่สามารถ ใช้แฟล็ก **-u** เพื่อย้อนกลับแอ็พพลิเคชันของโปรไฟล์ DoD, DoDv2, NERC, PCI หรือ PCIv3 เมื่อต้องการลบโปรไฟล์เหล่านี้หลังจากโปรไฟล์ถูกเพิ่มแล้ว ให้ใช้โปรไฟล์ที่ลงท้ายด้วย `_AIXDefault.xml` ตัวอย่างเช่น เมื่อต้องการลบโปรไฟล์ NERC.xml คุณต้องใช้โปรไฟล์ NERC_to_AIXDefault.xml |

## พารามิเตอร์

| รายการ | คำอธิบาย |
| --- | --- |
| *File* | ไฟล์เอาท์พุทที่เก็บการตั้งค่าการรักษาความปลอดภัย ต้องมีสิทธิ์รูทในการเข้าถึงไฟล์นี้ |
| *Level* | ระดับแบบกำหนดเองเพื่อตรวจสอบกับการตั้งค่าที่ใช้ก่อนหน้านี้ |
| *Profile* | ชื่อไฟล์ของโปรไฟล์ที่มีกฎมาตรฐาน สำหรับระบบ ต้องมีสิทธิ์รูทในการเข้าถึงไฟล์นี้ |

## การรักษาความปลอดภัย

คำสั่ง **pscxpert** สามารถรันได้เฉพาะรูท

## ตัวอย่าง

1. เพื่อเขียนอ็อพชันการรักษาความปลอดภัยระดับสูงไปยังไฟล์เอาท์พุท ให้ป้อนคำสั่งต่อไปนี้:

   ```
   pscxpert -l high -n /etc/security/pscexpert/plugin/myPreferredSettings.xml
   ```

   หลัง คุณรันคำสั่งนี้ ไฟล์เอาต์พุตจะสามารถแก้ไข และใส่เครื่องหมายข้อคิดเห็นกฎการรักษาความปลอดภัยที่ระบุ โดยการล้อมรอบในสตริงข้อคิดเห็น XML มาตรฐาน (<-- เริ่มต้น ข้อคิดเห็น และ -\> ปิดข้อคิดเห็น)
2. เพื่อใช้การตั้งค่าการรักษาความปลอดภัยจากไฟล์คอนฟิกูเรชัน Department of Defense STIG ให้ป้อนคำสั่งต่อไปนี้:

   ```
   pscxpert -f /etc/security/aixpert/custom/DoD.xml
   ```
3. เพื่อใช้การตั้งค่าการรักษาความปลอดภัยจากไฟล์คอนฟิกูเรชัน HIPAA ให้ป้อนคำสั่งต่อไปนี้:

   ```
   pscxpert -f /etc/security/aixpert/custom/Hipaa.xml
   ```
4. เมื่อต้องการตรวจสอบการตั้งค่าการรักษาความปลอดภัยของระบบ และเพื่อล็อกกฎที่ล้มเหลวในระบบย่อย การตรวจสอบ ให้ป้อนคำสั่งต่อไปนี้:

   ```
   pscxpert -c -p
   ```
5. เมื่อต้องการตรวจสอบระดับแบบกำหนดเองของการตั้งค่าการรักษาความปลอดภัยสำหรับโปรไฟล์ NERC บน ระบบ และเพื่อล็อกกฎที่ล้มเหลวในระบบย่อยการตรวจสอบ ป้อนคำสั่ง ต่อไปนี้:

   ```
   pscxpert -c -p -l NERC
   ```
6. เมื่อต้องการสร้างรายงานและเขียนรายงานไปยัง ไฟล์ /etc/security/aixpert/check_report.txt ป้อนคำสั่งต่อไปนี้:

   ```
   pscxpert -c -r
   ```

## ตำแหน่ง

| รายการ | คำอธิบาย |
|---|---|
| **/usr/sbin/pscxpert** | มีคำสั่ง **pscxpert** |

### Files

| รายการ | คำอธิบาย |
|---|---|
| **/etc/security/aixpert/log/aixpert.log** | ประกอบด้วยบันทึกการติดตามของค่าติดตั้งความปลอดภัยที่นำไปใช้ ไฟล์นี้ไม่ใช้ มาตรฐาน syslog คำสั่ง **pscxpert** เขียนลงไฟล์โดยตรง มี สิทธิ์อ่าน/เขียน และร้องการการรักษษความปลอดภัย root |
| **/etc/security/aixpert/log/firstboot.log** | มีบันทึกการติดตามของการตั้งค่าการรักษาความปลอดภัย ที่ถูกปรับใช้ระหว่างการบูตครั้งแรกของการติดตั้ง Secure by Default (SbD) |
| **/etc/security/aixpert/core/undo.xml** | มี XML ที่แสดงการตั้งค่าการรักษาความปลอดภัย ซึ่งสามารถยกเลิกได้ |

---

# 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 146

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. เพื่อแสดงกฎที่สอดคล้องกันที่สามารถใช้เพื่อสร้างกฎตัวกรองที่กำหนดเส้นทางทราฟฟิกภายในคอมเพล็กซ์ตัวประมวลผลกลาง ให้พิมพ์คำสั่งต่อไปนี้:

   ```
   vlantfw -G
   ```

**สิ่งอ้างอิงที่เกี่ยวข้อง**:

"คำสั่ง genvfilt" ในหน้า 168

# คำประกาศ

ข้อมูลนี้จัดทำขึ้นสำหรับผลิตภัณฑ์และเซอร์วิสที่นำเสนอในสหรัฐฯ

IBM อาจไม่นำเสนอผลิตภัณฑ์ เซอร์วิส หรือคุณลักษณะที่อธิบายในเอกสารนี้ในประเทศอื่น โปรดปรึกษาตัวแทน IBM ในท้องถิ่นของคุณสำหรับข้อมูลเกี่ยวกับผลิตภัณฑ์ และเซอร์วิส ที่มีอยู่ในพื้นที่ของคุณในปัจจุบัน การอ้างอิงใดๆ ถึงผลิตภัณฑ์ โปรแกรม หรือเซอร์วิสของ IBM ไม่ได้มีวัตถุประสงค์ที่จะระบุหรือตีความว่า สามารถใช้ได้เฉพาะผลิตภัณฑ์ โปรแกรม หรือเซอร์วิสของ IBM เพียงอย่างเดียว เท่านั้น ผลิตภัณฑ์ โปรแกรม หรือเซอร์วิสใดๆ ที่สามารถทำงานได้เท่าเทียมกัน และไม่ละเมิดสิทธิทรัพย์สินทางปัญญาของ IBM อาจนำมาใช้ แทนได้ อย่างไรก็ตาม ถือเป็นความรับผิดชอบของผู้ใช้ที่จะประเมินและตรวจสอบการดำเนินการของ ผลิตภัณฑ์ โปรแกรม หรือเซอร์วิสใดๆ ที่ไม่ใช่ของ IBM

IBM อาจมีสิทธิบัตร หรืออยู่ระหว่างดำเนินการขอ สิทธิบัตรที่ครอบคลุมถึงหัวข้อซึ่งอธิบายในเอกสารนี้ การนำเสนอเอกสารนี้ไม่ได้เป็นการให้ไลเซนส์ใดๆ ในสิทธิบัตรเหล่านี้แก่คุณ คุณสามารถส่งการสอบถามเกี่ยวกับไลเซนส์ เป็นลายลักษณ์อักษรไปยัง:

*IBM Director of Licensing*
*IBM Corporation*
*North Castle Drive, MD-NC119*
*Armonk, NY 10504-1785*
*United States of America*

หากมีคำถามเกี่ยวกับข้อมูลชุดอักขระไบต์คู่ (DBCS) โปรดติดต่อแผนกทรัพย์สินทางปัญญาของ IBM ในประเทศของคุณ หรือส่งคำถาม เป็นลายลักษณ์อักษร ไปยัง:

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

**ย่อหน้าต่อไปนี้ไม่ได้ใช้กับสหราชอาณาจักร หรือประเทศอื่นใดที่ ข้อกำหนดดังกล่าวไม่สอดคล้องกับกฎหมายท้องถิ่น:** INTERNATIONAL BUSINESS MACHINES CORPORATION นำเสนอสิ่งพิมพ์นี้ "ตามสภาพ" โดยไม่มีการรับประกันใดๆ โดยชัดแจ้งหรือ โดยนัย ซึ่งรวมถึงแต่ไม่จำกัดเฉพาะการรับประกันโดยนัยถึงการไม่ละเมิด การขายได้ หรือความเหมาะสมสำหรับวัตถุประสงค์เฉพาะ เนื่องจากบางรัฐไม่อนุญาตให้ปฏิเสธการรับประกันโดยชัดแจ้งหรือ โดยนัยในธุรกรรมบางอย่าง ดังนั้น ข้อความสั่งนี้จึงอาจไม่ใช้กับคุณ

ข้อมูลนี้อาจมีความไม่ถูกต้องด้านเทคนิคหรือข้อผิดพลาดจากการพิมพ์ มีการเปลี่ยนแปลง ข้อมูลในเอกสารนี้เป็นระยะ และการเปลี่ยนแปลงเหล่านี้จะรวมอยู่ในเอดิชันใหม่ของ สิ่งพิมพ์ IBM อาจปรับปรุง และ/หรือเปลี่ยนแปลงในผลิตภัณฑ์ และ/หรือโปรแกรมที่อธิบายในสิ่งพิมพ์นี้ได้ตลอดเวลา โดยไม่ต้องแจ้งให้ทราบ

การอ้างอิงใดๆ ในข้อมูลนี้ถึงเว็บไซต์ไม่ใช่ของ IBM มีการจัดเตรียมเพื่อความสะดวกเท่านั้น และ ไม่ได้เป็นการรับรองเว็บไซต์เหล่านั้นในลักษณะใดๆ เอกสารประกอบที่เว็บไซต์เหล่านั้นไม่ได้เป็น ส่วนหนึ่งของเอกสารประกอบสำหรับผลิตภัณฑ์ IBM นี้ และการใช้เว็บไซต์เหล่านั้นถือเป็นความเสี่ยงของคุณเอง

IBM อาจใช้ หรือแจกจ่าย ข้อมูลใดๆ ที่คุณให้ในวิธีที่ IBM เชื่อว่าเหมาะสมโดยไม่ก่อให้เกิดข้อผูกมัดใดๆ กับ คุณ

ผู้รับไลเซนส์ของโปรแกรมนี้ที่ต้องการข้อมูลเกี่ยวกับโปรแกรมสำหรับวัตถุประสงค์ในการเปิดใช้งาน: (i) การแลกเปลี่ยนข้อมูลระหว่างโปรแกรมที่สร้างขึ้นอย่างอิสระกับโปรแกรมอื่น (รวมถึง โปรแกรมนี้) และ (ii) การใช้ข้อมูลซึ่งแลกเปลี่ยนร่วมกัน ควร ติดต่อ:

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

ข้อมูลดังกล่าวอาจพร้อมใช้งาน ภายใต้ข้อตกลงและเงื่อนไขที่เหมาะสม รวมถึง การชำระค่าธรรมเนียมในบางกรณี

โปรแกรมที่มีไลเซนส์ซึ่งอธิบายในเอกสารนี้ และเอกสารประกอบที่มีไลเซนส์ทั้งหมดสำหรับโปรแกรม นั้น มีการจัดเตรียมโดย IBM ภายใต้ข้อตกลงของข้อตกลงกับลูกค้าของ IBM, ข้อตกลงไลเซนส์โปรแกรมระหว่างประเทศของ IBM หรือข้อตกลงที่เท่าเทียมกันใดๆ ระหว่างเรา

ข้อมูลประสิทธิภาพใดๆ ที่มีในเอกสารนี้ถูกกำหนดในสภาวะแวดล้อมที่ควบคุม ด้วยเหตุนี้ ผลลัพธ์ที่ได้ในสภาวะแวดล้อมการปฏิบัติการอื่นจึงอาจแตกต่างไปอย่างมาก การวัดบางอย่างอาจ ดำเนินการบนระบบที่อยู่ระหว่างการพัฒนา และไม่มีการรับประกันว่าการวัดเหล่านี้จะ เหมือนกันบนระบบที่พร้อมใช้งานโดยทั่วไป ยิ่งไปกว่านั้น การวัดบางอย่างอาจมีการประเมินโดยวิธีการ ประมาณค่านอกช่วง ผลลัพธ์จริงอาจแตกต่างไป ผู้ใช้เอกสารนี้จึงควรตรวจสอบ ข้อมูลที่สามารถใช้ได้สำหรับสภาวะแวดล้อมของตน

ข้อมูลเกี่ยวกับผลิตภัณฑ์ที่ไม่ใช่ของ IBM ได้รับมาจากซัพพลายเออร์ของผลิตภัณฑ์เหล่านั้น ประกาศที่เผยแพร่ หรือแหล่งข้อมูลที่เปิดเผยต่อสาธารณะ IBM ไม่ได้ทดสอบผลิตภัณฑ์ดังกล่าว และไม่สามารถยืนยันความถูกต้องของ ประสิทธิภาพ ความเข้ากันได้ หรือการเรียกร้องอื่นใดที่เกี่ยวข้องกับผลิตภัณฑ์ที่ไม่ใช่ของ IBM คำถามเกี่ยวกับ ความสามารถของผลิตภัณฑ์ที่ไม่ใช่ของ IBM ควรส่งไปยังซัพพลายเออร์ของผลิตภัณฑ์เหล่านั้น

ข้อความทั้งหมดเกี่ยวกับทิศทางหรือเจตนาในอนาคตของ IBM อาจมีการเปลี่ยนแปลง หรือเพิกถอนได้โดยไม่ต้องแจ้งให้ทราบ และแสดงถึงเป้าหมายและวัตถุประสงค์เท่านั้น

ราคาของ IBM ทั้งหมดที่แสดงเป็นราคาขายปลีกที่แนะนำของ IBM ซึ่งเป็นราคาปัจจุบัน และอาจเปลี่ยนแปลงได้โดยไม่ต้องแจ้งให้ทราบ ราคาของผู้แทนจำหน่ายอาจแตกต่างไป

ข้อมูลนี้ใช้สำหรับวัตถุประสงค์ของการวางแผนเท่านั้น ข้อมูลในเอกสารนี้อาจมีการเปลี่ยนแปลง ก่อนผลิตภัณฑ์ที่อธิบายจะวางจำหน่าย

ข้อมูลนี้มีตัวอย่างของข้อมูลและรายงานที่ใช้ในการดำเนินการทางธุรกิจรายวัน เพื่อ สาธิตข้อมูลให้สมบูรณ์ที่สุดเท่าที่จะเป็นไปได้ ตัวอย่างจึงมีชื่อของแต่ละบุคคล บริษัท ยี่ห้อ และผลิตภัณฑ์ ชื่อทั้งหมดเหล่านี้เป็นชื่อสมมติ และการคล้ายคลึงในชื่อและที่อยู่ซึ่งหน่วยธุรกิจจริงใช้เป็นความบังเอิญโดยสิ้นเชิง

ไลเซนส์ลิขสิทธิ์:

ข้อมูลนี้มีตัวอย่างแอ็พพลิเคชันโปรแกรมในภาษาต้นฉบับ ซึ่งแสดงถึง เทคนิคด้านโปรแกรมในหลากหลายแพล็ตฟอร์ม คุณอาจคัดลอก ปรับเปลี่ยน และแจกจ่าย โปรแกรมตัวอย่างเหล่านี้ในรูปแบบใดๆ โดยไม่ต้องชำระเงินให้แก่ IBM สำหรับวัตถุประสงค์ในการพัฒนา การใช้ การตลาด หรือการแจกจ่ายโปรแกรมแอ็พพลิเคชัน ที่สอดคล้องกับอินเตอร์เฟสการเขียนโปรแกรมแอ็พพลิเคชันสำหรับแพล็ตฟอร์มปฏิบัติการ ซึ่งเขียน โปรแกรมตัวอย่าง ตัวอย่างเหล่านี้ยังไม่ได้ผ่านการทดสอบในทุกสภาพ ดังนั้น IBM จึงไม่สามารถรับประกัน หรือบอกเป็นนัยถึง ความน่าเชื่อถือ ความสามารถบริการได้ หรือฟังก์ชันของโปรแกรมเหล่านี้ โปรแกรมตัวอย่างมีการนำเสนอ "ตาม สภาพ" โดยไม่มีการรับประกันประเภทใดๆ IBM ไม่รับผิดชอบ ต่อความเสียหายใดๆ ที่เกิดขึ้นเนื่องจากการใช้โปรแกรมตัวอย่างของคุณ

แต่ละสำเนา หรือส่วนใดๆ ของโปรแกรมตัวอย่างเหล่านี้ หรืองานที่สืบเนื่องใดๆ ต้องมี คำประกาศลิขสิทธิ์ดังนี้:

ส่วนของโค้ดนี้ได้มาจากโปรแกรมตัวอย่างของ IBM Corp.



---

## 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



## R



## S



## T



## ก



## ข

## ค



## ซ



## ต



## น



## ป



## ภ



## ม



## ร



## ล



## ส



## อ

พิมพ์ในสหรัฐอเมริกา