IBM PowerSC

Express Edition

เวอร์ชัน 1.1.3

PowerSC Express Edition

IBM PowerSC

Express Edition

เวอร์ชัน 1.1.3

PowerSC Express Edition

หมายเหตุ

ก่อนใช้ข้อมูลนี้ รวมถึงผลิตภัณฑ์ที่สนับสนุน โปรดอ่าน ข้อมูลใน “คำประกาศ” ในหน้า 37

เอดิชันนี้จะใช้กับ IBM PowerSC Express เวอร์ชัน 1.1.3 และการแก้ไขและรีลีสต่อมาทั้งหมดจนกว่าจะระบุไว้เป็นอย่างอื่น ในเอดิชันใหม่

สารบัญ

เกี่ยวกับเอกสารนี้

เอกสารนี้ให้ผู้ดูแลระบบมีข้อมูล ที่ครบถ้วนเกี่ยวกับ ไฟล์ ระบบ และการรักษาความปลอดภัยเครือข่าย

การไฮไลต์

มีการใช้ระเบียบการไฮไลต์ต่อไปนี้ในเอกสารนี้:

ตัวหนา	ระบุคำสั่ง รูทีนย่อย คีย์เวิร์ด ไฟล์ โครงสร้าง ไดเร็กทอรี และรายการอื่นๆ ที่มีชื่อ ถูกกำหนดไว้แล้วโดยระบบ รวมทั้งระบุอ็อบเจ็กต์กราฟิก เช่น ปุ่ม เลเบล และไอคอนที่ผู้ใช้เลือก
ตัวเอน	ระบุพารามิเตอร์ที่ชื่อแท้จริง หรือค่าจะถูกกำหนดโดยผู้ใช้
ไมโนสเปซ	ระบุตัวอย่างค่าข้อมูลที่ระบุ ตัวอย่างข้อความที่คล้ายกับที่คุณจะเห็นเมื่อถูกแสดง ตัวอย่าง ของส่วนของโค้ดโปรแกรมที่คล้ายกับที่คุณอาจเขียนในฐานะที่เป็นโปรแกรมเมอร์ ข้อความจากระบบ หรือข้อมูลที่คุณควรพิมพ์

การตรงตามตัวพิมพ์ใน AIX®

ทุกสิ่งในระบบปฏิบัติการ AIX เป็นแบบตรงตาม ตัวพิมพ์ ซึ่งหมายความว่ามีการแยกแยะความแตกต่างระหว่างตัวอักษรพิมพ์ใหญ่ และพิมพ์เล็ก ตัวอย่างเช่น คุณสามารถใช้คำสั่ง **ls** เพื่อ แสดงรายชื่อไฟล์ หากคุณพิมพ์ `LS` ระบบจะตอบกลับว่า คำสั่งคือ `not found` ในลักษณะคล้ายกัน `FILEA`, `FiLea`, และ `filea` คือชื่อไฟล์ที่แตกต่างกันสามไฟล์ แม้ว่า จะอยู่ในไดเร็กทอรีเดียวกันก็ตาม เพื่อหลีกเลี่ยงสาเหตุการเกิดการดำเนินการที่ต้องการ ให้กระทำ ทำให้แน่ใจเสมอว่าคุณใช้ขนาดตัวพิมพ์ถูกต้อง

ISO 9000

ระบบรับรองคุณภาพที่ลงทะเบียน ISO 9000 ใช้ในการพัฒนาและการผลิตผลิตภัณฑ์นี้

IBM PowerSC Express Edition 1.1.3

IBM® PowerSC™ Express Edition จะมีคุณลักษณะ Security and Compliance Automation ที่จัดการ โปรไฟล์ที่กำหนดไว้ล่วงหน้าสำหรับความปลอดภัย และการปฏิบัติตามมาตรฐาน PowerSC Express Edition ยังมี คุณลักษณะ PowerSC Real Time Compliance ซึ่งสามารถกำหนดคอนฟิกเพื่อให้มีการแจ้งเตือนแบบเรียลไทม์เมื่อ เกิดการละเมิด หรือเมื่อไฟล์สำคัญบางไฟล์มีการเปลี่ยนแปลง

มีอะไรใหม่ใน PowerSC Express Edition 1.1.3

อ่านเกี่ยวกับข้อมูลใหม่หรือข้อมูลที่มีการเปลี่ยนแปลงที่สำคัญสำหรับ มีอะไรใหม่ในชุดหัวข้อ PowerSC Express Edition 1.1.3

วิธีการดู มีอะไรใหม่หรือมีอะไรที่เปลี่ยนแปลง

ในไฟล์ PDF นี้ คุณอาจมองเห็นแถบการปรับปรุงใหม่ (|) ในขอบด้านซ้าย ที่ระบุข้อมูลใหม่หรือข้อมูลที่เปลี่ยนแปลง

ธันวาคม 2013

ข้อมูลต่อไปนี้ จะมีสรุปของเนื้อหาใหม่และที่ปรับปรุงสำหรับ PowerSC Express Edition 1.1.3:

- เพิ่มข้อมูลเกี่ยวกับไฟล์ README.ICEexpress ใน “การติดตั้ง PowerSC Express Edition เวอร์ชัน 1.1.3” ในหน้า 2
- อัพเดตข้อมูลเกี่ยวกับการสนับสนุนสำหรับมาตรฐาน Payment Card Industry – Data Security Standard สำหรับเวอร์ชัน 2.0 ของ มาตรฐานใน “มาตรฐาน Payment Card Industry – Data Security Standard” ในหน้า 5
- เพิ่ม “คำสั่ง pscxpert” ในหน้า 31

พฤษภาคม 2013

เพิ่มตารางที่อธิบายวิธี ที่คุณลักษณะ AIX Security Expert แน่ใจว่าปฏิบัติตาม Payment Card Industry – Data Security Standard ใน “มาตรฐาน Payment Card Industry – Data Security Standard” ในหน้า 5

พฤศจิกายน 2012

ข้อมูลต่อไปนี้ จะมีสรุปของเนื้อหาใหม่และเนื้อหาที่ปรับปรุงสำหรับ PowerSC Express Edition 1.1.2:

- เพิ่มเอกสารที่อธิบายคุณลักษณะ Real Time Compliance ใน “PowerSC Real Time Compliance” ในหน้า 29
- เพิ่มเอกสารคู่มือสำหรับการสนับสนุนมาตรฐานดังกำหนด โดย “Health Insurance Portability and Accountability Act (HIPAA)” ในหน้า 19

แนวคิด PowerSC Express Edition 1.1.3

ภาพรวมของ PowerSC จะอธิบาย คุณลักษณะ, คอมโพเนนต์ และการสนับสนุนทางฮาร์ดแวร์ที่เกี่ยวข้องกับคุณลักษณะ PowerSC Express Edition

PowerSC Express Edition 1.1.3 จะมี การรักษาความปลอดภัย และการควบคุมของระบบปฏิบัติการภายในระบบคลาวด์ หรือใน ศูนย์ข้อมูลเสมือน และมีมุมมององค์กรและความสามารถ ในการจัดการ PowerSC Express Edition เป็นชุดคุณลักษณะที่ประกอบด้วย Security and Compliance Automation และ Real Time Compliance เทคโนโลยีการรักษาความปลอดภัย ที่อยู่ภายในเลเยอร์เทคโนโลยีเสมือนจัดให้มีการรักษาความปลอดภัย เพิ่มเติมสำหรับระบบสแตนด์อะโลน

ตารางต่อไปนี้จัดให้มีรายละเอียดเกี่ยวกับเอดิชัน คุณลักษณะ ที่รวมในเอดิชัน คอมโพเนนต์ และฮาร์ดแวร์ที่อิงตาม ตัวประมวลผลที่ซึ่งมีแต่ละคอมโพเนนต์อยู่

ตารางที่ 1. PowerSC Express Edition คอมโพเนนต์, คำอธิบาย, ระบบปฏิบัติการที่สนับสนุน และฮาร์ดแวร์ที่สนับสนุน

คอมโพเนนต์	คำอธิบาย	ระบบปฏิบัติการที่สนับสนุน	ฮาร์ดแวร์ที่สนับสนุน
ความปลอดภัยและความเข้ากันได้อัตโนมัติ	ทำให้การตั้งค่า การมอนิเตอร์ และการตรวจสอบการกำหนดคอนฟิก การรักษาความปลอดภัยและความเข้ากันได้เป็นอัตโนมัติสำหรับมาตรฐานต่อไปนี้: • Payment Card Industry Data Security Standard (PCI DSS) • Sarbanes-Oxley Act and COBIT compliance (SOX/COBIT) • U.S. Department of Defense (DoD) STIG • Health Insurance Portability and Accountability Act (HIPAA)	• AIX 5.3 • AIX 6.1 • AIX 7.1	• POWER5 • POWER6® • POWER7®
Real Time Compliance	มอนิเตอร์ระบบ AIX ที่เปิดใช้งานเพื่อดูแลการรักษาความปลอดภัย และ จัดให้มีการแจ้งเตือนเมื่อการเปลี่ยนแปลงระบบละเมิดกฎที่ระบุในนโยบายการกำหนดคอนฟิก	• 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	ไม่มีข้อกำหนดฮาร์ดแวร์ที่เจาะจง

การติดตั้ง PowerSC Express Edition เวอร์ชัน 1.1.3

PowerSC Express Edition มีแพ็กเกจ `powerscExp.ice` ซึ่งแพ็กเกจ `powerscExp.ice` สนับสนุน AIX 5.3, AIX 6.1 และ AIX เวอร์ชัน 7.1

แพ็กเกจ `powerscExp.ice` จ้องถูกติดตั้งบนระบบ AIX ทั้งหมด ที่ต้องการใช้คุณลักษณะความปลอดภัยและความร่วมมือของ PowerSC Express Edition

ติดตั้ง PowerSC Express Edition โดยใช้หนึ่งในอินเตอร์เฟสต่อไปนี้:

- คำสั่ง **installp** จากอินเตอร์เฟสบรรทัดรับคำสั่ง (CLI)

| • อินเตอร์เฟส SMIT

| เมื่อต้องการติดตั้ง PowerSC Express Edition โดยใช้ อินเตอร์เฟส SMIT ดำเนินขั้นตอนต่อไปนี้:

| 1. รันคำสั่งต่อไปนี้:

```
| % smitty installp
```

| 2. เลือกอ็อพชัน **ติดตั้งซอฟต์แวร์**

| 3. เลือกอุปกรณ์อินพุต หรือไดเร็กทอรีสำหรับซอฟต์แวร์เพื่อระบุ ตำแหน่งและไฟล์การติดตั้งของอิมเมจการติดตั้ง IBM Compliance Expert ตัวอย่างเช่น ถ้าอิมเมจการติดตั้งมีไดเร็กทอรีพาธ และชื่อไฟล์ `/usr/sys/inst.images/powerscExp.ice` คุณต้องระบุไฟล์พาธในฟิลด์ **INPUT**

| 4. ดูและยอมรับข้อตกลงไลเซนส์ ยอมรับข้อตกลงการอนุญาตใช้สิทธิ์ โดยใช้ลูกศรลงเพื่อเลือก **ยอมรับข้อตกลงการอนุญาตใช้สิทธิ์ใหม่** และกดปุ่ม tab เพื่อเปลี่ยนค่าเป็น **ใช่**

| 5. กด **Enter** เพื่อเริ่มต้นการติดตั้ง

| 6. ตรวจสอบว่าสถานะคำสั่งเป็น **ตกลง** หลังจากการติดตั้ง เสร็จสมบูรณ์

| ไฟล์ Readme ที่ชื่อ `README.ICEexpress` จะถูกติดตั้งในไดเร็กทอรี `/etc/security/aixpert` ไฟล์นี้จะมีรายละเอียดการปรับใช้สำหรับโปรไฟล์ Compliance ที่มีอยู่ใน PowerSC Express Edition

| การดูซอฟต์แวร์ไลเซนส์

| ซอฟต์แวร์ไลเซนส์ สามารถดูได้ใน CLI โดยใช้คำสั่งต่อไปนี้:

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

| โดย *path/filename* ระบุ อิมเมจการติดตั้ง PowerSC Standard Edition

| ตัวอย่างเช่น คุณสามารถป้อนคำสั่งต่อไปนี้โดยใช้ CLI เพื่อระบุข้อมูลไลเซนส์ที่เกี่ยวข้องกับ PowerSC Express Edition:

```
| % installp -lE -d  /usr/sys/inst.images/powerscExp.ice
```

|

ความปลอดภัยและความเข้ากันได้อัตโนมัติ

AIX Profile Manager จัดการ โปรไฟล์ที่กำหนดล่วงหน้าสำหรับความปลอดภัยและความเข้ากันได้ 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 คุณลักษณะความปลอดภัยและความเข้ากันได้มีอยู่ใน PowerSC Express Edition และ PowerSC Standard Edition

แพ็กเกจการติดตั้ง PowerSC Express Edition, 5765-G82 ต้องติดตั้งบนระบบที่ถูกจัดการ AIX แพ็กเกจการติดตั้ง ติดตั้ง `powerscExp.ice` fileset ที่สามารถอิมพลีเมนต์ บนระบบโดยใช้คำสั่ง AIX Profile Manager หรือ **aixpert** PowerSC ที่มีมาตรฐาน IBM Compliance Expert Express (ICEE) จะถูกเปิดใช้เพื่อจัดการและปรับปรุงโปรไฟล์ XML โปรไฟล์ XML ถูกจัดการโดย AIX Profile Manager

แนวคิดของความปลอดภัยและความเข้ากันได้อัตโนมัติ

คุณลักษณะการรักษาความปลอดภัยและความเข้ากันได้ PowerSC คือเมธอดอัตโนมัติ เพื่อกำหนดคอนฟิก และตรวจสอบระบบ AIX ตาม U.S. Department of Defense (DoD) Security Technical Implementation Guide (STIG)

PowerSC ช่วยให้ การกำหนดคอนฟิกและติดตามระบบโดยอัตโนมัติ ต้องเข้ากันได้กับมาตรฐานความปลอดภัยข้อมูล (DSS) เวอร์ชัน 1.2 ของ Payment Card Industry (PCI) 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) โปรไฟล์ PowerSC Express Edition xml สามารถใช้กับคำสั่ง **aixpert** คล้ายกับ ICEE

โปรไฟล์ความเข้ากันได้ที่กำหนดคอนฟิกล่วงหน้าถูกจัดส่งพร้อม PowerSC Express Edition ช่วยลดเวิร์กโหลดของการควบคุมดูแลสำหรับการตีความเอกสารคู่มือความเข้ากันได้ และการอิมพลีเมนต์มาตรฐานพารามิเตอร์ของคอนฟิกูเรชันระบบที่ระบุ เทคโนโลยีนี้ช่วยลดค่าใช้จ่ายในการกำหนดคอนฟิกความเข้ากันได้ และการตรวจสอบโดยกระบวนการอัตโนมัติ IBM PowerSC Express 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 คำสั่งนี้สร้างนโยบาย และกำหนดความรับผิดชอบต่อ defense information security agency (DISA) ของสหรัฐเพื่อจัดเตรียม คำแนะนำการกำหนดคอนฟิกด้านความปลอดภัย

DISA พัฒนาหลักการ และแนวทาง ใน UNIX STIG ที่จัดให้มี สภาวะแวดล้อมที่ตรงตาม หรือสูงกว่าข้อกำหนดการรักษาความปลอดภัย ของระบบ DoD ที่ดำเนินการตาม mission assurance category (MAC) II sensitive level ซึ่งมีข้อมูลสำคัญ U.S. DoD เข้มงวดต่อ ข้อกำหนดการรักษาความปลอดภัย IT และแจกแจงรายละเอียดของการตั้งค่า การกำหนดคอนฟิกที่ต้องการเพื่อให้แน่ใจว่าระบบดำเนินการในลักษณะที่มี ความปลอดภัย คุณสามารถ ยกระดับคำแนะนำของผู้เชี่ยวชาญที่จำเป็น PowerSC Express Edition ช่วยให้ กระบวนการกำหนดคอนฟิกค่าติดตั้งอัตโนมัติตามที่กำหนดโดย DoD

หมายเหตุ: ไฟล์สคริปต์ที่กำหนดเองทั้งหมดมีไว้ เพื่อดูแลรักษาความเข้ากันได้ DoD จะอยู่ในไดเร็กทอรี `/etc/security/pscexpert/bin`

ข้อมูลที่เกี่ยวข้อง:

มาตรฐาน 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

ส่วนที่ 1.1.5 และส่วนที่ 2.2.2: รายการเอกสาร ของเซอร์วิสและพอร์ตที่จำเป็นสำหรับธุรกิจ ข้อกำหนดนี้จะ ถูกใช้โดยการปิดใช้เซอร์วิสที่ไม่จำเป็น และเซอร์วิสที่ไม่ปลอดภัย

ส่วนที่ 1.3.6: การรักษาความปลอดภัย และการซิงโครไนซ์ไฟล์กำหนดค่าคอนฟิก เราเตอร์ ข้อกำหนดนี้จะถูกใช้โดยการตั้งค่า *clean_partial_conns* ของอ็อพชัน Network เป็น 1

ข้อกำหนดที่ 2: อย่าใช้ค่าดีฟอลต์ที่กำหนดโดยผู้จำหน่ายสำหรับ รหัสผ่านของระบบและพารามิเตอร์ความปลอดภัยอื่นๆ

ส่วนที่ 2.1: เปลี่ยนค่าดีฟอลต์ที่กำหนดโดยผู้จำหน่ายเสมอ ก่อนที่คุณจะติดตั้งระบบบนเครือข่าย ข้อกำหนดนี้จะถูกใช้โดยการปิดใช้งาน Simple Network Management Protocol (SNMP) daemon

ข้อกำหนดที่ 3: ปกป้องข้อมูลที่จัดเก็บไว้ของสมาชิก

ข้อกำหนดนี้จะถูกใช้โดยการเปิดใช้งาน คุณลักษณะ Encrypted File System (EFS) ที่มาพร้อมกับระบบปฏิบัติการ AIX

ข้อกำหนดที่ 4: เข้ารหัสข้อมูลของสมาชิกเมื่อคุณส่ง ข้อมูลข้ามเครือข่ายพับลิกที่เปิด

ข้อกำหนดนี้จะถูกใช้โดยการเปิดใช้ คุณลักษณะ IP Security (IPSEC) ที่มาพร้อมกับระบบปฏิบัติการ AIX

ข้อกำหนดที่ 5: ใช้ และอัพเดตโปรแกรมซอฟต์แวร์ป้องกันไวรัส

ข้อกำหนดนี้จะถูกใช้โดยการใช้โปรแกรมนโยบาย Trusted Execution Trusted Execution เป็นซอฟต์แวร์ป้องกันไวรัสที่แนะนำ และมีอยู่ในระบบปฏิบัติการ AIX PCI ต้องการให้คุณ บันทึกล็อกจากโปรแกรม Trusted Execution โดยการเปิดใช้ข้อมูล การรักษาความปลอดภัย และการจัดการเหตุการณ์ (SIEM) เพื่อมอนิเตอร์การแจ้งเตือน โดย การรันโปรแกรม Trusted Execution ในโหมดบันทึกเท่านั้น โปรแกรมจะ ไม่หยุดการตรวจสอบเมื่อเกิดข้อผิดพลาดจากแฮชไม่ตรงกัน

ข้อกำหนดที่ 6: พัฒนาและดูแลรักษาระบบความปลอดภัยและแอ็พพลิเคชัน

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

ข้อกำหนดที่ 7: จำกัดการเข้าถึงข้อมูลผู้ถือบัตร ตามที่ธุรกิจ จำเป็นต้องรู้

คุณสามารถใช้มาตรการการควบคุมการเข้าถึงที่ปลอดภัย โดยการใช้คุณลักษณะ RBAC เพื่อเปิดใช้กฎและบทบาท RBAC ไม่สามารถ ดำเนินการโดยอัตโนมัติเนื่องจากต้องมีอินพุทของผู้ดูแลระบบเพื่อ เปิดใช้

RbacEnablement จะตรวจสอบระบบ เพื่อระบุว่าคุณสมบัติ isso, so และ sa สำหรับบทบาท มีอยู่บนระบบหรือไม่ หากคุณสมบัติเหล่านี้ไม่มีอยู่ สคริปต์ จะสร้างขึ้นมา สคริปต์นี้ยังถูกรันเป็นส่วนหนึ่งของการตรวจสอบ AIXPert ที่จะเสร็จสมบูรณ์เมื่อรันคำสั่ง เช่น คำสั่ง aixpert -c

ขั้นตอนที่ 8: กำหนด ID เฉพาะให้กับแต่ละบุคคลที่มีการเข้าถึง คอมพิวเตอร์

คุณสามารถใช้ข้อกำหนดนี้โดยการเปิดใช้ โปรไฟล์ PCI กฎต่อไปนี้จะใช้ถูกนำมาใช้กับนโยบาย PCI:

- ส่วนที่ 8.5.9: เปลี่ยนแปลงรหัสผ่านผู้ใช้อย่างน้อยทุกๆ 90 วัน
- ส่วนที่ 8.5.10: ต้องมีความยาวรหัสผ่านต่ำสุดเท่ากับ 7 อักขระ
- ส่วนที่ 8.5.11: ใช้รหัสผ่านที่มีทั้งตัวเลข และ ตัวอักษร
- ส่วนที่ 8.5.12: ไม่อนุญาตให้แต่ละบุคคลส่งรหัสผ่านใหม่ ที่เป็นรหัสผ่านเดียวกับรหัสผ่านสี่ตัวที่ใช้ก่อนหน้านี้
- ส่วนที่ 8.5.13: จำกัดความพยายามในการเข้าถึงซ้ำโดยการล็อก ID ผู้ใช้หลังจากการพยายามเข้าถึงที่ไม่สำเร็จ 6 ครั้ง
- ส่วนที่ 8.5.14: ตั้งค่าช่วงเวลาการล็อกเท่ากับ 30 นาที หรือจนกว่า ผู้ดูแลระบบจะเปิดใช้ ID ผู้ใช้ใหม่อีกครั้ง
- ส่วนที่ 8.5.15: ต้องให้ผู้ใช้ป้อนรหัสผ่านใหม่อีกครั้งเพื่อเปิดใช้ เทอร์มินัลหลังกจากไม่ได้ทำงานเป็นเวลา 15 นาทีหรือนานกว่า

ข้อกำหนดที่ 9: จำกัดการเข้าถึงทางกายภาพต่อข้อมูลผู้ถือบัตร

จัดเก็บที่เก็บข้อมูลที่มีข้อมูลผู้ถือบัตรที่สำคัญ ในห้องที่มีการจำกัดการเข้าถึง

ข้อกำหนดที่ 10: ติดตามและเฝ้าดูการเข้าถึงรีซอร์สเครือข่าย และข้อมูลผู้ถือบัตรทั้งหมด

ส่วนที่ 10.2: ข้อกำหนดนี้จะถูกใช้โดย การล็อกอินเพื่อเข้าถึงคอมโพเนนต์ระบบโดยการเปิดใช้การ ล็อกออนไปยังคอมโพเนนต์ระบบโดยอัตโนมัติ

ข้อกำหนดที่ 11: ทดสอบระบบและกระบวนการด้านความปลอดภัยเป็นประจำ

ข้อกำหนดนี้จะถูกใช้โดยการใช้คุณลักษณะ Real-Time Compliance

ข้อกำหนดที่ 12: รักษานโยบายการรักษาความปลอดภัยที่มีข้อมูล ความปลอดภัยของพนักงานและผู้รับจ้าง

ส่วนที่ 12.3.9: เปิดใช้งานโมเด็มเฉพาะสำหรับผู้จำหน่ายเมื่อจำเป็น ต้องใช้ และปิดใช้งานทันทีหลังจากการใช้ ข้อกำหนดนี้ จะถูกใช้โดยการปิดใช้การล็อกอินรูทแบบรีโมท การเปิดใช้บนพื้นฐาน ที่จำเป็นโดยผู้ดูแลระบบ จากนั้นจะปิดใช้งานเมื่อ ไม่จำเป็นต้องใช้

PowerSC Express Edition จะลดการจัดการการกำหนดค่าคอนฟิกที่จำเป็นเพื่อให้ตรง ตามแนวทางที่กำหนดโดย PCI DSS อย่างไรก็ตาม กระบวนการทั้งหมดไม่สามารถดำเนินการแบบอัตโนมัติ

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

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

ตารางต่อไปนี้แสดงวิธี PowerSC Express Edition ระบุ ข้อกำหนดของมาตรฐาน PCI DSS โดยการใช้ฟังก์ชันของ ยูทิลิตี้ AIX Security Expert :

ตารางที่ 2. การตั้งค่าที่เกี่ยวข้องกับมาตรฐานการปฏิบัติตามข้อกำหนด PCI DSS 2.0

การปรับใช้มาตรฐาน PCI DSS เหล่านี้	ข้อมูลจำเพาะการนำไปปฏิบัติ	การปรับใช้ AIX Security Expert	ตำแหน่งของค่าและการตั้งค่าที่ จำเป็นสำหรับการปฏิบัติตาม (ถ้ามี)
2.1	เปลี่ยนค่าดีฟอลต์ที่กำหนดโดยผู้จำหน่ายเสมอก่อน การติดตั้งระบบบนเครือข่าย ตัวอย่างเช่น สตริงชุมชนของโปรโตคอล การจัดการเครือข่ายพื้นฐาน รวมถึงรหัสผ่าน และลบ บัญชีที่ไม่จำเป็นออก	ตั้งค่าจำนวนต่ำสุดของสัปดาห์ที่ต้องผ่านไป ก่อนที่คุณจะสามารถเปลี่ยนรหัสผ่านให้เท่ากับ 0 สัปดาห์	**ตำแหน่ง** /etc/security/pscexpert/bin/chusrattr **ค่ามาตรฐาน** minage=0
8.5.9	เปลี่ยนแปลงรหัสผ่านผู้ใช้อย่างน้อยทุกๆ 90 วัน	ตั้งค่าจำนวนต่ำสุดของสัปดาห์ที่รหัสผ่าน สามารถใช้งานได้เป็น 13 สัปดาห์	**ตำแหน่ง** /etc/security/pscexpert/bin/chusrattr **ค่ามาตรฐาน** maxage=13
2.1	เปลี่ยนค่าดีฟอลต์ที่กำหนดโดยผู้จำหน่ายเสมอก่อน การติดตั้งระบบบนเครือข่าย ตัวอย่างเช่น สตริงชุมชนของโปรโตคอล การจัดการเครือข่ายพื้นฐาน รวมถึงรหัสผ่าน และลบ บัญชีที่ไม่จำเป็นออก	ตั้งค่าจำนวนสัปดาห์ที่บัญชีที่มีรหัสผ่านที่หมดอายุสามารถอยู่ในระบบเป็น 8 สัปดาห์	**ตำแหน่ง** /etc/security/pscexpert/bin/chusrattr **ค่ามาตรฐาน** maxexpired=8
8.5.10	ต้องมีความยาวรหัสผ่านต่ำสุดอย่างน้อย 7 ตัวอักษร	ตั้งค่าความยาวรหัสผ่านต่ำสุดเท่ากับ 7 ตัวอักษร	**ตำแหน่ง** /etc/security/pscexpert/bin/chusrattr **ค่ามาตรฐาน** minlen=7
8.5.11	ใช้รหัสผ่านที่มีทั้งตัวเลขและตัวอักษร	ตั้งค่าจำนวนต่ำสุดของตัวอักษรที่จำเป็นต้องมีในรหัสผ่านเท่ากับ 1 การตั้งค่านี้เพื่อให้แน่ใจว่า รหัสผ่านจะประกอบด้วยตัวอักษร	**ตำแหน่ง** /etc/security/pscexpert/bin/chusrattr **ค่ามาตรฐาน** minalpha=1
8.5.11	ใช้รหัสผ่านที่มีทั้งตัวเลขและตัวอักษร	ตั้งค่าจำนวนต่ำสุดของอักขระที่ไม่ใช่ตัวอักษร ที่จำเป็นต้องมีในรหัสผ่านเท่ากับ 1 การตั้งค่านี้เพื่อให้แน่ใจว่า รหัสผ่านจะประกอบด้วยอักขระที่ไม่ใช่ตัวอักษร	**ตำแหน่ง** /etc/security/pscexpert/bin/chusrattr **ค่ามาตรฐาน** minother=1
2.1	เปลี่ยนค่าดีฟอลต์ที่กำหนดโดยผู้จำหน่ายเสมอก่อน การติดตั้งระบบบนเครือข่าย ตัวอย่างเช่น สตริงชุมชนของโปรโตคอล การจัดการเครือข่ายพื้นฐาน รวมถึงรหัสผ่าน และลบ บัญชีที่ไม่จำเป็นออก	ตั้งค่าจำนวนครั้งต่ำสุดที่ตัวอักษรสามารถซ้ำกันในรหัสผ่านเท่ากับ 8 การตั้งค่านี้จะระบุว่า ตัวอักษรในรหัสผ่านสามารถซ้ำกันได้โดยไม่จำกัดจำนวนครั้ง ตามใดที่เป็นไปตามข้อจำกัดของรหัสผ่านอื่นๆ	**ตำแหน่ง** /etc/security/pscexpert/bin/chusrattr **ค่ามาตรฐาน** maxrepeats=8

ตารางที่ 2. การตั้งค่าที่เกี่ยวข้องกับมาตรฐานการปฏิบัติตามข้อกำหนด PCI DSS 2.0 (ต่อ)

การปรับใช้มาตรฐาน PCI DSS เหล่านี้	ข้อมูลจำเพาะการนำไปปฏิบัติ	การปรับใช้ AIX Security Expert	ตำแหน่งของค่าและการตั้งค่าที่ จำเป็นสำหรับการปฏิบัติตาม (ถ้ามี)
8.5.12	ไม่อนุญาตให้แต่ละบุคคลส่งรหัสผ่านใหม่ ที่เป็นรหัสผ่านเดียวกับรหัสผ่านสี่ตัวที่ใช้ก่อนหน้านี้	ตั้งค่าจำนวนสัปดาห์ก่อนที่จะสามารถนำรหัสผ่าน กลับมาใช้ใหม่เท่ากับ 52	**ตำแหน่ง** `/etc/security/pscexpert/bin/chusrattr` **ค่ามาตรฐาน** histexpire=52
8.5.12	ไม่อนุญาตให้แต่ละบุคคลส่งรหัสผ่านใหม่ ที่เป็นรหัสผ่านเดียวกับรหัสผ่านสี่ตัวที่ใช้ก่อนหน้านี้	ตั้งค่าจำนวนของรหัสผ่านก่อนหน้าที่คุณ ไม่สามารถนำกลับมาใช้เท่ากับ 4	**ตำแหน่ง** `/etc/security/pscexpert/bin/chusrattr` **ค่ามาตรฐาน** histsize=4
8.5.13	จำกัดความพยายามในการเข้าถึงซ้ำโดยการล็อก ID ผู้ใช้หลังจากการพยายามเข้าถึงที่ไม่สำเร็จ 6 ครั้ง	ตั้งค่าจำนวนของความพยายามในการล็อกอิน ที่ไม่สำเร็จต่อเนื่องกันที่ปิดใช้งานบัญชีเท่ากับความพยายาม 6 ครั้งสำหรับแต่ละบัญชีผู้ใช้ ที่ไม่ใช่รูท	**ตำแหน่ง** `/etc/security/pscexpert/bin/chusrattr` **ค่ามาตรฐาน** loginretries=6
8.5.13	จำกัดความพยายามในการเข้าถึงซ้ำโดยการล็อก ID ผู้ใช้หลังจากการพยายามเข้าถึงที่ไม่สำเร็จ 6 ครั้ง	ตั้งค่าจำนวนความพยายามในการล็อกอิน ที่ไม่สำเร็จต่อเนื่องกันที่ปิดใช้งานพอร์ตเท่ากับความพยายาม 6 ครั้ง	**ตำแหน่ง** `/etc/security/pscexpert/bin/chdefstanza` `/etc/security/login.cfg` **ค่ามาตรฐาน** logindisable=6
8.5.14	ตั้งค่าช่วงเวลาการล็อกเท่ากับ 30 นาที หรือจนกว่า ผู้ดูแลระบบจะเปิดใช้ ID ผู้ใช้ใหม่อีกครั้ง	ตั้งค่าระยะเวลาที่พอร์ตถูกล็อกหลังจากถูกปิดใช้งานโดยแอ็ตทริบิวต์ *logindisable* เท่ากับ 30 นาที	**ตำแหน่ง** `/etc/security/pscexpert/bin/chdefstanza` `/etc/security/login.cfg` **ค่ามาตรฐาน** loginreenable=30
12.3.9	เปิดใช้งานเทคโนโลยีการเข้าถึงแบบรีโมทสำหรับ ผู้จำหน่ายและหุ้นส่วนทางธุรกิจเฉพาะเมื่อจำเป็นต้องใช้โดยผู้จำหน่ายและหุ้นส่วน ทางธุรกิจ และปิดใช้งานทันทีหลังจากใช้	ปิดใช้งานฟังก์ชันการล็อกอินรูทแบบรีโมทโดยการตั้งค่า เป็น False ผู้ดูแลระบบสามารถเปิดใช้งานฟังก์ชันการล็อกอิน แบบรีโมทเมื่อต้องการ จากนั้นให้ปิดใช้งานเมื่องาน เสร็จสมบูรณ์	**ตำแหน่ง** `/etc/security/pscexpert/bin/chuserstanza` `/etc/security/user` **ค่ามาตรฐาน** rlogin=false root
8.1	กำหนด ID เฉพาะให้กับผู้ใช้ทั้งหมดก่อนที่จะอนุญาต ให้สามารถเข้าถึงคอมโพเนนต์ระบบหรือข้อมูลของผู้ถือบัตร	เปิดใช้งานฟังก์ชันโดยแน่ใจว่าผู้ใช้ทั้งหมด มีชื่อผู้ใช้ที่ไม่ซ้ำกันก่อนที่จะสามารถเข้าถึงคอมโพเนนต์ระบบหรือ ข้อมูลผู้ถือบัตรโดยการตั้งค่าฟังก์ชันนั้นให้มีค่าเป็น True	**ตำแหน่ง** `/etc/security/pscexpert/bin/chuserstanza` `/etc/security/user` **ค่ามาตรฐาน** login=true root

ตารางที่ 2. การตั้งค่าที่เกี่ยวข้องกับมาตรฐานการปฏิบัติตามข้อกำหนด PCI DSS 2.0 (ต่อ)

การปรับใช้มาตรฐาน PCI DSS เหล่านี้	ข้อมูลจำเพาะการนำไปปฏิบัติ	การปรับใช้ AIX Security Expert	ตำแหน่งของค่าและการตั้งค่าที่ จำเป็นสำหรับการปฏิบัติตาม (ถ้ามี)
10.2	เปิดใช้งานการตรวจสอบบนระบบ	เปิดใช้งานการตรวจสอบไฟล์ไลบรารีบน ระบบ	**ตำแหน่ง** `/etc/security/pscexpert/bin/pciaudit` **ค่ามาตรฐาน** `h`
1.1.5 2.2.2	ปิดใช้งานเซอร์วิสที่ไม่ปลอดภัยและเซอร์วิสที่ไม่จำเป็น ซึ่ง รวมถึง `lpd` daemon	หยุด `lpd` daemon และคอมเม้นต์รายการที่เกี่ยวข้องในไฟล์ `/etc/inittab` ที่สตาร์ท daemon โดยอัตโนมัติ	**ตำแหน่ง** `/etc/security/pscexpert/bin/comntrows` **ค่ามาตรฐาน** `lpd: /etc/inittab : d`
1.1.5 2.2.2	ปิดใช้งานเซอร์วิสที่ไม่ปลอดภัยและเซอร์วิสที่ไม่จำเป็น ซึ่ง รวมถึง Common Desktop Environment (CDE)	ปิดใช้งานฟังก์ชัน CDE เมื่อ layer four traceroute (LFT) ไม่ถูกกำหนดค่าคอนฟิกไว้	**ตำแหน่ง** `/etc/security/pscexpert/bin/comntrows` **ค่ามาตรฐาน** `"dt" "/etc/inittab" ":" d`
1.1.5 2.2.2	ปิดใช้งานเซอร์วิสที่ไม่ปลอดภัยและเซอร์วิสที่ไม่จำเป็น ซึ่ง รวมถึง `timed` daemon	หยุด `timed` daemon และ คอมเม้นต์รายการที่เกี่ยวข้องในไฟล์ `/etc/rc.tcpip` ที่สตาร์ท daemon โดยอัตโนมัติ	**ตำแหน่ง** `/etc/security/pscexpert/bin/rctcpip` **ค่ามาตรฐาน** `timed d`
1.1.5 2.2.2	ปิดใช้งานเซอร์วิสที่ไม่ปลอดภัยและเซอร์วิสที่ไม่จำเป็น ซึ่ง รวมถึง `NTP` daemon	หยุด `NTP` daemon และคอมเม้นต์รายการที่เกี่ยวข้องในไฟล์ `/etc/rc.tcpip` ที่สตาร์ท daemon โดยอัตโนมัติ	**ตำแหน่ง** `/etc/security/pscexpert/bin/rctcpip` **ค่ามาตรฐาน** `xntpd d`
1.1.5 2.2.2	ปิดใช้งานเซอร์วิสที่ไม่ปลอดภัยและเซอร์วิสที่ไม่จำเป็น ซึ่ง รวมถึง `rwhod` daemon	หยุด `rwhod` daemon และ คอมเม้นต์รายการที่เกี่ยวข้องในไฟล์ `/etc/rc.tcpip` ที่สตาร์ท daemon โดยอัตโนมัติ	**ตำแหน่ง** `/etc/security/pscexpert/bin/rctcpip` **ค่ามาตรฐาน** `rwhod d`
2.1	เปลี่ยนค่าดีฟอลต์ที่กำหนดโดยผู้จำหน่ายก่อนการติดตั้ง ระบบบนเครือข่าย ซึ่งรวมถึงการปิดใช้งาน `SNMP` daemon	หยุด `SNMP` daemon และคอมเม้นต์ รายการที่เกี่ยวข้องในไฟล์ `/etc/rc.tcpip` ที่สตาร์ท daemon โดยอัตโนมัติ	**ตำแหน่ง** `/etc/security/pscexpert/bin/rctcpip` **ค่ามาตรฐาน** `snmpd d`
2.1	เปลี่ยนค่าดีฟอลต์ที่กำหนดโดยผู้จำหน่ายก่อนการติดตั้ง ระบบบนเครือข่าย ซึ่งรวมถึงการปิดใช้งาน `SNMPMIBD` daemon	ปิดใช้งาน `SNMPMIBD` daemon	**ตำแหน่ง** `/etc/security/pscexpert/bin/rctcpip` **ค่ามาตรฐาน** `snmpmibd d`
2.1	เปลี่ยนค่าดีฟอลต์ที่กำหนดโดยผู้จำหน่ายก่อนการติดตั้ง ระบบบนเครือข่าย ซึ่งรวมถึงการปิดใช้งาน `AIXMIBD` daemon	ปิดใช้งาน `AIXMIBD` daemon	**ตำแหน่ง** `/etc/security/pscexpert/bin/rctcpip` **ค่ามาตรฐาน** `aixmibd d`

ตารางที่ 2. การตั้งค่าที่เกี่ยวข้องกับมาตรฐานการปฏิบัติตามข้อกำหนด PCI DSS 2.0 (ต่อ)

การปรับใช้มาตรฐาน PCI DSS เหล่านี้	ข้อมูลจำเพาะการนำไปปฏิบัติ	การปรับใช้ AIX Security Expert	ตำแหน่งของค่าและการตั้งค่าที่ จำเป็นสำหรับการปฏิบัติตาม (ถ้ามี)
2.1	เปลี่ยนค่าดีฟอลต์ที่กำหนดโดยผู้จำหน่ายก่อนการติดตั้ง ระบบบนเครือข่าย ซึ่งรวมถึงการปิดใช้งาน HOSTMIBD daemon	ปิดใช้งาน HOSTMIBD daemon	**ตำแหน่ง** /etc/security/pscexpert/bin/rctcpip **ค่ามาตรฐาน** hostmibd d
1.1.5 2.2.2	ปิดใช้งานเซอร์วิสที่ไม่ปลอดภัยและเซอร์วิสที่ไม่จำเป็น ซึ่ง รวมถึง DPID2 daemon	หยุด DPID2 daemon และ คอมเม้นต์รายการที่เกี่ยวข้องในไฟล์ /etc/rc.tcpip ที่สตาร์ท daemon โดยอัตโนมัติ	**ตำแหน่ง** /etc/security/pscexpert/bin/rctcpip **ค่ามาตรฐาน** dpid2 d
2.1	เปลี่ยนค่าดีฟอลต์ที่กำหนดโดยผู้จำหน่ายก่อนการติดตั้ง ระบบบนเครือข่าย ซึ่งรวมถึงการหยุดเซิร์ฟเวอร์ DHCP	ปิดใช้งานเซิร์ฟเวอร์ DHCP	**ตำแหน่ง** /etc/security/pscexpert/bin/rctcpip **ค่ามาตรฐาน** dhcpsd d
1.1.5 2.2.2	ปิดใช้งานเซอร์วิสที่ไม่ปลอดภัยและเซอร์วิสที่ไม่จำเป็น ซึ่ง รวมถึงเอเจนต์ DHCP	หยุดและปิดใช้งานเอเจนต์รีเลย์ DHCP และคอมเม้นต์รายการที่เกี่ยวข้องในไฟล์ /etc/rc.tcpip ที่สตาร์ทเอเจนต์โดยอัตโนมัติ	**ตำแหน่ง** /etc/security/pscexpert/bin/rctcpip **ค่ามาตรฐาน** dhcprd d
1.1.5 2.2.2	ปิดใช้งานเซอร์วิสที่ไม่ปลอดภัยและเซอร์วิสที่ไม่จำเป็น ซึ่ง รวมถึง rshd daemon	หยุดและปิดใช้งานอินสแตนซ์ทั้งหมดของ rshd และเซอร์วิส rshdpci_shell และคอมเม้นต์รายการที่เกี่ยวข้องในไฟล์ /etc/inetd.conf ที่สตาร์ทอินสแตนซ์โดยอัตโนมัติ	**ตำแหน่ง** /etc/security/pscexpert/bin/cominetdconf **ค่ามาตรฐาน** shell tcp d
1.1.5 2.2.2	ปิดใช้งานเซอร์วิสที่ไม่ปลอดภัยและเซอร์วิสที่ไม่จำเป็น ซึ่ง รวมถึง rlogind daemon	หยุดและปิดใช้งานอินสแตนซ์ทั้งหมดของ rlogind daemon และเซอร์วิส rlogindpci.rlogin ยูทิลิตี้ AIX Security Expert ยัง คอมเม้นต์รายการที่เกี่ยวข้องในไฟล์ /etc/inetd.conf ที่สตาร์ทอินสแตนซ์โดยอัตโนมัติ	**ตำแหน่ง** /etc/security/pscexpert/bin/cominetdconf **ค่ามาตรฐาน** login tcp d
1.1.5 2.2.2	ปิดใช้งานเซอร์วิสที่ไม่ปลอดภัยและเซอร์วิสที่ไม่จำเป็น ซึ่ง รวมถึง rexecd daemon	หยุดและปิดใช้งานอินสแตนซ์ทั้งหมดของ rexecd daemon ยูทิลิตี้ AIX Security Expert ยังคอมเม้นต์รายการที่เกี่ยวข้อง ในไฟล์ /etc/inetd.conf ที่สตาร์ท daemon โดยอัตโนมัติ	**ตำแหน่ง** /etc/security/pscexpert/bin/cominetdconf **ค่ามาตรฐาน** exec tcp d
1.1.5 2.2.2	ปิดใช้งานเซอร์วิสที่ไม่ปลอดภัยและเซอร์วิสที่ไม่จำเป็น ซึ่ง รวมถึง comsat daemon	หยุดและปิดใช้งานอินสแตนซ์ทั้งหมดของ comsat daemon ยูทิลิตี้ AIX Security Expert ยังคอมเม้นต์รายการที่เกี่ยวข้อง ในไฟล์ /etc/inetd.conf ที่สตาร์ท daemon โดยอัตโนมัติ	**ตำแหน่ง** /etc/security/pscexpert/bin/cominetdconf **ค่ามาตรฐาน** comsat udp d

ตารางที่ 2. การตั้งค่าที่เกี่ยวข้องกับมาตรฐานการปฏิบัติตามข้อกำหนด PCI DSS 2.0 (ต่อ)

การปรับใช้มาตรฐาน PCI DSS เหล่านี้	ข้อมูลจำเพาะการนำไปปฏิบัติ	การปรับใช้ AIX Security Expert	ตำแหน่งของค่าและการตั้งค่าที่ จำเป็นสำหรับการปฏิบัติตาม (ถ้ามี)
1.1.5 2.2.2	ปิดใช้งานเซอร์วิสที่ไม่ปลอดภัยและเซอร์วิสที่ไม่จำเป็น ซึ่ง รวมถึง `fingerd` daemon	หยุดและปิดใช้งานอินสแตนซ์ทั้งหมดของ `fingerd` daemon ยูทิลิตี้ AIX Security Expert ยังคอมเม้นต์รายการที่เกี่ยวข้อง ในไฟล์ `/etc/inetd.conf` ที่สตาร์ท daemon โดยอัตโนมัติ	**ตำแหน่ง** `/etc/security/pscexpert/bin/cominetdconf` **ค่ามาตรฐาน** finger tcp d
1.1.5 2.2.2	ปิดใช้งานเซอร์วิสที่ไม่ปลอดภัยและเซอร์วิสที่ไม่จำเป็น ซึ่ง รวมถึง `systat` daemon	หยุดและปิดใช้งานอินสแตนซ์ทั้งหมดของ `systat` daemon ยูทิลิตี้ AIX Security Expert ยังคอมเม้นต์รายการที่เกี่ยวข้อง ในไฟล์ `/etc/inetd.conf` ที่สตาร์ท daemon โดยอัตโนมัติ	**ตำแหน่ง** `/etc/security/pscexpert/bin/cominetdconf` **ค่ามาตรฐาน** systat tcp d
2.1	เปลี่ยนค่าดีฟอลต์ที่กำหนดโดยผู้จำหน่ายก่อนการติดตั้ง ระบบบนเครือข่าย ซึ่งรวมถึงการปิดใช้งานคำสั่ง `netstat`	ปิดใช้งานคำสั่ง `netstat`	**ตำแหน่ง** `/etc/security/pscexpert/bin/cominetdconf` **ค่ามาตรฐาน** netstat tcp d
1.1.5 2.2.2	ปิดใช้งานเซอร์วิสที่ไม่ปลอดภัยและเซอร์วิสที่ไม่จำเป็น ซึ่ง รวมถึง `tftp` daemon	หยุดและปิดใช้งานอินสแตนซ์ทั้งหมดของ `tftp` daemon ยูทิลิตี้ AIX Security Expert ยังคอมเม้นต์รายการที่เกี่ยวข้อง ในไฟล์ `/etc/inetd.conf` ที่สตาร์ท daemon โดยอัตโนมัติ	**ตำแหน่ง** `/etc/security/pscexpert/bin/cominetdconf` **ค่ามาตรฐาน** tftp udp d
1.1.5 2.2.2	ปิดใช้งานเซอร์วิสที่ไม่ปลอดภัยและเซอร์วิสที่ไม่จำเป็น ซึ่ง รวมถึง `talkd` daemon	หยุดและปิดใช้งานอินสแตนซ์ทั้งหมดของ `talkd` daemon ยูทิลิตี้ AIX Security Expert ยังคอมเม้นต์รายการที่เกี่ยวข้อง ในไฟล์ `/etc/inetd.conf` ที่สตาร์ท daemon โดยอัตโนมัติ	**ตำแหน่ง** `/etc/security/pscexpert/bin/cominetdconf` **ค่ามาตรฐาน** talk udp d
1.1.5 2.2.2	ปิดใช้งานเซอร์วิสที่ไม่ปลอดภัยและเซอร์วิสที่ไม่จำเป็น ซึ่ง รวมถึง `rquotad` daemon	หยุดและปิดใช้งานอินสแตนซ์ทั้งหมดของ `rquotad` daemon ยูทิลิตี้ AIX Security Expert ยังคอมเม้นต์รายการที่เกี่ยวข้อง ในไฟล์ `/etc/inetd.conf` ที่สตาร์ท daemon โดยอัตโนมัติ	**ตำแหน่ง** `/etc/security/pscexpert/bin/cominetdconf` **ค่ามาตรฐาน** rquotad udp d
1.1.5 2.2.2	ปิดใช้งานเซอร์วิสที่ไม่ปลอดภัยและเซอร์วิสที่ไม่จำเป็น ซึ่ง รวมถึง `rstatd` daemon	หยุดและปิดใช้งานอินสแตนซ์ทั้งหมดของ `rstatd` daemon ยูทิลิตี้ AIX Security Expert ยังคอมเม้นต์รายการที่เกี่ยวข้อง ในไฟล์ `/etc/inetd.conf` ที่สตาร์ท daemon โดยอัตโนมัติ	**ตำแหน่ง** `/etc/security/pscexpert/bin/cominetdconf` **ค่ามาตรฐาน** rstatd udp d

ตารางที่ 2. การตั้งค่าที่เกี่ยวข้องกับมาตรฐานการปฏิบัติตามข้อกำหนด PCI DSS 2.0 (ต่อ)

การปรับใช้มาตรฐาน PCI DSS เหล่านี้	ข้อมูลจำเพาะการนำไปปฏิบัติ	การปรับใช้ AIX Security Expert	ตำแหน่งของค่าและการตั้งค่าที่ จำเป็นสำหรับการปฏิบัติตาม (ถ้ามี)
1.1.5 2.2.2	ปิดใช้งานเซอร์วิสที่ไม่ปลอดภัยและเซอร์วิสที่ไม่จำเป็น ซึ่ง รวมถึง rusersd daemon	หยุดและปิดใช้งานอินสแตนซ์ทั้งหมดของ rusersd daemon ยูทิลิตี้ AIX Security Expert ยังคอมเม้นต์รายการที่เกี่ยวข้อง ในไฟล์ /etc/inetd.conf ที่สตาร์ท daemon โดยอัตโนมัติ	**ตำแหน่ง** /etc/security/pscexpert/bin/cominetdconf **ค่ามาตรฐาน** rusersd udp d
1.1.5 2.2.2	ปิดใช้งานเซอร์วิสที่ไม่ปลอดภัยและเซอร์วิสที่ไม่จำเป็น ซึ่ง รวมถึง rwalld daemon	หยุดและปิดใช้งานอินสแตนซ์ทั้งหมดของ rwalld daemon ยูทิลิตี้ AIX Security Expert ยังคอมเม้นต์รายการที่เกี่ยวข้อง ในไฟล์ /etc/inetd.conf ที่สตาร์ท daemon โดยอัตโนมัติ	**ตำแหน่ง** /etc/security/pscexpert/bin/cominetdconf **ค่ามาตรฐาน** rwalld udp d
1.1.5 2.2.2	ปิดใช้งานเซอร์วิสที่ไม่ปลอดภัยและเซอร์วิสที่ไม่จำเป็น ซึ่ง รวมถึง sprayd daemon	หยุดและปิดใช้งานอินสแตนซ์ทั้งหมดของ sprayd daemon ยูทิลิตี้ AIX Security Expert ยังคอมเม้นต์รายการที่เกี่ยวข้อง ในไฟล์ /etc/inetd.conf ที่สตาร์ท daemon โดยอัตโนมัติ	**ตำแหน่ง** /etc/security/pscexpert/bin/cominetdconf **ค่ามาตรฐาน** sprayd udp d
1.1.5 2.2.2	ปิดใช้งานเซอร์วิสที่ไม่ปลอดภัยและเซอร์วิสที่ไม่จำเป็น ซึ่ง รวมถึง pcnfsd daemon	หยุดและปิดใช้งานอินสแตนซ์ทั้งหมดของ pcnfsd daemon ยูทิลิตี้ AIX Security Expert ยังคอมเม้นต์รายการที่เกี่ยวข้อง ในไฟล์ /etc/inetd.conf ที่สตาร์ท daemon โดยอัตโนมัติ	**ตำแหน่ง** /etc/security/pscexpert/bin/cominetdconf **ค่ามาตรฐาน** pcnfsd udp d
1.1.5 2.2.2	ปิดใช้งานเซอร์วิสที่ไม่ปลอดภัยและเซอร์วิสที่ไม่จำเป็น ซึ่ง รวมถึงเซอร์วิส TCP echo	หยุดและปิดใช้งานอินสแตนซ์ทั้งหมดของเซอร์วิส echo(tcp) ยูทิลิตี้ AIX Security Expert ยังคอมเม้นต์รายการที่เกี่ยวข้อง ในไฟล์ /etc/inetd.conf ที่สตาร์ท เซอร์วิสโดยอัตโนมัติ	**ตำแหน่ง** /etc/security/pscexpert/bin/cominetdconf **ค่ามาตรฐาน** echo tcp d
1.1.5 2.2.2	ปิดใช้งานเซอร์วิสที่ไม่ปลอดภัยและเซอร์วิสที่ไม่จำเป็น ซึ่ง รวมถึงเซอร์วิส TCP discard	หยุดและปิดใช้งานอินสแตนซ์ทั้งหมดของเซอร์วิส discard(tcp) ยูทิลิตี้ AIX Security Expert ยังคอมเม้นต์รายการที่เกี่ยวข้อง ในไฟล์ /etc/inetd.conf ที่สตาร์ท เซอร์วิสโดยอัตโนมัติ	**ตำแหน่ง** /etc/security/pscexpert/bin/cominetdconf **ค่ามาตรฐาน** discard tcp d
1.1.5 2.2.2	ปิดใช้งานเซอร์วิสที่ไม่ปลอดภัยและเซอร์วิสที่ไม่จำเป็น ซึ่ง รวมถึงเซอร์วิส TCP chargen	หยุดและปิดใช้งานอินสแตนซ์ทั้งหมดของเซอร์วิส chargen(tcp) ยูทิลิตี้ AIX Security Expert ยังคอมเม้นต์รายการที่เกี่ยวข้อง ในไฟล์ /etc/inetd.conf ที่สตาร์ท เซอร์วิสโดยอัตโนมัติ	**ตำแหน่ง** /etc/security/pscexpert/bin/cominetdconf **ค่ามาตรฐาน** chargen tcp d

ตารางที่ 2. การตั้งค่าที่เกี่ยวข้องกับมาตรฐานการปฏิบัติตามข้อกำหนด PCI DSS 2.0 (ต่อ)

การปรับใช้มาตรฐาน PCI DSS เหล่านี้	ข้อมูลจำเพาะการนำไปปฏิบัติ	การปรับใช้ AIX Security Expert	ตำแหน่งของค่าและการตั้งค่าที่ จำเป็นสำหรับการปฏิบัติตาม (ถ้ามี)
1.1.5 2.2.2	ปิดใช้งานเซอร์วิสที่ไม่ปลอดภัยและเซอร์วิสที่ไม่จำเป็น ซึ่ง รวมถึงเซอร์วิส TCP daytime	หยุดและปิดใช้งานอินสแตนซ์ทั้งหมดของเซอร์วิส daytime(tcp) ยูทิลิตี้ AIX Security Expert ยังคอมเม้นต์รายการที่เกี่ยวข้องในไฟล์ /etc/inetd.conf ที่สตาร์ท เซอร์วิสโดยอัตโนมัติ	**ตำแหน่ง** /etc/security/pscexpert/bin/cominetdconf **ค่ามาตรฐาน** daytime tcp d
1.1.5 2.2.2	ปิดใช้งานเซอร์วิสที่ไม่ปลอดภัยและเซอร์วิสที่ไม่จำเป็น ซึ่ง รวมถึงเซอร์วิส TCP time	หยุดและปิดใช้งานอินสแตนซ์ทั้งหมดของเซอร์วิส timed(tcp) ยูทิลิตี้ AIX Security Expert ยังคอมเม้นต์รายการที่เกี่ยวข้องในไฟล์ /etc/inetd.conf ที่สตาร์ท เซอร์วิสโดยอัตโนมัติ	**ตำแหน่ง** /etc/security/pscexpert/bin/cominetdconf **ค่ามาตรฐาน** time tcp d
1.1.5 2.2.2	ปิดใช้งานเซอร์วิสที่ไม่ปลอดภัยและเซอร์วิสที่ไม่จำเป็น ซึ่ง รวมถึงเซอร์วิส UDP echo	หยุดและปิดใช้งานอินสแตนซ์ทั้งหมดของเซอร์วิส echo(udp) ยูทิลิตี้ AIX Security Expert ยังคอมเม้นต์รายการที่เกี่ยวข้องในไฟล์ /etc/inetd.conf ที่สตาร์ท เซอร์วิสโดยอัตโนมัติ	**ตำแหน่ง** /etc/security/pscexpert/bin/cominetdconf **ค่ามาตรฐาน** echo udp d
1.1.5 2.2.2	ปิดใช้งานเซอร์วิสที่ไม่ปลอดภัยและเซอร์วิสที่ไม่จำเป็น ซึ่ง รวมถึงเซอร์วิส UDP discard	หยุดและปิดใช้งานอินสแตนซ์ทั้งหมดของเซอร์วิส discard(udp) ยูทิลิตี้ AIX Security Expert ยังคอมเม้นต์รายการที่เกี่ยวข้องในไฟล์ /etc/inetd.conf ที่สตาร์ท เซอร์วิสโดยอัตโนมัติ	**ตำแหน่ง** /etc/security/pscexpert/bin/cominetdconf **ค่ามาตรฐาน** discard udp d
1.1.5 2.2.2	ปิดใช้งานเซอร์วิสที่ไม่ปลอดภัยและเซอร์วิสที่ไม่จำเป็น ซึ่ง รวมถึงเซอร์วิส UDP chargen	หยุดและปิดใช้งานอินสแตนซ์ทั้งหมดของเซอร์วิส chargen(udp) ยูทิลิตี้ AIX Security Expert ยังคอมเม้นต์รายการที่เกี่ยวข้องในไฟล์ /etc/inetd.conf ที่สตาร์ท เซอร์วิสโดยอัตโนมัติ	**ตำแหน่ง** /etc/security/pscexpert/bin/cominetdconf **ค่ามาตรฐาน** chargen udp d
1.1.5 2.2.2	ปิดใช้งานเซอร์วิสที่ไม่ปลอดภัยและเซอร์วิสที่ไม่จำเป็น ซึ่ง รวมถึงเซอร์วิส UDP daytime	หยุดและปิดใช้งานอินสแตนซ์ทั้งหมดของเซอร์วิส daytime(udp) ยูทิลิตี้ AIX Security Expert ยังคอมเม้นต์รายการที่เกี่ยวข้องในไฟล์ /etc/inetd.conf ที่สตาร์ท เซอร์วิสโดยอัตโนมัติ	**ตำแหน่ง** /etc/security/pscexpert/bin/cominetdconf **ค่ามาตรฐาน** daytime udp d
1.1.5 2.2.2	ปิดใช้งานเซอร์วิสที่ไม่ปลอดภัยและเซอร์วิสที่ไม่จำเป็น ซึ่ง รวมถึงเซอร์วิส UDP time	หยุดและปิดใช้งานอินสแตนซ์ทั้งหมดของเซอร์วิส timed(udp) ยูทิลิตี้ AIX Security Expert ยังคอมเม้นต์รายการที่เกี่ยวข้องในไฟล์ /etc/inetd.conf ที่สตาร์ท เซอร์วิสโดยอัตโนมัติ	**ตำแหน่ง** /etc/security/pscexpert/bin/cominetdconf **ค่ามาตรฐาน** time udp d

ตารางที่ 2. การตั้งค่าที่เกี่ยวข้องกับมาตรฐานการปฏิบัติตามข้อกำหนด PCI DSS 2.0 (ต่อ)

การปรับใช้มาตรฐาน PCI DSS เหล่านี้	ข้อมูลจำเพาะการนำไปปฏิบัติ	การปรับใช้ AIX Security Expert	ตำแหน่งของค่าและการตั้งค่าที่ จำเป็นสำหรับการปฏิบัติตาม (ถ้ามี)
1.1.5 2.2.2	ปิดใช้งานเซอร์วิสที่ไม่ปลอดภัยและเซอร์วิสที่ไม่จำเป็น ซึ่ง รวมถึงเซอร์วิส FTP	หยุดและปิดใช้งานอินสแตนซ์ทั้งหมดของ ftpd daemon ยูทิลิตี้ AIX Security Expert ยังคอมเม้นต์รายการที่เกี่ยวข้อง ในไฟล์ /etc/inetd.conf ที่สตาร์ท daemon โดยอัตโนมัติ	**ตำแหน่ง** /etc/security/pscexpert/bin/cominetdconf **ค่ามาตรฐาน** ftp tcp d
1.1.5 2.2.2	ปิดใช้งานเซอร์วิสที่ไม่ปลอดภัยและเซอร์วิสที่ไม่จำเป็น ซึ่ง รวมถึงเซอร์วิส telnet	หยุดและปิดใช้งานอินสแตนซ์ทั้งหมดของ telnetd daemon ยูทิลิตี้ AIX Security Expert ยังคอมเม้นต์รายการที่เกี่ยวข้อง ในไฟล์ /etc/inetd.conf ที่สตาร์ท daemon โดยอัตโนมัติ	**ตำแหน่ง** /etc/security/pscexpert/bin/cominetdconf **ค่ามาตรฐาน** telnet tcp d
1.1.5 2.2.2	ปิดใช้งานเซอร์วิสที่ไม่ปลอดภัยและเซอร์วิสที่ไม่จำเป็น ซึ่ง รวมถึง dtspc	หยุดและปิดใช้งานอินสแตนซ์ทั้งหมดของ dtspc daemon ยูทิลิตี้ AIX Security Expert ยังคอมเม้นต์รายการที่เกี่ยวข้องในไฟล์ /etc/inittab ที่สตาร์ท daemon โดยอัตโนมัติ เมื่อ LFT ไม่ถูกกำหนดค่าคอนฟิกไว้ และ CDE ถูกปิดใช้งานในไฟล์ /etc/inittab	**ตำแหน่ง** /etc/security/pscexpert/bin/cominetdconf **ค่ามาตรฐาน** dtspc tcp d
1.1.5 2.2.2	ปิดใช้งานเซอร์วิสที่ไม่ปลอดภัยและเซอร์วิสที่ไม่จำเป็น ซึ่ง รวมถึงเซอร์วิส ttdbserver	หยุดและปิดใช้งานอินสแตนซ์ทั้งหมดของเซอร์วิส ttdbserver ยูทิลิตี้ AIX Security Expert ยังคอมเม้นต์รายการที่เกี่ยวข้องในไฟล์ /etc/inetd.conf ที่สตาร์ท เซอร์วิสโดยอัตโนมัติ	**ตำแหน่ง** /etc/security/pscexpert/bin/cominetdconf **ค่ามาตรฐาน** ttdbserver tcp d
1.1.5 2.2.2	ปิดใช้งานเซอร์วิสที่ไม่ปลอดภัยและเซอร์วิสที่ไม่จำเป็น ซึ่ง รวมถึงเซอร์วิส cmsd	หยุดและปิดใช้งานอินสแตนซ์ทั้งหมดของเซอร์วิส cmsd ยูทิลิตี้ AIX Security Expert ยังคอมเม้นต์รายการที่เกี่ยวข้อง ในไฟล์ /etc/inetd.conf ที่สตาร์ท เซอร์วิสโดยอัตโนมัติ	**ตำแหน่ง** /etc/security/pscexpert/bin/cominetdconf **ค่ามาตรฐาน** cmsd udp d
2.2.3	กำหนดค่าคอนฟิกพารามิเตอร์การรักษาความปลอดภัยของระบบเพื่อป้องกัน ความผิดพลาด	ลบคำสั่ง Set User ID (SUID)	**ตำแหน่ง** /etc/security/pscexpert/bin/rmsuidfrmrcmds **ค่ามาตรฐาน** r
2.2.3	กำหนดค่าคอนฟิกพารามิเตอร์การรักษาความปลอดภัยของระบบเพื่อป้องกัน ความผิดพลาด	เปิดใช้ระดับการรักษาความปลอดภัยต่ำสุดสำหรับ File Permissions Manager	**ตำแหน่ง** /etc/security/pscexpert/bin/filepermgr **ค่ามาตรฐาน** l

ตารางที่ 2. การตั้งค่าที่เกี่ยวข้องกับมาตรฐานการปฏิบัติตามข้อกำหนด PCI DSS 2.0 (ต่อ)

การปรับใช้มาตรฐาน PCI DSS เหล่านี้	ข้อมูลจำเพาะการนำไปปฏิบัติ	การปรับใช้ AIX Security Expert	ตำแหน่งของค่าและการตั้งค่าที่ จำเป็นสำหรับการปฏิบัติตาม (ถ้ามี)
2.2.3	กำหนดค่าคอนฟิกพารามิเตอร์การรักษาความปลอดภัยของระบบเพื่อป้องกัน ความผิดพลาด	เปิดใช้พารามิเตอร์การรักษาความปลอดภัยที่ระบุโดยโปรโตคอล Network File System	**ตำแหน่ง** `/etc/security/pscexpert/bin/nfsconfig` **ค่ามาตรฐาน** `e`
2.2.2	เปิดใช้เฉพาะเซอร์วิสการรักษาความปลอดภัย และเซอร์วิสที่จำเป็น, โปรโตคอล, daemons และอื่นๆ ตามที่จำเป็นสำหรับการทำงานที่ถูกต้องของระบบ ปรับใช้คุณลักษณะการรักษาความปลอดภัยสำหรับเซอร์วิสที่จำเป็น โปรโตคอล หรือ daemons ที่ถือว่าไม่ปลอดภัย	ปิดใช้งาน `rlogind`, `rshd` และ `tftpd` daemons ซึ่งไม่ ปลอดภัย	**ตำแหน่ง** `/etc/security/pscexpert/bin/disrmtdmns` **ค่ามาตรฐาน** `d`
2.2.2	เปิดใช้เฉพาะเซอร์วิสการรักษาความปลอดภัย และเซอร์วิสที่จำเป็น, โปรโตคอล, daemons และอื่นๆ ตามที่จำเป็นสำหรับการทำงานที่ถูกต้องของระบบ ปรับใช้คุณลักษณะการรักษาความปลอดภัยสำหรับเซอร์วิสที่จำเป็น โปรโตคอล หรือ daemons ที่ถือว่าไม่ปลอดภัย	ปิดใช้งาน `rlogind`, `rshd` และ `tftpd` daemons ซึ่งไม่ ปลอดภัย	**ตำแหน่ง** `/etc/security/pscexpert/bin/rmrhostsnetrc` **ค่ามาตรฐาน** `h`
2.2.2	เปิดใช้เฉพาะเซอร์วิสการรักษาความปลอดภัย และเซอร์วิสที่จำเป็น, โปรโตคอล, daemons และอื่นๆ ตามที่จำเป็นสำหรับการทำงานที่ถูกต้องของระบบ ปรับใช้คุณลักษณะการรักษาความปลอดภัยสำหรับเซอร์วิสที่จำเป็น โปรโตคอล หรือ daemons ที่ถือว่าไม่ปลอดภัย	ปิดใช้งาน `logind`, `rshd` และ `tftpdpci_rmetchostsequiv` daemons, ซึ่งไม่ปลอดภัย	**ตำแหน่ง** `/etc/security/pscexpert/bin/rmetchostsequiv` **ค่ามาตรฐาน** ไม่ต้องมีค่ามาตรฐาน
1.3.6	ใช้การตรวจสอบสถานะสัมพันธ์หรือการกรองแพ็กเกจ ซึ่งมีเฉพาะการเชื่อมต่อที่สร้างขึ้นที่ได้รับอนุญาตบนเครือข่าย	เปิดใช้อ็อพชัน `clean_partial_conns` บนเครือข่ายโดยการตั้งค่าเป็น 1	**ตำแหน่ง** `/etc/security/pscexpert/bin/ntwkopts` **ค่ามาตรฐาน** clean_partial_conns=1 s
1.3.6	ใช้การตรวจสอบสถานะสัมพันธ์หรือการกรองแพ็กเกจ ซึ่งมีเฉพาะการเชื่อมต่อที่สร้างขึ้นที่ได้รับอนุญาตบนเครือข่าย	เปิดใช้การรักษาความปลอดภัย TCP โดยการตั้งค่าอ็อพชัน `tcp_tcpsecure` บนเครือข่ายให้มีค่าเท่ากับ 7 การตั้งค่านี้จะ ช่วยป้องกันการโจมตีข้อมูล, รีเซ็ต (RST), และคำขอการเชื่อมต่อ TCP (SYN)	**ตำแหน่ง** `/etc/security/pscexpert/bin/ntwkopts` **ค่ามาตรฐาน** tcp_tcpsecure=7 s

ตารางที่ 2. การตั้งค่าที่เกี่ยวข้องกับมาตรฐานการปฏิบัติตามข้อกำหนด PCI DSS 2.0 (ต่อ)

การปรับใช้มาตรฐาน PCI DSS เหล่านี้	ข้อมูลจำเพาะการนำไปปฏิบัติ	การปรับใช้ AIX Security Expert	ตำแหน่งของค่าและการตั้งค่าที่ จำเป็นสำหรับการปฏิบัติตาม (ถ้ามี)
	ปกป้องการเข้าถึงที่ไม่ได้รับอนุญาตไปยังพอร์ตที่ไม่ได้ใช้งาน	ตั้งค่าระบบเพื่อหลบหลีกโฮสต์เป็นเวลา 5 นาที เพื่อป้องกันระบบอื่นๆ ไม่ให้เข้าถึงพอร์ตที่ไม่ได้ใช้งาน	**ตำแหน่ง** `/etc/security/pscexpert/bin/ipsecshunhosthls` **ค่ามาตรฐาน** ไม่ต้องมีค่ามาตรฐาน
	ปกป้องโฮสต์จากการสแกนพอร์ต	ตั้งค่าระบบเพื่อหลบหลีกพอร์ตที่มีช่องโหว่ เป็นเวลา 5 นาที ซึ่งจะป้องกันการสแกนพอร์ต	**ตำแหน่ง** `/etc/security/pscexpert/bin/ipsecshunports` **ค่ามาตรฐาน** ไม่ต้องมีค่ามาตรฐาน
	จำกัดสิทธิ์การสร้างอ็อบเจ็กต์	ตั้งค่าสิทธิ์การสร้างอ็อบเจ็กต์ดีฟอลต์เป็น 22	**ตำแหน่ง** `/etc/security/pscexpert/bin/chusrattr` **ค่ามาตรฐาน** umask=22
	จำกัดการเข้าถึงระบบ	ให้มีเฉพาะ ID รูทที่แสดงในไฟล์ `cron.allow` และลบไฟล์ `cron.deny` ออกจากระบบ	**ตำแหน่ง** `/etc/security/pscexpert/bin/limitsysacc` **ค่ามาตรฐาน** `h`
	ลบจุดออกจากพาธรูท	ลบจุดออกจากตัวแปรสภาพแวดล้อม PATH ในไฟล์ต่อไปนี้ที่อยู่ในโฮมไดเร็กทอรีรูท: • .cshrc • .kshrc • .login • .profile	**ตำแหน่ง** `/etc/security/pscexpert/bin/rmdotfrmpathroot` **ค่ามาตรฐาน** ไม่ต้องมีค่ามาตรฐาน
	ลบจุดออกจากพาธที่ไม่ใช่รูท	ลบจุดออกจากตัวแปรสภาพแวดล้อม *PATH* ในไฟล์ต่อไปนี้ที่อยู่ในโฮมไดเร็กทอรี ของผู้ใช้: • .cshrc • .kshrc • .login • .profile	**ตำแหน่ง** `/etc/security/pscexpert/bin/rmdotfrmpathnroot` **ค่ามาตรฐาน** ไม่ต้องมีค่ามาตรฐาน
	จำกัดการเข้าถึงระบบ	เพิ่มความสามารถของผู้ใช้รูทและชื่อผู้ใช้ในไฟล์ `/etc/ftpusers`	**ตำแหน่ง** `/etc/security/pscexpert/bin/chetcftpusers` **ค่ามาตรฐาน** `a`

ตารางที่ 2. การตั้งค่าที่เกี่ยวข้องกับมาตรฐานการปฏิบัติตามข้อกำหนด PCI DSS 2.0 (ต่อ)

การปรับใช้มาตรฐาน PCI DSS เหล่านี้	ข้อมูลจำเพาะการนำไปปฏิบัติ	การปรับใช้ AIX Security Expert	ตำแหน่งของค่าและการตั้งค่าที่ จำเป็นสำหรับการปฏิบัติตาม (ถ้ามี)
	ลบบัญชีเกสต์	ลบบัญชีเกสต์ และไฟล์ออก	**ตำแหน่ง** `/etc/security/pscexpert/bin/execmds` **ค่ามาตรฐาน** `"rmuser guest; rm -rf /home/guest; ODMDIR=/etc/objrepos odmdelete -qloc0=/home/guest -o inventory"`
	ป้องการเรียกโปรแกรมในพื้นที่เนื้อหา	เปิดใช้คุณลักษณะปิดใช้งานการดำเนินการสแต็ก (SED)	**ตำแหน่ง** `/etc/security/pscexpert/bin/sedconfig` **ค่ามาตรฐาน** ไม่ต้องมีค่ามาตรฐาน
	ตรวจสอบให้แน่ใจว่ารหัสผ่านสำหรับรูทมีความปลอดภัย	เริ่มต้นการตรวจสอบความสมบูรณ์รหัสผ่านรูท เพื่อให้แน่ใจว่ารหัสผ่านรูทมีความปลอดภัย	**ตำแหน่ง** `/etc/security/pscexpert/bin/chuserstanza` **ค่ามาตรฐาน** `/etc/security/user dictionlist=/etc/security/aixpert/dictionary/English rootpci_rootpwdintchk`
8.5.15	จำกัดการเข้าถึงระบบโดยการตั้งค่าเวลาที่ไม่มีการทำงาน เซสชัน	ตั้งค่าจำกัดเวลาที่ไม่ทำงานเท่ากับ 15 นาที หาก เซสชันไม่ทำงานนานมากกว่า 15 นาที คุณต้องป้อนรหัสผ่านใหม่อีกครั้ง	**ตำแหน่ง** `/etc/security/pscexpert/bin/autologoff` **ค่ามาตรฐาน** `900`
	จำกัดทราฟฟิกการเข้าถึงข้อมูลผู้ถือบัตร	ตั้งค่าข้อบังคับด้านทราฟฟิกของ TCP ไปที่การตั้งค่า สูงสุด ซึ่งจะแก้ไขผลกระทบจากการโจมตี DDoS บนพอร์ต	**ตำแหน่ง** `/etc/security/pscexpert/bin/tcptr_aixpert` **ค่ามาตรฐาน** `pci`
	รักษาการเชื่อมต่อที่ปลอดภัยเมื่อโอนย้ายข้อมูล	เปิดใช้การสร้างทันเนลของ IP Security (IPSec) โดยอัตโนมัติระหว่าง Virtual I/O Servers ขณะโอนย้ายพาร์ติชันที่ใช้งานอยู่	**ตำแหน่ง** `/etc/security/pscexpert/bin/cfgsecmig` **ค่ามาตรฐาน** `on`
1.3.5	จำกัดแพ็กเกจจากแหล่งที่ไม่รู้จัก	อนุญาตแพ็กเกจจาก Hardware Management Console	**ตำแหน่ง** `/etc/security/pscexpert/bin/ipsecpermithostorport` **ค่ามาตรฐาน** ไม่ต้องมีค่ามาตรฐาน

ตารางที่ 2. การตั้งค่าที่เกี่ยวข้องกับมาตรฐานการปฏิบัติตามข้อกำหนด PCI DSS 2.0 (ต่อ)

การปรับใช้มาตรฐาน PCI DSS เหล่านี้	ข้อมูลจำเพาะการนำไปปฏิบัติ	การปรับใช้ AIX Security Expert	ตำแหน่งของค่าและการตั้งค่าที่ จำเป็นสำหรับการปฏิบัติตาม (ถ้ามี)
5.1.1	บำรุงรักษาซอฟต์แวร์ป้องกันไวรัส	บำรุงรักษาความสมบูรณ์ของระบบโดยการตรวจจับ การลบ และการป้องกันประเภทของซอฟต์แวร์ที่เป็นอันตรายที่ไม่รู้จัก	**ตำแหน่ง** `/etc/security/pscexpert/bin/manageITsecurity` **ค่ามาตรฐาน** ไม่ต้องมีค่ามาตรฐาน
	รักษาการเข้าถึงตามพื้นฐานที่จำเป็น	เปิดใช้การควบคุมการเข้าถึงตามบทบาท (RBAC) โดยการสร้างโอเปอเรเตอร์ของระบบ, ผู้ดูแลระบบ และบทบาทของผู้ใช้ที่เป็นเจ้าหน้าที่รักษาความปลอดภัยระบบข้อมูลที่มีสิทธิ์ที่จำเป็น	**ตำแหน่ง** `/etc/security/pscexpert/bin/EnableRbac` **ค่ามาตรฐาน** ไม่ต้องมีค่ามาตรฐาน

ข้อมูลที่เกี่ยวข้อง:

มาตรฐาน DSS ของ Payment card industry

ความเข้ากันได้กับ Sarbanes-Oxley Act และ COBIT

Sarbanes-Oxley (SOX) Act of 2002 ที่เป็นพื้นฐานของ 107th congress ของประเทศสหรัฐอเมริกาตรวจสอบ บริษัทมหาชนในเรื่องกฎหมายหลักทรัพย์ 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 Express Edition SOX/COBIT XML จัดให้มีการกำหนดค่าการรักษาความปลอดภัยของระบบ AIX และ Virtual I/O Server (VIOS ที่จำเป็นต้องมีเพื่อให้เป็นไปตามแนวทางความเข้ากันได้กับ COBIT

IBM Compliance Expert Express Edition รันบน AIX 7.1, AIX 6.1 และ AIX 5.3

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

 มาตรฐาน Sarbanes-Oxley (SOX)

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 ใช้กับเอนทิตีที่ครอบคลุมต่อไปนี้:

- ผู้ให้บริการด้านบริการสุขภาพ
- แผนสุขภาพ
- ศูนย์การบริการด้านสุขภาพ
- ใบสั่งยาโครงการประกันสุขภาพ และผู้สนับสนุนบัตรยา

ตารางต่อไปนี้มีรายละเอียดเกี่ยวกับหลายๆ ส่วนของ กฎการรักษาความปลอดภัย HIPAA และแต่ละส่วนได้แก่มาตรฐานหลายๆ อย่างและ ข้อมูลจำเพาะการนำไปปฏิบัติ

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

ตารางที่ 3. กฎ HIPAA และรายละเอียด การนำไปปฏิบัติ

ส่วนของกฎการรักษาความปลอดภัย HIPAA	ข้อมูลจำเพาะการนำไปปฏิบัติ	การนำไปปฏิบัติ aixpert	คำสั่ง และค่าส่งคืน
164.308 (a) (1) (ii) (D) 164.308 (a) (5) (ii) (C) 164.312 (b)	ประยุกต์ใช้โพรซีเดอร์เพื่อตรวจทานเร็กคอร์ด ทั่วไปของกิจกรรมระบบข้อมูล เช่นล็อกการตรวจสอบ รายงานการเข้าถึง และรายการการรักษาความปลอดภัยที่เกิดขึ้น	พิจารณาว่าการตรวจสอบถูกเปิดใช้งานในระบบ หรือไม่	**คำสั่ง:** **#audit query** **ค่า ส่งคืน:** ถ้าสำเร็จ คำสั่งนี้ออกโดยมีค่าเป็น 0 ถ้าไม่สำเร็จ คำสั่งออกโดยมีค่า 1

ตารางที่ 3. กฎ HIPAA และรายละเอียด การนำไปปฏิบัติ (ต่อ)

ส่วนของกฎการรักษาความปลอดภัย HIPAA	ข้อมูลจำเพาะการนำไปปฏิบัติ	การนำไปปฏิบัติ aixpert	คำสั่ง และค่าส่งคืน
164.308 (a) (1) (ii) (D) 164.308 (a) (5) (ii) (C) 166.312 (b)	ประยุกต์ใช้โพรซีเดอร์เพื่อตรวจทานเร็กคอร์ด ทั่วไปของกิจกรรมระบบข้อมูล เช่นล็อกการตรวจสอบ รายงานการเข้าถึง และรายการการรักษาความปลอดภัยที่เกิดขึ้น	เปิดใช้การตรวจสอบในระบบ รวมถึงกำหนดคอนฟิก เหตุการณ์ที่จะถูกบันทึก	**คำสั่ง:** **# audit start >/dev/null 2>&1.** **ค่าส่งคืน:** ถ้าสำเร็จ คำสั่งนี้ออกโดยมีค่าเป็น 0 ถ้าไม่สำเร็จ คำสั่ง ออกโดยมีค่า 1 เหตุการณ์ต่อไปนี้ถูกตรวจสอบ: **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**
164.312 (a) (2) (iV)	การเข้ารหัสและการถอดรหัส (A):ประยุกต์ใช้ กลไกเพื่อเข้ารหัส และถอดรหัส EPHI	พิจารณาว่า encrypted file system (EFS) ถูกเปิดใช้งานบนระบบหรือไม่	**คำสั่ง:** **# efskeymgr -V >/dev/null 2>&1.** **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:** **grep TMOUT= /etc/security /.profile > /dev/null 2>&1** **echo "TMOUT=900 ; TIMEOUT=900; export TMOUT TIMEOUT.** **ค่า ส่งคืน:** ถ้าคำสั่งไม่พบค่า **TMOUT=15** และสคริปต์ออกโดยมีค่า 1 มิฉะนั้นคำสั่งจะออกโดยมี ค่าเป็น 0
164.308 (a) (5) (ii) (D) 164.312 (a) (2) (i)	การจัดการรหัสผ่าน (A) :ประยุกต์ใช้ กระบวนการสำหรับการสร้าง การเปลี่ยนแปลง และการป้องกันรหัสผ่าน	ให้แน่ใจว่ารหัสผ่านทั้งหมดที่นั้นยาว 14 อักขระ	**คำสั่ง:** **chsec -f /etc/security/user -s user -a minlen=8** **ค่า ส่งคืน:** ถ้าสำเร็จ สคริปต์นี้ออกโดยมีค่าเป็น 0 ถ้าไม่สำเร็จ สคริปต์ออกโดยมีโค้ดระบุความผิดพลาดเป็น 1
164.308 (a) (5) (ii) (D) 164.312 (a) (2) (i)	การจัดการรหัสผ่าน (A) :ประยุกต์ใช้ กระบวนการสำหรับการสร้าง การเปลี่ยนแปลง และการป้องกันรหัสผ่าน	ให้แน่ใจว่ารหัสผ่านทั้งหมดประกอบด้วยอักขระแบบตัวอักษรอย่างน้อยสองตัวอักษร หนึ่งในนั้นต้อเป็นตัวพิมพ์ใหญ่	**คำสั่ง:** **chsec -f /etc/security/user -s user -a minalpha=4** **ค่า ส่งคืน:** ถ้าสำเร็จ สคริปต์นี้ออกโดยมีค่าเป็น 0 ถ้าไม่สำเร็จ คำสั่งออกโดยมีโค้ดระบุความผิดพลาดเป็น 1

ตารางที่ 3. กฎ HIPAA และรายละเอียด การนำไปปฏิบัติ (ต่อ)

ส่วนของกฎการรักษาความปลอดภัย HIPAA	ข้อมูลจำเพาะการนำไปปฏิบัติ	การนำไปปฏิบัติ aixpert	คำสั่ง และค่าส่งคืน
164.308 (a) (5) (ii) (D) 164.312 (a) (2) (i)	การจัดการรหัสผ่าน (A) :ประยุกต์ใช้ กระบวนการสำหรับการสร้าง การเปลี่ยนแปลง และการป้องกันรหัสผ่าน	ระบุจำนวนอักขระที่ไม่ใช่ตัวอักษรผสมตัวเลขขั้นต่ำ 2 ตัว	**คำสั่ง:** **#chsec –f /etc/security/user –s user –a minother=2** **ค่า ส่งคืน:** ถ้าสำเร็จ สคริปต์นี้ออกโดยมีค่าเป็น 0 ถ้าไม่สำเร็จ คำสั่งออกโดยมีโค้ดระบุความผิดพลาดเป็น 1
164.308 (a) (5) (ii) (D) 164.312 (a) (2) (i)	การจัดการรหัสผ่าน (A) :ประยุกต์ใช้ กระบวนการสำหรับการสร้าง การเปลี่ยนแปลง และการป้องกันรหัสผ่าน	ให้แน่ใจว่ารหัสผ่านทั้งหมดไม่มีอักขระ ซ้ำกัน	**คำสั่ง:** **#chsec –f /etc/security/user –s user –a maxrepeats=1** **ค่า ส่งคืน:** ถ้าสำเร็จ สคริปต์นี้ออกโดยมีค่าเป็น 0 ถ้าไม่สำเร็จ คำสั่งออกโดยมีโค้ดระบุความผิดพลาดเป็น 1
164.308 (a) (5) (ii) (D) 164.312 (a) (2) (i)	การจัดการรหัสผ่าน (A) :ประยุกต์ใช้ กระบวนการสำหรับการสร้าง การเปลี่ยนแปลง และการป้องกันรหัสผ่าน	ให้แน่ใจว่ารหัสผ่านไม่ถูกนำมาใช้ซ้ำภายใน การเปลี่ยนแปลงอย่างน้อยห้าครั้ง	**คำสั่ง:** **#chsec –f /etc/security/user –s user –a histsize=5** **ค่า ส่งคืน:** ถ้าสำเร็จ สคริปต์นี้ออกโดยมีค่าเป็น 0 ถ้าไม่สำเร็จ คำสั่งออกโดยมีโค้ดระบุความผิดพลาดเป็น 1
164.308 (a) (5) (ii) (D) 164.312 (a) (2) (i)	การจัดการรหัสผ่าน (A) :ประยุกต์ใช้ กระบวนการสำหรับการสร้าง การเปลี่ยนแปลง และการป้องกันรหัสผ่าน	ระบุจำนวนสัปดาห์สูงสุดถือ 13 สัปดาห์ เพื่อที่รหัสผ่านจะยังคงถูกต้อง	**คำสั่ง:** **#chsec –f /etc/security/user –s user –a maxage=8** **ค่า ส่งคืน:** ถ้าสำเร็จ สคริปต์นี้ออกโดยมีค่าเป็น 0 ถ้าไม่สำเร็จ คำสั่งออกโดยมีโค้ดระบุความผิดพลาดเป็น 1
164.308 (a) (5) (ii) (D) 164.312 (a) (2) (i)	การจัดการรหัสผ่าน (A) :ประยุกต์ใช้ กระบวนการสำหรับการสร้าง การเปลี่ยนแปลง และการป้องกันรหัสผ่าน	นำจำนวนต่ำสุดของข้อกำหนดจำนวนสัปดาห์ ก่อนที่รหัสผ่านจะสามารถเปลี่ยนการเปลี่ยนแปลง	**คำสั่ง:** **#chsec –f /etc/security/user –s user –a minage=2** **ค่า ส่งคืน:** ถ้าสำเร็จ สคริปต์นี้ออกโดยมีค่าเป็น 0 ถ้าไม่สำเร็จ คำสั่งออกโดยมีโค้ดระบุความผิดพลาดเป็น 1
164.308 (a) (5) (ii) (D) 164.312 (a) (2) (i)	การจัดการรหัสผ่าน (A) :ประยุกต์ใช้ กระบวนการสำหรับการสร้าง การเปลี่ยนแปลง และการป้องกันรหัสผ่าน	ระบุจำนวนสัปดาห์สูงสุดเป็น 4 สัปดาห์ เพื่อเปลี่ยนแปลงรหัสผ่านที่หมดอายุ หลังจากค่าของพารามิเตอร์ **maxage** ถูกตั้งค่าโดยผู้ใช้ที่หมดอายุ	**คำสั่ง:** **#chsec –f /etc/security/user –s user –a maxexpired=4** **ค่า ส่งคืน:** ถ้าสำเร็จ สคริปต์นี้ออกโดยมีค่าเป็น 0 ถ้าไม่สำเร็จ คำสั่งออกโดยมีโค้ดระบุความผิดพลาดเป็น 1

ตารางที่ 3. กฎ HIPAA และรายละเอียด การนำไปปฏิบัติ (ต่อ)

ส่วนของกฎการรักษาความปลอดภัย HIPAA	ข้อมูลจำเพาะการนำไปปฏิบัติ	การนำไปปฏิบัติ aixpert	คำสั่ง และค่าส่งคืน
164.308 (a) (5) (ii) (D) 164.312 (a) (2) (i)	การจัดการรหัสผ่าน (A) :ประยุกต์ใช้ กระบวนการสำหรับการสร้าง การเปลี่ยนแปลง และการป้องกันรหัสผ่าน	ระบุจำนวนอักขระขั้นต่ำที่ไม่สามารถมีซ้ำจากรหัสผ่านคือ 4 อักขระ	**คำสั่ง:** **#chsec −f /etc/security/user −s user −a mindiff=4** **ค่า ส่งคืน:** ถ้าสำเร็จ สคริปต์นี้ออกโดยมีค่าเป็น 0 ถ้าไม่สำเร็จ คำสั่งออกโดยมีโค้ดระบุความผิดพลาดเป็น 1
164.308 (a) (5) (ii) (D) 164.312 (a) (2) (i)	การจัดการรหัสผ่าน (A) :ประยุกต์ใช้ กระบวนการสำหรับการสร้าง การเปลี่ยนแปลง และการป้องกันรหัสผ่าน	ระบุว่าจำนวนวันคือ 5 เพื่อรอ ก่อนที่ระบบจะออกคำเตือนว่าจำเป็นต้องมีการเปลี่ยนแปลงรหัสผ่าน	**คำสั่ง:** **#chsec −f /etc/security/user −s user −a pwdwarntime = 5** **ค่า ส่งคืน:** ถ้าสำเร็จ สคริปต์นี้ออกโดยมีค่าเป็น 0 ถ้าไม่สำเร็จ คำสั่งออกโดยมีโค้ดระบุความผิดพลาดเป็น 1
164.308 (a) (5) (ii) (D) 164.312 (a) (2) (i)	การจัดการรหัสผ่าน (A) :ประยุกต์ใช้ กระบวนการสำหรับการสร้าง การเปลี่ยนแปลง และการป้องกันรหัสผ่าน	ตรวจสอบความถูกต้องของนิยามผู้ใช้ และแก้ไขข้อผิดพลาด	**คำสั่ง:** **/usr/bin/usrck −y ALL** **/usr/bin/usrck −n ALL.** **ค่า ส่งคืน:** คำสั่งไม่ส่งคืนค่า คำสั่งตรวจสอบ และแก้ไขข้อผิดพลาดถ้ามี
164.308 (a) (5) (ii) (D) 164.312 (a) (2) (i)	การจัดการรหัสผ่าน (A) :ประยุกต์ใช้ กระบวนการสำหรับการสร้าง การเปลี่ยนแปลง และการป้องกันรหัสผ่าน	ล็อกแอคเคาต์หลังจากพยายามล็อกอินแล้วล้มเหลว ติดต่อกันสามครั้ง	**คำสั่ง:** **#chsec −f /etc/security/user −s user −a loginretries=3** **ค่า ส่งคืน:** ถ้าสำเร็จ สคริปต์นี้ออกโดยมีค่าเป็น 0 ถ้าไม่สำเร็จ คำสั่งออกโดยมีโค้ดระบุความผิดพลาดเป็น 1
164.308 (a) (5) (ii) (D) 164.312 (a) (2) (i)	การจัดการรหัสผ่าน (A) :ประยุกต์ใช้ กระบวนการสำหรับการสร้าง การเปลี่ยนแปลง และการป้องกันรหัสผ่าน	ระบุการหน่วงเวลาระหว่างการล็อกอิน ที่ไม่สำเร็จหนึ่งครั้งกับการล็อกอินอื่นๆ เป็น 5 วินาที	**คำสั่ง:** **chsec −f /etc/security/login.cfg −s default −a logindelay=5** **ค่า ส่งคืน:** ถ้าสำเร็จ สคริปต์นี้ออกโดยมีค่าเป็น 0 ถ้าไม่สำเร็จ คำสั่งออกโดยมีโค้ดระบุความผิดพลาดเป็น 1
164.308 (a) (5) (ii) (D) 164.312 (a) (2) (i)	การจัดการรหัสผ่าน (A) :ประยุกต์ใช้ กระบวนการสำหรับการสร้าง การเปลี่ยนแปลง และการป้องกันรหัสผ่าน	ระบุจำนวนครั้งที่พยายามล็อกอินแล้วไม่สำเร็จ บนพอร์ต ก่อนที่พอร์ตถูกล็อกเป็น 10	**คำสั่ง:** **chsec −f /etc/security/lastlog −s username −a \ unsuccessful_login_count=10** **ค่า ส่งคืน:** ถ้าสำเร็จ สคริปต์นี้ออกโดยมีค่าเป็น 0 ถ้าไม่สำเร็จ คำสั่งออกโดยมีโค้ดระบุความผิดพลาดเป็น 1

ตารางที่ 3. กฎ HIPAA และรายละเอียด การนำไปปฏิบัติ (ต่อ)

ส่วนของกฎการรักษาความปลอดภัย HIPAA	ข้อมูลจำเพาะการนำไปปฏิบัติ	การนำไปปฏิบัติ aixpert	คำสั่ง และค่าส่งคืน
164.308 (a) (5) (ii) (D) 164.312 (a) (2) (i)	การจัดการรหัสผ่าน (A) :ประยุกต์ใช้ กระบวนการสำหรับการสร้าง การเปลี่ยนแปลง และการป้องกันรหัสผ่าน	ระบุช่วงเวลาในพอร์ตสำหรับความพยายามล็อกอินที่ไม่สำเร็จก่อนพอร์ตถูกปิดใช้งานเป็น 60 วินาที	**คำสั่ง:** **#chsec -f /etc/security/lastlog -s user -a time_last_unsuccessful_login=60** **ค่า ส่งคืน:** ถ้าสำเร็จ สคริปต์นี้ออกโดยมีค่าเป็น 0 ถ้าไม่สำเร็จ คำสั่งออกโดยมีโค้ดระบุความผิดพลาดเป็น 1
164.308 (a) (5) (ii) (D) 164.312 (a) (2) (i)	การจัดการรหัสผ่าน (A) :ประยุกต์ใช้ กระบวนการสำหรับการสร้าง การเปลี่ยนแปลง และการป้องกันรหัสผ่าน	ระบุช่วงเวลาหลังจากพอร์ต ถูกล็อก และหลังจากถูกปิดใช้งาน เป็น 30 นาที	**คำสั่ง:** **#chsec -f /etc/security/login.cfg -s default -a loginreenable = 30** **ค่า ส่งคืน:** ถ้าสำเร็จ สคริปต์นี้ออกโดยมีค่าเป็น 0 ถ้าไม่สำเร็จ คำสั่งออกโดยมีโค้ดระบุความผิดพลาดเป็น 1
164.308 (a) (5) (ii) (D) 164.312 (a) (2) (i)	การจัดการรหัสผ่าน (A) :ประยุกต์ใช้ กระบวนการสำหรับการสร้าง การเปลี่ยนแปลง และการป้องกันรหัสผ่าน	ระบุช่วงเวลาเพื่อพิมพ์รหัสผ่านเป็น 30 วินาที	**คำสั่ง:** **chsec -f /etc/security/login.cfg -s usw -a logintimeout=30** **ค่า ส่งคืน:** ถ้าสำเร็จ สคริปต์นี้ออกโดยมีค่าเป็น 0 ถ้าไม่สำเร็จ คำสั่งออกโดยมีโค้ดระบุความผิดพลาดเป็น 1
164.308 (a) (5) (ii) (D) 164.312 (a) (2) (i)	การจัดการรหัสผ่าน (A) :ประยุกต์ใช้ กระบวนการสำหรับการสร้าง การเปลี่ยนแปลง และการป้องกันรหัสผ่าน	ให้แน่ใจว่าแอคเคาต์ถูกล็อกหลังไม่ได้ใช้งาน 35 วัน	**คำสั่ง:** **grep TMOUT= /etc/security /.profile > /dev/null 2>&1if TMOUT = (35x24x60x60){#chsec -f /etc/security/user -s user -aaccount_locked = true}** **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:** เปิด **CHKEXEC, CHKSHLIB, CHKSCRIPT, CHKKERNEXT, STOP_ON_CHKFAIL,TE=ON** **ตัวอย่างเช่น trustchk -p TE=ON CHKEXEC = ON, CHKSHLIB,=ON, CHKSCRIPT=ON, CHKKERNEXT = ON** **ค่าส่งคืน:** เมื่อล้มเหลว สคริปต์ ออกโดยมีค่าเป็น 1
164.312 (e) (1)	ประยุกต์ใช้การวัดการรักษาความปลอดภัยด้านเทคนิคเพื่อป้องกันการเข้าถึงที่ไม่ได้รับอนุญาตใน EPHI ที่กำลังถูกส่งผ่านเครือข่ายการสื่อสารอิเล็กทรอนิกส์	พิจารณาว่า **ssh** filesets ถูก ติดตั้งหรือไม่ ถ้าไม่ ให้แสดงข้อความแสดงข้อผิดพลาด	**คำสั่ง:** **# lslpp -l | grep openssh > /dev/null 2>&1** **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 4. ฟังก์ชัน HIPAA และรายละเอียด การนำไปปฏิบัติ

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

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
```

ในตัวอย่างนี้ไม่มีกฎที่ล้มเหลว 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` และค้นหากฎทมี่ล้มเหลว 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` โดยการลบกฎที่เข้ากันไม่ได้จากแท็ก XML ที่เปิด `<AIXPertEntry name...` ไปยังแท็ก XML สิ้นสุด `</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:

```
aixpert -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) อยู่ ในไดเร็กทอรี `/etc/security/aixpert/core`

การกำหนดคอนฟิกความเข้ากันได้ PowerSC จากบรรทัดรับคำสั่ง

ประยุกต์ใช้หรือตรวจสอบโฟรไฟล์ความเข้ากันได้โดยใช้คำสั่ง **aixpert** บนระบบ AIX และคำสั่ง **viosecure** บน Virtual I/O Server (VIOS)

เพื่อปรับใช้โปรไฟล์ความเข้ากันได้ PowerSC บนระบบ AIX ให้ป้อนหนึ่งในคำสั่งต่อไปนี้ ซึ่งจะขึ้นอยู่กับ ระดับมาตรฐานความปลอดภัยที่คุณต้องการปรับใช้

ตารางที่ 5. คำสั่ง PowerSC สำหรับ AIX

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

เมื่อต้องการใช้โปรไฟล์ความเข้ากันได้ PowerSC บนระบบ VIOS ป้อนหนึ่งในคำสั่งต่อไปนี้สำหรับระดับความเข้ากันได้ของการรักษาความปลอดภัย ที่คุณต้องการใช้

ตารางที่ 6. 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/PCI.xml	*มาตรฐานความปลอดภัยข้อมูลของ Payment card industry*
% viosecure -file /etc/security/aixpert/custom/SOX-COBIT.xml	*Sarbanes-Oxley Act ประจำปี 2002 – COBIT IT Governance*

คำสั่ง **aixpert** บนระบบ AIX และคำสั่ง **viosecure** ใน VIOS อาจ ใช้เวลาเพื่อรันเนื่องจากกำลังตรวจสอบ หรือตั้งค่าทั้งระบบ และทำการเปลี่ยนแปลงการกำหนดคอนฟิกที่เกี่ยวกับการรักษาความปลอดภัย 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 24
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

สำหรับการนำไปใช้ที่สำเร็จสำหรับ DoD, PCI หรือ SOX, PowerSC Express Edition หรือ PowerSC Standard Edition ต้องติดตั้งไว้ที่จุดปลายของระบบ AIX ถ้าระบบที่กำลังถูกปรับใช้ไม่มี PowerSC ติดตั้งอยู่ การปรับใช้จะล้มเหลว IBM Systems Director นำเท็มเพลตคอนฟิกูเรชัน ไปใช้กับจุดปลายของระบบ 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 ถูกติดตั้งกับ PowerSC Express Edition และไม่ใช่ ส่วนหนึ่งของระบบปฏิบัติการ AIX พื้นฐาน

เมื่อต้องการติดตั้ง PowerSC Express Edition ซึ่งรวม PowerSC Real Time Compliance ดำเนิน ขั้นตอนต่อไปนี้:

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
2. ถ้าคุณติดตั้ง PowerSC Express Edition เวอร์ชัน 1.1.2.0 หรือใหม่กว่าไว้แล้ว คุณสามารถเพิ่มไฟล์ที่ต้องการสำหรับคุณลักษณะ PowerSC Real Time Compliance โดยการติดตั้ง PowerSC Express Edition อีกครั้ง หรือโดยการอัพเดต เวอร์ชันที่ติดตั้งของคุณลักษณะ PowerSC Real Time Compliance เป็นเวอร์ชันล่าสุด
3. เมื่อต้องการอัพเดต fileset คุณลักษณะ PowerSC Real Time Compliance ให้ติดตั้ง `powerscExp.rtc` fileset จาก แพ็กเกจการติดตั้งสำหรับ PowerSC Express Edition เวอร์ชัน 1.1.2.0 หรือใหม่กว่า
4. สำหรับการติดตั้งใหม่ของ PowerSC Express Edition เวอร์ชัน 1.1.2.0 หรือก่อนหน้า ให้ปฏิบัติตามคำแนะนำใน การติดตั้ง PowerSC Express Edition เวอร์ชัน 1.1.2 หรือ ก่อนหน้า

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 เมธอดหนึ่งคือใช้คำสั่ง **aixpert** และอีกเมธอดหนึ่งคือ 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` คุณสามารถแก้ไขไฟล์นี้เพื่ออัพเดตข้อมูล โดยใช้ เอดิเตอร์ข้อความ

สำหรับข้อมูลเพิ่มเติมเกี่ยวกับอ็อพชันและวิธีแก้ไขไฟล์นี้ ดูข้อมูลเกี่ยวกับไฟล์ rtcd.conf

ข้อมูลที่เกี่ยวข้อง:

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

คำสั่ง PowerSC Express Edition

คำสั่งที่สามารถใช้ได้กับ PowerSC Express Edition จะมี วิธีการในการเปลี่ยนแปลงการตั้งค่า Compliance โดยการใช้บรรทัดคำสั่ง

คำสั่ง pscxpert

วัตถุประสงค์

ช่วยผู้ดูแลระบบใน การตั้งค่าการกำหนดค่าคอนฟิกการรักษาความปลอดภัย

ไวยากรณ์

pscxpert

pscxpert -l h|high | m|medium | l|low | d|default [-p] [-n -o *filename*] [**-a -o** *filename*]

pscxpert -c [-P *filename*] [**-r**] [**-R**] [**-l h|high | m|medium | l|low | d|default**] [**-p**]

pscxpert -u [**-p**]

pscxpert -d

pscxpert [**-f** *profile_name*]

pscxpert [**-f** *profile_name*] [**-a -o** *filename*] [**-p**]

pscxpert -t

คำอธิบาย

pscxpert คือชุดคำสั่งต่างๆ ของการตั้งค่าคอนฟิกูเรชันของระบบ เพื่อเปิดใช้ระดับการรักษาความปลอดภัยที่ต้องการ

การรันคำสั่ง **pscxpert** ที่มีเฉพาะชุดแฟล็ก **-l** จะใช้การตั้งค่าการรักษาความปลอดภัยโดย ไม่อนุญาตให้ผู้ใช้กำหนดค่าคอนฟิกการตั้งค่า ตัวอย่างเช่น การรัน คำสั่ง **pscxpert -l high** จะใช้การตั้งค่า การรักษาความปลอดภัยระดับสูงทั้งหมดกับระบบโดยอัตโนมัติ อย่างไรก็ตาม การรันคำสั่ง **pscxpert -l** ที่มีอ็อพชัน **-n** และ **-o** *filename* จะบันทึกการตั้งค่าการรักษาความปลอดภัยไปยังไฟล์ ที่ระบุโดยพารามิเตอร์ *filename* แฟล็ก **-f** จะใช้การกำหนดค่าคอนฟิกใหม่

หลังจากการเลือกขั้นต้น เมนูจะแสดงรายการอ็อพชัน การกำหนดค่าคอนฟิกการรักษาความปลอดภัยทั้งหมดที่เกี่ยวข้องกับระดับการรักษาความปลอดภัย ที่เลือกไว้ สามารถยอมรับอ็อพชันเหล่านี้ทั้งหมดหรือสลับเปิดหรือปิด แต่ละรายการ หลังจากการเปลี่ยนแปลงครั้งที่สอง คำสั่ง **pscxpert** จะยังคงใช้การตั้งค่าการรักษาความปลอดภัยกับ ระบบคอมพิวเตอร์

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

แฟล็ก

รายการ	คำอธิบาย
-a	การตั้งค่าที่มีอ็อพชันของระดับการรักษาความปลอดภัย ที่เกี่ยวข้องจะถูกเขียนไปยังไฟล์ที่ระบุโดยแฟล็ก **-o** ในรูปแบบตัวย่อ คุณต้องระบุอ็อพชัน **-o** เมื่อคุณระบุอ็อพชัน **-a**
-c	ตรวจสอบการตั้งค่าการรักษาความปลอดภัยกับชุดของกฎ ที่ปรับใช้ก่อนหน้านี้ หากการตรวจสอบกฎล้มเหลว เวอร์ชันก่อนหน้า ของกฎจะถูกตรวจสอบ กระบวนการนี้จะดำเนินการต่อจนกว่า การตรวจสอบจะผ่านหรือจนกว่าอินสแตนซ์ทั้งหมดของกฎที่ล้มหลว ในไฟล์ **/etc/security/aixpert/core/appliedaixpert.xml** จะถูกตรวจสอบ
-d	แสดงนิยามของชนิดเอกสาร (DTD)

รายการ	คำอธิบาย
-f	ใช้การตั้งค่าการรักษาความปลอดภัย ที่ระบุในไฟล์ *profile_name* เฉพาะ โปรไฟล์จะอยู่ในไดเร็กทอรี `/etc/security/aixpert/custom`โปรไฟล์ที่มีจะมีโปรไฟล์มาตรฐาน ต่อไปนี้: **DataBase.xml** ไฟล์นี้จะมีข้อกำหนดสำหรับการตั้งค่าฐานข้อมูลดีฟอลต์ **DoD.xml** ไฟล์นี้จะมีข้อกำหนดสำหรับการตั้งค่า Department of Defense Security Technical Implementation Guide (STIG) **DoD_to_AIXDefault.xml** ไฟล์นี้จะเปลี่ยนแปลงการตั้งค่าเป็นการตั้งค่า AIX ดีฟอลต์ **Hipaa.xml** ไฟล์นี้จะมีข้อกำหนดสำหรับการตั้งค่า Health Insurance Portability and Accountability Act (HIPAA) **PCI.xml** ไฟล์นี้จะมีข้อกำหนดสำหรับการตั้งค่า Payment card industry Data Security Standard **PCI_to_AIXDefault.xml** ไฟล์นี้จะเปลี่ยนแปลงการตั้งค่าเป็นการตั้งค่า AIX ดีฟลอต์ **SCBPS.xml** ไฟล์นี้จะมีข้อกำหนดสำหรับการตั้งค่า Sarbanes-Oxley Act and COBIT คุณยังสามารถสร้างโปรไฟล์ที่กำหนดเองในไดเร็กทอรี เดียวกัน และใช้กับการตั้งค่าของคุณโดยการเปลี่ยนชื่อและแก้ไข ไฟล์ XML ที่มีอยู่ ตัวอย่างเช่น คำสั่งต่อไปนี้จะปรับใช้โปรไฟล์ HIPAA กับระบบของคุณ: `pscxpert -f /etc/security/aixpert/custom/Hipaa.xml` เมื่อคุณระบุอ็อพชัน **-f** การตั้งค่าการรักษาความปลอดภัย จะถูกปรับใช้อย่างต่อเนื่องจากระบบหนึ่งไปยังอีกระบบหนึ่ง โดยการถ่ายโอนอย่างปลอดภัย และปรับใช้ไฟล์ **appliedaixpert.xml** จากระบบหนึ่งไปยังอีกระบบหนึ่ง กฎที่ปรับใช้สำเร็จทั้งหมดจะถูกเขียนไปยังไฟล์ **/etc/security/aixpert/core/appliedaixpert.xml** และกฎการดำเนินการ `undo` ที่เกี่ยวข้อง จะถูกเขียนไปยังไฟล์ **/etc/security/aixpert/core/undo.xml**
-l	กำหนดการตั้งค่าการรักษาความปลอดภัยระบบไปยังระดับ ที่ระบุ แฟล็กนี้จะมีอ็อพชันต่อไปนี้: **h|high** ระบุอ็อพชันการรักษาความปลอดภัยระดับสูง **m|medium** ระบุอ็อพชันการรักษาความปลอดภัยระดับปานกลาง **l|low** ระบุอ็อพชันการรักษาความปลอดภัยระดับล่าง **d|default** ระบุอ็อพชันการรักษาความปลอดภัยระดับมาตรฐาน AIX หากคุณระบุทั้งแฟล็ก **-l** และ **-n** การตั้งค่าการรักษาความปลอดภัยจะไม่ถูกใช้บนระบบ อย่างไรก็ตาม จะถูกเขียนไปยังไฟล์ที่คุณระบุในแฟล็ก **-o** เท่านั้น กฎที่ปรับใช้สำเร็จทั้งหมดจะถูกเขียนไปยังไฟล์ **/etc/security/aixpert/core/appliedaixpert.xml** และกฎการดำเนินการที่สอดคล้องกัน จะถูกเขียนไปยังไฟล์ **/etc/security/aixpert/core/undo.xml** **ข้อควรสนใจ:** เมื่อคุณใช้อ็อพชัน **d|default** สาอ็อพชันสามารถเขียนทับการตั้งค่าการรักษาความปลอดภัยที่กำหนดค่าคอนฟิกไว้ ที่คุณได้กำหนดค่าไว้ก่อนหน้านี้โดยการใช้คำสั่ง **pscxpert** หรือ ด้วยตัวเอง และคืนค่าระบบไปยังการกำหนดค่าคอนฟิกที่เปิดแบบดั้งเดิม

รายการ	คำอธิบาย
–n	เขียนการตั้งค่าที่มีอ็อพชันระดับการรักษาความปลอดภัย ที่เกี่ยวข้องไปยังไฟล์ที่ระบุโดยแฟล็ก **–o** คุณต้องระบุอ็อพชัน **–o** เมื่อคุณใช้อ็อพชัน **–n**
–o	บันทึกเอาท์พุทการรักษาความปลอดภัยไปยังไฟล์ที่ระบุ โดยตัวแปร *filename* สิทธิ์การอ่านและ การเขียนไฟล์เอาท์พุทจะถูกกำหนดค่าเป็นรูทเพื่อความปลอดภัย ไฟล์นี้จะต้องได้รับการปกป้องจากการเข้าถึงที่ไม่ต้องการ
–p	ระบุว่าเอาท์พุทของ กฎการรักษาความปลอดภัยจะแสดงขึ้นโดยใช้เอาท์พุท Verbose อ็อพชัน **–p** จะบันทึกกฎที่ประมวลผลในระบบย่อยการตรวจสอบหากอ็อพชัน **auditing** ถูกเปิดใช้ อ็อพชันนี้สามารถใช้กับอ็อพชัน **–l, –u, –c** และ **–f**
–P	ยอมรับชื่อโปรไฟล์เป็นอินพุท อ็อพชันนี้จะถูกใช้ร่วมกับอ็อพชัน **–c** อ็อพชัน **–c** ร่วมกับอ็อพชัน **–P** จะถูกใช้เพื่อตรวจสอบการทำงานร่วมกัน ของระบบที่มีโปรไฟล์ที่ส่งผ่าน
–r	เขียนการตั้งค่าที่มีอยู่ ของระบบไปยังไฟล์ `/etc/security/aixpert/check_report.txt` คุณสามารถใช้เอาท์พุทในรายงานการตรวจสอบการปฏิบัติตามมาตรฐานและการรักษาความปลอดภัย รายงานจะอธิบายแต่ละการตั้งค่า และมีความเกี่ยวข้องกับข้อกำหนดของการปฏิบัติตาม ข้อบังคับอย่างไร และไม่ว่าการตรวจสอบจะผ่านหรือล้มเหลว
–R	จะให้เอาท์พุทเช่นเดียวกับแฟล็ก **–r** แต่แฟล็กนี้จะมีคำอธิบายเพิ่มเติมเกี่ยวกับแต่ละ สคริปต์และโปรแกรมที่ใช้เพื่อปรับใช้การตั้งค่าคอนฟิกูเรชัน
–t	แสดงชนิดของโปรไฟล์ ที่ปรับใช้บนระบบ
–u	ยกเลิกการตั้งค่าการรักษาความปลอดภัยที่ปรับใช้

พารามิเตอร์

รายการ	คำอธิบาย
filename	ไฟล์เอาท์พุทที่เก็บการตั้งค่าการรักษาความปลอดภัย ต้องมีสิทธิ์รูทในการเข้าถึงไฟล์นี้
profile_name	ชื่อไฟล์ของโปรไฟล์ที่มีกฎมาตรฐาน สำหรับระบบ ต้องมีสิทธิ์รูทในการเข้าถึงไฟล์นี้

การรักษาความปลอดภัย

คำสั่ง **pscxpert** สามารถรันได้เฉพาะรูท

ตัวอย่าง

1. เพื่อเขียนอ็อพชันการรักษาความปลอดภัยระดับสูงไปยังไฟล์เอาท์พุท ให้ป้อนคำสั่งต่อไปนี้:

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

   หลังจาก เสร็จสิ้นคำสั่งนี้ ไฟล์เอาท์พุทจะสามารถแก้ไข และ สามารถคอมเม้นต์กฎการรักษาความปลอดภัยเฉพาะโดยการล้อมรอบใน สตริงคอมเม้นต์ XML มาตรฐาน (<-- เริ่มต้น คอมเม้นต์ และ -\> ปิดคอมเม้นต์)
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. เพื่อตรวจสอบการตั้งค่าการรักษาความปลอดภัยของระบบ และเพื่อบันทึกกฎ ที่ล้มเหลวลงในระบบย่อยการตรวจสอบ ให้ป้อนคำสั่งต่อไปนี้:

   ```
   pscxpert -c -p
   ```
5. เพื่อสร้างรายงานและเขียนไปยังไฟล์ `/etc/security/aixpert/check_report.txt` ให้ป้อนคำสั่งต่อไปนี้:

   ```
   pscxpert -c -r
   ```

ตำแหน่ง

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

Files

รายการ	คำอธิบาย
/etc/security/aixpert/log/aixpert.log	มีบันทึกการติดตามของการตั้งค่าการรักษาความปลอดภัยที่ปรับใช้ซึ่งไม่ได้ใช้มาตรฐาน syslog คำสั่ง **pscxpert** จะเขียนโดยตรงไปยังไฟล์ มีสิทธิ์การอ่านและเขียน และต้องมีการรักษาความปลอดภัยรูท
/etc/security/aixpert/log/firstboot.log	มีบันทึกการติดตามของการตั้งค่าการรักษาความปลอดภัย ที่ถูกปรับใช้ระหว่างการบูตครั้งแรกของการติดตั้ง Secure by Default (SbD)
/etc/security/aixpert/core/undo.xml	มี XML ที่แสดงการตั้งค่าการรักษาความปลอดภัย ซึ่งสามารถยกเลิกได้

คำประกาศ

ข้อมูลนี้จัดทำขึ้นสำหรับผลิตภัณฑ์และการบริการที่นำเสนอในสหรัฐอเมริกา

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

IBM อาจมีสิทธิบัตรหรืออยู่ระหว่างการขอสิทธิบัตรที่ครอบคลุมหัวข้อที่อธิบายในเอกสารนี้ การนำเสนอเอกสารนี้ไม่ได้เป็นการมอบใบอนุญาตในสิทธิบัตรดังกล่าวให้แก่คุณ คุณสามารถส่งคำถามเกี่ยวกับใบอนุญาตเป็นลายลักษณ์อักษรไปที่:

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

หากมีคำถามเกี่ยวกับข้อมูลชุดอักขระไบต์คู่ (DBCS) โปรดติดต่อแผยกทรัพย์สินทางปัญญาของ IBM ในประเทศของคุณ หรือส่งคำถามเป็นลายลักษณ์อักษรไปที่ :

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

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

ข้อมูลนี้อาจมีความไม่ถูกต้องด้านเทคนิคหรือข้อผิดพลาดจากการพิมพ์ มีการดำเนินการเปลี่ยนแปลงข้อมูลในเอกสารนี้เป็นครั้งคราว การเปลี่ยนแปลงเหล่านี้จะรวมอยู่ในสิ่งพิมพ์เอดิชันใหม่ IBM อาจปรับปรุงและ/หรือเปลี่ยนแปลงในผลิตภัณฑ์และ/หรือโปรแกรมที่อธิบายไว้ในสิ่งพิมพ์นี้ได้ตลอดเวลาโดยไม่ต้องแจ้งให้ทราบ

การอ้างอิงใด ๆ ในข้อมูลเกี่ยวกับเว็บไซต์ที่ไม่ใช่ของ IBM ถูกนำเสนอเพื่อความสะดวกเท่านั้น และไม่อนุญาตให้กระทำการใด ๆ บนเว็บไซต์ เอกสารประกอบที่เว็บไซต์ดังกล่าวไม่ได้เป็นส่วนประกอบของเอกสารประกอบสำหรับIBM ผลิตภัณฑ์นี้และการใช้เว็บไซต์ดังกล่าวถือเป็นความเสี่ยงของคุณเอง

IBM อาจใช้หรือแจกจ่ายข้อมูลใดๆ ที่คุณให้ในรูปแบบต่างๆ ซึ่ง IBM เชื่อว่ามีความเหมาะสมได้โดยไม่เกิดข้อผูกมัดใดๆ กับคุณ

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

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

ข้อมูลดังกล่าวอาจพร้อมใช้งานภายใต้ระยะเวลาและเงื่อนไขที่เหมาะสม โดยมีการชำระค่าธรรมเนียมในบางกรณี

โปรแกรมที่ได้รับอนุญาตซึ่งอธิบายไว้ในเอกสารนี้และเอกสารประกอบที่ได้รับอนุญาตทั้งหมดที่มีอยู่มีการนำเสนอโดย IBM ภายใต้ระยะเวลา IBM ข้อตกลงกับลูกค้า IBM ข้อตกลงเกี่ยวกับใบอนุญาตโปรแกรมระหว่างประเทศของ หรือข้อตกลงที่เท่าเทียมใดๆระหว่างเรา

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

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

ข้อความทั้งหมดเกี่ยวกับแนวทางในอนาคตของ IBM หรือความตั้งใจสามารถเปลี่ยนหรือถอดถอนได้โดยไม่ต้องแจ้งให้ทราบ หรือแสดงเป้าหมายและวัตถุประสงค์เท่านั้น

ราคาที่แสดงทั้งหมดของ IBM เป็นราคาเสนอขายปลีกของ IBM ในปัจจุบันและอาจเปลี่ยนแปลงโดยไม่ต้องแจ้งให้ทราบ ผลลัพธ์จริงอาจแตกต่างไป

ข้อมูลนี้สำหรับวัตถุประสงค์การวางแผนเท่านั้น ข้อมูลนี้อาจมีการเปลี่ยนแปลงได้ก่อนที่ผลิตภัณฑ์ดังกล่าวใช้ประโยชน์ได้

ข้อมูลนี้มีตัวอย่างของข้อมูลและรายงานที่ใช้ในการดำเนินธุรกิจประจำวัน เพื่อแสดงข้อมูลให้สมบูรณ์ที่สุดเท่าที่จะเป็นไปได้ ตัวอย่างจึงมีชื่อของแต่ละบุคคล บริษัท ยี่ห้อ และผลิตภัณฑ์ต่างๆ ชื่อทุกชื่อเหล่านี้เป็นชื่อที่แต่งขึ้น และการเหมือนกันกับชื่อและที่อยู่ที่องค์กรธุรกิจจริงใช้งานถือเป็นเรื่องบังเอิญอย่างแท้จริง

ใบอนุญาตลิขสิทธิ์:

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

สำเนาแต่ละฉบับหรือส่วนใดๆ ของโปรแกรมตัวอย่างเหล่านี้หรืองานที่ต่อเนื่องใดๆ ต้องมีคำประกาศลิขสิทธิ์ดังนี้:

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

หากคุณกำลังดูสำเนาชั่วคราวข้อมูลนี้ ภาพถ่ายและภาพประกอบสีอาจไม่ปรากฏ

สิ่งที่ต้องพิจารณาเกี่ยวกับนโยบายความเป็นส่วนตัว

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

ข้อเสนอซอฟต์แวร์นี้ไม่ใช้คุกกี้ หรือเทคโนโลยีอื่นเพื่อรวบรวมข้อมูลอัตลักษณ์ส่วนบุคคล

ถ้าคอนฟิกูเรชันถูกปรับใช้สำหรับ ข้อเสนอกนี้จัดเตรียมให้คุณในฐานะลูกค้าสามารถรวบรวม ข้อมูลอัตลักษณ์ส่วนบุคคลจากผู้ใช้ขั้นปลายผ่านทางคุกกี้ และเทคโนโลยีอื่น คุณควรปรึกษากับที่ปรึกษาด้านกฎหมายเกี่ยวกับ ที่ใช้บังคับในการรวบรวมข้อมูล รวมถึงข้อกำหนดต่างๆ เพื่อการแจ้งเตือนและการยินยอม

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

เครื่องหมายการค้า

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

UNIX เป็นเครื่องหมายการค้าที่จดทะเบียนของ The Open Group ในสหรัฐฯ และประเทศอื่นๆ

ดัชนี

P

R

S

ก

ข

ค

ภ

ม

ร

พิมพ์ในสหรัฐอเมริกา