IBM PowerSC

Express Edition

เวอร์ชัน 1.1.3

PowerSC Express Edition

IBM PowerSC

Express Edition

เวอร์ชัน 1.1.3

PowerSC Express Edition

หมายเหตุ

ก่อนที่คุณจะใช้ข้อมูลนี้และผลิตภัณฑ์ที่สนับสนุน โปรดอ่านข้อมูลใน “คำประกาศ” ในหน้า 129

เอดิชันนี้ใช้กับ IBM PowerSC Express Edition Version 1.1.3 และกับรีลีสและโมดิฟิเคชันถัดมาทั้งหมดจนกว่า จะกล่าวไว้เป็นอย่างอื่นในเอดิชันใหม่

สารบัญ

เกี่ยวกับเอกสารนี้

เอกสารนี้ให้ผู้ดูแลระบบมีข้อมูล ที่ครบถ้วนเกี่ยวกับ ไฟล์ ระบบ และการรักษาความปลอดภัยเครือข่าย

การเน้น

ระเบียบการไฮไลต์ต่อไปนี้ถูกใช้ในเอกสารนี้:

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 ตัวอย่าง คุณสามารถใช้คำสั่ง **ls** เพื่อแสดงรายการไฟล์ หากคุณพิมพ์ `LS` ระบบจะตอบกลับว่า คำสั่งคือ `not found` เช่นเดียวกับ `FILEA`, `FiLea` และ `filea` ถือเป็นชื่อไฟล์ต่างกันสามชื่อ แม้ว่า ไฟล์เหล่านี้จะอยู่ในไดเร็กทอรีเดียวกัน เพื่อหลีกเลี่ยงการเกิดการดำเนินการ แอ็คชันที่ไม่ต้องการ ให้แน่ใจว่าคุณใช้ขนาดตัวพิมพ์ที่ถูกต้องเสมอ

ISO 9000

ระบบรับรองคุณภาพที่ลงทะเบียน ISO 9000 ใช้ในการพัฒนาและการผลิตผลิตภัณฑ์นี้

มีอะไรใหม่ใน PowerSC Express Edition 1.1.3

อ่านเกี่ยวกับข้อมูลใหม่หรือข้อมูลที่มีการเปลี่ยนแปลงที่สำคัญสำหรับ มีอะไรใหม่ในชุดหัวข้อ PowerSC™ Express Edition 1.1.3

วิธีดูสิ่งใหม่ หรือที่เปลี่ยนแปลง

ในไฟล์ PDF นี้ คุณอาจมองเห็นแถบการปรับปรุงใหม่ (|) ในขอบด้านซ้าย ที่ระบุข้อมูลใหม่หรือข้อมูลที่เปลี่ยนแปลง

ธันวาคม 2014

ข้อมูลต่อไปนี้ จัดเตรียมสรุปของเนื้อหาใหม่และอัพเดตสำหรับ PowerSC Express Edition 1.1.3.2:

- อัพดตแอ็คชันที่สอดคล้องกันสำหรับไอเท็มโปรไฟล์ต่างๆ ใน “ความเข้ากันได้ STIG ของกระทรวงกลาโหม” ในหน้า 10
- อัพเดตข้อมูลโปรโตคอล Network File System ใน “มาตรฐาน Payment Card Industry – Data Security Standard” ในหน้า 93
- อัพเดตแอ็คชันที่สอดคล้องกันสำหรับไอเท็มโปรไฟล์ต่างๆ ใน “มาตรฐาน Payment Card Industry – Data Security Standard” ในหน้า 93
- อัพเดต “คำสั่ง pscxpert” ในหน้า 123
- แทนที่การอ้างอิงกับคำสั่ง **aixpert** ด้วยคำสั่ง **pscxpert** ในหัวข้อต่างๆ
- ลบและอัพเดตข้อมูลที่ล้าสมัยในหัวข้อต่างๆ

พฤษภาคม 2014

ข้อมูลต่อไปนี้จัดเตรียมสรุปของเนื้อหาใหม่ และเนื้อหาที่อัพเดตสำหรับ PowerSC Express Edition 1.1.3.1:

- อัพเดตข้อมูลเกี่ยวกับส่วนสนับสนุนสำหรับ United States Department of Defense STIG ใน “ความเข้ากันได้ STIG ของกระทรวงกลาโหม” ในหน้า 10
- อัพเดตแฟล็กสำหรับ “คำสั่ง pscxpert” ในหน้า 123
- ลบและอัพเดตข้อมูลที่ล้าสมัยในหัวข้อต่างๆ

ธันวาคม 2013

ข้อมูลต่อไปนี้ จะมีสรุปของเนื้อหาใหม่และที่ปรับปรุงสำหรับ PowerSC Express Edition 1.1.3:

- เพิ่มข้อมูลเกี่ยวกับไฟล์ README.ICEexpress ใน “การติดตั้ง PowerSC Express Edition เวอร์ชัน 1.1.3” ในหน้า 7
- อัพเดตข้อมูลเกี่ยวกับการสนับสนุนสำหรับมาตรฐาน Payment Card Industry – Data Security Standard สำหรับเวอร์ชัน 2.0 ของ มาตรฐานใน “มาตรฐาน Payment Card Industry – Data Security Standard” ในหน้า 93
- อัพเดตพาธสำหรับคำสั่ง **RbacEnablement** ใน “Health Insurance Portability and Accountability Act (HIPAA)” ในหน้า 108
- เพิ่ม “คำสั่ง pscxpert” ในหน้า 123
- อัพเดตตัวอย่างใน “คำสั่ง pscxpert” ในหน้า 123

พฤษภาคม 2013

เพิ่มตารางที่อธิบายวิธี ที่คุณลักษณะ AIX Security Expert แน่ใจว่าปฏิบัติตาม Payment Card Industry – Data Security Standard ใน “มาตรฐาน Payment Card Industry – Data Security Standard” ในหน้า 93

พฤศจิกายน 2012

ข้อมูลต่อไปนี้ จะมีสรุปของเนื้อหาใหม่และเนื้อหาที่ปรับปรุงสำหรับ PowerSC Express Edition 1.1.2:

- เพิ่มเอกสารที่อธิบายคุณลักษณะ Real Time Compliance ใน “PowerSC Real Time Compliance” ในหน้า 121
- เพิ่มเอกสารคู่มือสำหรับการสนับสนุนมาตรฐานดังกำหนด โดย “Health Insurance Portability and Accountability Act (HIPAA)” ในหน้า 108

PowerSC Express Edition Release Notes Version 1.1.3

รีลีสโน้ตมีข้อมูลเกี่ยวกับการเปลี่ยนไปเป็น PowerSC Express Edition เวอร์ชัน 1.1.3 ที่ระบุไว้หลังจากที่เอกสารนี้สมบูรณ์แล้ว

มีอะไรใหม่

อ่านเกี่ยวกับข้อมูลใหม่หรือข้อมูลที่มีการเปลี่ยนแปลงใน คอลเล็กชันหัวข้อรีลีสโน้ตของ IBM® PowerSC Express Edition

พฤษภาคม 2014

ข้อมูลต่อไปนี้ กล่าวถึงไอเท็มใหม่หรือไอเท็มที่มีการเปลี่ยนแปลงซึ่งถูกระบุไว้หลังจากที่ ทำเนื้อหาของ IBM PowerSC Express Edition เสร็จสิ้นแล้ว:

เมื่อคุณโอนย้าย พาร์ติชันด้วยโปรไฟล์ DataBase, Department of Defense, Department of Defense Version 2 หรือ Payment Card Industry ที่เปิดใช้งานบน Virtual I/O Server (VIOS) ของคุณแล้ว ท่อความปลอดภัยจะถูกร้องขอ เพื่อการโอนย้ายโดยอัตโนมัติ อัพเดตไปยังกระบวนการโอนย้ายท่อความปลอดภัย จะถูกจัดเตรียมไว้ใน VIOS Service Pack 2.2.3.3

ธันวาคม 2013

ตำแหน่ง ของเนื้อหา IBM PowerSC ในศูนย์ข้อมูล จะถูกจัดโครงสร้างใหม่

อ่านข้อมูลนี้ก่อนการติดตั้ง

เมื่อต้องการดูเวอร์ชันปัจจุบันของรีลีส โน้ต ให้ไปที่ รีลีส โน้ต แบบออนไลน์ใน Knowledge Center (http://www.ibm.com/support/knowledgecenter/SSNRQU_1.1.3/com.ibm.powersc113.ee/powersc_ee_rn.htm)

PowerSC Express Edition มีโปรแกรมไลเซนส์ และไม่ได้สอดแทรกไว้ในระบบปฏิบัติการ AIX

หมายเหตุ: ซอฟต์แร์นี้อาจมีข้อผิดพลาดที่อาจส่งผลให้เกิดผลกระทบเชิงธุรกิจ ที่รุนแรง ติดตั้งโปรแกรมฟิกซ์ล่าสุด ก่อนที่จะใช้ซอฟต์แวร์นี้

การติดตั้ง การโอนย้าย การอัพเกรด และข้อมูล คอนฟิกูเรชัน

สำหรับข้อมูลเกี่ยวกับการติดตั้ง PowerSC โปรดดู “การติดตั้ง PowerSC Express Edition เวอร์ชัน 1.1.3” ในหน้า 7

Fix for Live Partition Mobility (LPM) โดยใช้ท่อ IP Security (IPSec)

โปรแกรมฟิกซ์สำหรับส่วนสนับสนุนท่อความปลอดภัยจะพร้อมใช้งานใน VIOS เซอร์วิสแพ็ก 2.2.3.3 เซอร์วิสแพ็กนี้จะแสดง APAR IV59934 และควรติดตั้งไว้บนเซิร์ฟเวอร์ VIOS

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 และการตรวจสอบการกำหนดคอนฟิกการรักษาความปลอดภัยและความเข้ากันได้เป็นอัตโนมัติสำหรับมาตรฐานต่อไปนี้: • 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. รัน คำสั่งต่อไปนี้:
   ```
   % 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 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 คุณลักษณะความปลอดภัยและความเข้ากันได้มีอยู่ใน PowerSC Express Edition และ PowerSC Standard Edition

แพ็กเกจการติดตั้ง PowerSC Express Edition, 5765-G82 ต้องติดตั้งบนระบบที่ถูกจัดการ AIX แพ็กเกจการติดตั้ง ชุดไฟล์ `powerscExp.ice` ที่สามารถนำไปใช้ได้บนระบบโดยใช้คำสั่ง AIX Profile Manager หรือ **pscxpert** PowerSC ที่มีมาตรฐาน IBM Compliance Expert Express (ICEE) จะถูกเปิดใช้เพื่อจัดการและปรับปรุงโปรไฟล์ XML โปรไฟล์ XML ถูกจัดการโดย AIX Profile Manager

หมายเหตุ: ติดตั้งแอ็พพลิเคชันทั้งหมดบนระบบก่อนที่คุณจะใช้โปรไฟล์ ความปลอดภัย

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 **pscxpert** ที่คล้ายกับ ICEE

โปรไฟล์ความเข้ากันได้ที่กำหนดคอนฟิกล่วงหน้าถูกจัดส่งพร้อม PowerSC Express Edition ช่วยลดเวิร์กโหลดของการควบคุมดูแลสำหรับการตีความเอกสารคู่มือความเข้ากันได้ และการอิมพลีเมนต์มาตรฐานพารามิเตอร์ของคอนฟิกูเรชันระบบที่

ระบุ 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 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 Express Edition ช่วยให้ กระบวนการกำหนดคอนฟิกค่าติดตั้งอัตโนมัติตามที่กำหนดโดย DoD

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

เริ่มต้นด้วยเซอร์วิสแพ็ก 1.1.3.1 ของ IBM PowerSC ซึ่ง PowerSC จะสนับสนุนข้อกำหนดของ AIX DoD STIG เวอร์ชัน 1 รีลีส 2 ข้อสรุปของข้อกำหนดและวิธีการตรวจสอบให้เกิดความมั่นใจว่า มีความสอดคล้องกันจะอยู่ในตารางต่อไปนี้

ตารางที่ 2. 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` **แอ็คชันความเข้ากันได้** ตรวจสอบให้แน่ใจว่า ระบบตรงกับข้อกำหนดที่ระบุไว้
AIX00040	2	คำสั่ง **securetcpip** ต้องถูกนำมาใช้	**ตำแหน่ง** `/etc/security/pscexpert/dodv2/dodsecuretcpip` **แอ็คชันความเข้ากันได้** ตรวจสอบให้แน่ใจว่า ระบบตรงกับข้อกำหนดที่ระบุไว้

ตารางที่ 2. 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` **แอ็คชันความเข้ากันได้** ตรวจสอบทุกสัปดาห์เพื่อระบุความเปลี่ยนแปลงกับไฟล์ ที่ระบุไว้
AIX00080	1	แอ็ตทริบิวต์ `SYSTEM` ต้องไม่ถูกตั้งค่าเป็น *none* สำหรับแอคเคาต์ใดๆ	**ตำแหน่ง** `/etc/security/pscexpert/dodv2/SYSattr` **แอ็คชันความเข้ากันได้** ตรวจสอบให้แน่ใจว่า แอ็ตทริบิวต์ที่ระบุถูกตั้งที่ไม่ใช่ *none* **หมายเหตุ:** ค่าติดตั้งนี้ไม่ได้ถูกเปลี่ยนโดยอัตโนมัติเมื่อรีเซ็ตนโยบายเป็น นโยบายดีฟอลต์ของ AIX โดยใช้ไฟล์ `DoDv2_to_AIXDefault.xml` คุณต้องเปลี่ยนค่าติดตั้งนี้แบบแมนวล
AIX00200	2	ระบบต้องไม่อนุญาตให้บอร์ดคาสก์โดยตรง เพื่อย้ายผ่านเกตเวย์	**ตำแหน่ง** `/etc/security/pscexpert/dodv2/ntwkoptsdod` **แอ็คชันความเข้ากันได้** ตั้งค่าอ็อพชันเครือข่าย `direct_broadcast` ไปเป็น *0*
AIX00210	2	ระบบต้องจัดเตรียมการป้องกันการจู่โจมจาก Internet Control Message Protocol (ICMP) บนการเชื่อมต่อ TCP	**ตำแหน่ง** `/etc/security/pscexpert/dodv2/ntwkoptsdod` **แอ็คชันความเข้ากันได้** ตั้งค่าอ็อพชันเครือข่าย `tcp_icmpsecure` เป็น *1*
AIX00220	2	ระบบต้องจัดเตรียมการป้องกันสำหรับสแต็ก TCP กับการรีเซ็ตการเชื่อมต่อ ซิงโครไนซ์ (SYN) และการติดไวรัส ของข้อมูล	**ตำแหน่ง** `/etc/security/pscexpert/dodv2/ntwkoptsdod` **แอ็คชันความเข้ากันได้** ตรวจสอบให้แน่ใจว่า ค่าสำหรับอ็อพชัน `tcp_tcpsecure` ถูกตั้งค่าเป็น *7*
AIX00230	2	ระบบต้องจัดเตรียมการป้องกันการจู่โจมการทำแฟรกเมนต์ IP	**ตำแหน่ง** `/etc/security/pscexpert/dodv2/ntwkoptsdod` **แอ็คชันความเข้ากันได้** ตั้งค่าอ็อพชันเครือข่าย `ip_nfrag` เป็น *200*

ตารางที่ 2. 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` **แอ็คชันความเข้ากันได้** ปิดใช้งานเซอร์วิสที่ระบุ
AIX00310	2	ไฟล์ `/etc/ftpaccess.ctl` ต้องมีอยู่	**ตำแหน่ง** `/etc/security/pscexpert/dodv2/dodv2loginherald` **แอ็คชันความเข้ากันได้** ตรวจสอบให้แน่ใจว่า ไฟล์มีอยู่จริง
GEN000020	2	ระบบต้องมีการพิสูจน์ตัวตน เมื่อเริ่มต้นโหมดผู้ใช้เดี่ยว	**ตำแหน่ง** `/etc/security/pscexpert/dodv2/rootpasswd_home` **แอ็คชันความเข้ากันได้** ตรวจสอบให้แน่ใจว่า แอคเคาต์สำหรับพาร์ติชันที่สามารถบูตได้มีรหัสผ่านอยู่ในไฟล์ `/etc/security/passwd` **หมายเหตุ:** ค่าติดตั้งนี้ไม่ได้ถูกเปลี่ยนโดยอัตโนมัติเมื่อรีเซ็ตนโยบายเป็น นโยบายดีฟอลต์ของ AIX โดยใช้ไฟล์ `DoDv2_to_AIXDefault.xml` คุณต้องเปลี่ยนค่าติดตั้งนี้แบบแมนวล
GEN000100	1	ระบบปฏิบัติการต้องสนับสนุน รีลีส	**ตำแหน่ง** `/etc/security/pscexpert/dodv2/dodv2cat1` **แอ็คชันความเข้ากันได้** แสดงผลลัพธ์ของการทดสอบกฎที่ระบุเฉพาะ
GEN000120	2	แพตช์และอัพเดตความปลอดภัยของระบบปัจจุบันโดยส่วนใหญ่ ต้องถูกติดตั้งไว้	**ตำแหน่ง** `/usr/sbin/instfix -i` `/etc/security/pscexpert/dodv2/dodv2cat1` **แอ็คชันความเข้ากันได้** กำหนดคอนฟิกนี้โดยใช้คุณลักษณะ Trusted Network Connect

ตารางที่ 2. 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 **แอ็คชันความเข้ากันได้** ตรวจสอบทุกสัปดาห์เพื่อระบุความเปลี่ยนแปลงกับไฟล์ที่ระบุไว้
GEN000220	2	ระบบต้องถูกตรวจสอบทุกสัปดาห์สำหรับไฟล์ setuid ที่ไม่ได้รับสิทธิ์ และโมดิฟิเคชันที่ไม่ได้รับสิทธิ์เพื่อให้สิทธิ์กับไฟล์ setuid	**ตำแหน่ง** /etc/security/pscexpert/dodv2/trust **แอ็คชันความเข้ากันได้** ตรวจสอบทุกสัปดาห์เพื่อระบุความเปลี่ยนแปลงกับไฟล์ที่ระบุไว้
GEN000240	2	นาฬิกาของระบบต้องถูกซิงโครไนซ์กับแหล่งข้อมูลเวลา Department of Defense (DoD) ที่ได้รับสิทธิ์	**ตำแหน่ง** /etc/security/pscexpert/dodv2/dodv2cmntrows **แอ็คชันความเข้ากันได้** ตรวจสอบให้แน่ใจว่า เวลาของระบบสอดคล้องกัน
GEN000241	2	นาฬิกาของระบบต้องถูกซิงโครไนซ์อย่างต่อเนื่อง หรืออย่างน้อยทุกวัน	**ตำแหน่ง** /etc/security/pscexpert/dodv2/dodv2cmntrows **แอ็คชันความเข้ากันได้** ตรวจสอบให้แน่ใจว่า เวลาของระบบสอดคล้องกัน
GEN000242	2	ระบบต้องใช้แหล่งข้อมูลเวลาอย่างน้อยสองแหล่ง สำหรับการซิงโครไนซ์นาฬิกา	**ตำแหน่ง** /etc/security/pscexpert/dodv2/dodv2netrules **แอ็คชันความเข้ากันได้** ตรวจสอบให้แน่ใจว่ามีแหล่งข้อมูลเวลามากกว่าหนึ่งแหล่งที่ต้องถูกใช้สำหรับการซิงโครไนซ์นาฬิกา
GEN000280	2	การล็อกอินโดยตรงไปยังชนิดของแอคเคาต์ต่อไปนี้ไม่ได้รับอนุญาต: • แอ็พพลิเคชัน • ค่าดีฟอลต์ • แบ่งใช้ • ยูทิลิตี	**ตำแหน่ง** /etc/security/pscexpert/dodv2/lockacc_rlogin **แอ็คชันความเข้ากันได้** จัดเตรียมการล็อกอินโดยตรงไปยังแอคเคาต์ที่ระบุเฉพาะ

ตารางที่ 2. ข้อกำหนดทั่วไปของ DoD (ต่อ)

ID จุดตรวจสอบของ Department of Defense STIG	หมวดหมู่ของกฎ STIG	รายละเอียด	ตำแหน่งของสคริปต์ที่นิยามแอ็คชัน และผลลัพธ์ของแอ็คชันที่เปิดใช้งานความเข้ากันได้
GEN000290	2	ระบบต้องไม่มีแอคเคาต์ที่ไม่จำเป็น	**ตำแหน่ง** `/etc/security/pscexpert/dodv2/lockacc_rlogin` **แอ็คชันความเข้ากันได้** ตรวจสอบให้แน่ใจว่าไม่มีแอคเคาต์ที่ไม่ได้ใช้งาน
GEN000300 (เกี่ยวข้องกับ GEN000320, GEN000380, GEN000880)	2	แอคเคาต์ทั้งหมดบนระบบต้องเป็นผู้ใช้หรือชื่อแอคเคาต์ที่ไม่ซ้ำกัน และรหัสผ่านผู้ใช้หรือรหัสผ่านแอคเคาต์ที่ไม่ซ้ำกัน	**ตำแหน่ง** `/etc/security/pscexpert/dodv2/grpusrpass_chk` **แอ็คชันความเข้ากันได้** ตรวจสอบให้แน่ใจว่าแอคเคาต์ทั้งหมดตรงกับข้อกำหนดที่ระบุไว้เฉพาะ **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` **แอ็คชันความเข้ากันได้** ตรวจสอบให้แน่ใจว่าแอคเคาต์ทั้งหมดตรงกับข้อกำหนดที่ระบุไว้เฉพาะ **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` **แอ็คชันความเข้ากันได้** ค่าติดตั้งถูกเปิดใช้งานโดยอัตโนมัติเพื่อบังคับใช้กฎนี้

ตารางที่ 2. 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` **แอ็คชันความเข้ากันได้** ค่าติดตั้งนี้เปิดใช้งานโดยอัตโนมัติเพื่อบังคับใช้กฎนี้
GEN000380 (เกี่ยวข้องกับ GEN000300, GEN000320, GEN000880)	2	แอคเคาต์ทั้งหมดบนระบบต้องเป็นผู้ใช้หรือชื่อแอคเคาต์ที่ไม่ซ้ำกัน และรหัสผ่านผู้ใช้หรือรหัสผ่านแอคเคาต์ที่ไม่ซ้ำกัน	**ตำแหน่ง** `/etc/security/pscexpert/dodv2/grpusrpass_chk` **แอ็คชันความเข้ากันได้** ตรวจสอบให้แน่ใจว่าแอคเคาต์ทั้งหมดตรงกับข้อกำหนดที่ระบุไว้เฉพาะ
GEN000400	2	แบนเนอร์ล็อกอิน Department of Defense (DoD) ต้องถูกแสดงในทันทีก่อนหรือเป็นส่วนหนึ่งของพร้อมต์ล็อกอิน คอนโซล	**ตำแหน่ง** `/etc/security/pscexpert/dodv2/dodv2loginherald` **แอ็คชันความเข้ากันได้** แสดงแบนเนอร์ที่ต้องการ
GEN000402	2	แบนเนอร์ล็อกอิน DoD ต้องถูกแสดงในทันที ก่อน หรือเป็นส่วนหนึ่งของพร้อมต์ล็อกอินสภาวะแวดล้อมเดสก์ท็อปแบบกราฟิก	**ตำแหน่ง** `/etc/security/pscexpert/dodv2/dodv2loginherald` **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` **แอ็คชันความเข้ากันได้** แสดงแบนเนอร์เมื่อคุณใช้ FTP
GEN000440	2	ความพยายามในการล็อกอินหรือล็อกเอาต์ที่สำเร็จหรือไม่สำเร็จ ต้องถูกบันทึก	**ตำแหน่ง** `/etc/security/pscexpert/dodv2/loginout` **แอ็คชันความเข้ากันได้** เปิดใช้งานการล็อกที่จำเป็น
GEN000452	2	ระบบต้องแสดงวันที่และเวลาล็อกอินแอคเคาต์ล่าสุดที่เป็นผลสำเร็จ ในแต่ละครั้งที่ล็อกอิน	**ตำแหน่ง** `/etc/security/pscexpert/dodv2/sshDoDconfig` **แอ็คชันความเข้ากันได้** แสดงข้อมูลที่จำเป็น

ตารางที่ 2. 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` **แอ็คชันความเข้ากันได้** ตั้งค่าข้อจำกัดของความพยายามในการล็อกอินตามค่าที่ระบุไว้
GEN000480	2	กฎนี้ตั้งค่าเวลาหน่วงของการล็อกอินไว้ 4 วินาที	**ตำแหน่ง** `/etc/security/pscexpert/dodv2/chdefstanzadod` **แอ็คชันความเข้ากันได้** ตั้งค่าเวลาหน่วงของการล็อกอินไว้เป็นค่าต้องการ
GEN000540	2	ค่านี้ทำให้มั่นใจได้ว่า การกำหนดค่าของไฟล์คอนฟิกูเรชันสำหรับ รหัสผ่านโกลบอลของระบบเป็นไปตามข้อกำหนดเกี่ยวกับรหัสผ่าน	**ตำแหน่ง** `/etc/security/pscexpert/dodv2/chusrattrdod` **แอ็คชันความเข้ากันได้** ตั้งค่ารหัสผ่านที่ต้องการ
GEN000560	1	แอคเคาต์ทั้งหมดบนระบบต้องมี รหัสผ่านที่ถูกต้อง	**ตำแหน่ง** `/etc/security/pscexpert/dodv2/grpusrpass_chk` **แอ็คชันความเข้ากันได้** ตรวจสอบให้แน่ใจว่า แอคเคาต์มีรหัสผ่าน
GEN000580	2	กฎนี้ทำให้มั่นใจได้ว่า รหัสผ่านทั้งหมดมีอักขระ อย่างน้อยที่สุด 14 ตัวอักษร	**ตำแหน่ง** `/etc/security/pscexpert/dodv2/chusrattrdod` **แอ็คชันความเข้ากันได้** ตั้งค่าความยาวรหัสผ่านต่ำสุดเป็น 14 ตัวอักษร
GEN000585	2	ระบบต้องใช้ Federal Information Processing Standards (FIPS) 140-2 ที่ได้รับการอนุมัติในส่วนของอัลกอริทึมการแฮชของการเข้ารหัส สำหรับการสร้างการแฮชรหัสผ่านแอคเคาต์	**ตำแหน่ง** `/etc/security/pscexpert/dodv2/fipspasswd` **แอ็คชันความเข้ากันได้** ตรวจสอบให้แน่ใจว่า การแฮชรหัสผ่านใช้อัลกอริทึมการแฮชที่ได้รับอนุญาต

ตารางที่ 2. 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` **แอ็คชันความเข้ากันได้** ตรวจสอบให้แน่ใจว่า การแฮชรหัสผ่านใช้อัลกอริทึมการแฮชที่ได้รับอนุญาต
GEN000595	2	ใช้ FIPS 140-2 ที่ได้รับการอนุมัติในส่วนของ อัลกอริทึมการแฮชของการเข้ารหัสผ่านเมื่อสร้างการแฮชรหัสผ่านที่ถูกเก็บไว้บนระบบ	**ตำแหน่ง** `/etc/security/pscexpert/dodv2/fipspasswd` **แอ็คชันความเข้ากันได้** ตรวจสอบให้แน่ใจว่า การแฮชรหัสผ่านใช้อัลกอริทึมการแฮชที่ได้รับอนุญาต
GEN000640	2	กฎนี้ต้องการอักขระที่ไม่ใช่ตัวอักษรอย่างน้อยหนึ่งตัว ในรหัสผ่าน	**ตำแหน่ง** `/etc/security/pscexpert/dodv2/chusrattrdod` **แอ็คชันความเข้ากันได้** ตั้งค่าจำนวนต่ำสุดของอักขระที่ไม่ใช่ตัวอักษรในรหัสผ่าน เป็น 1
GEN000680	2	กฎนี้ทำให้มั่นใจว่า รหัสผ่านไม่มีอักขระที่ซ้ำกันต่อเนื่อง มากกว่าสามตัวอักษร	**ตำแหน่ง** `/etc/security/pscexpert/dodv2/chusrattrdod` **แอ็คชันความเข้ากันได้** ตั้งค่าจำนวนต่ำสุดของอักขระที่ซ้ำกันในรหัสผ่าน เป็น 3
GEN000700	2	ค่านี้ทำให้มั่นใจได้ว่า การกำหนดค่าของไฟล์คอนฟิกูเรชันสำหรับ รหัสผ่านโกลบอลของระบบเป็นไปตามข้อกำหนดเกี่ยวกับรหัสผ่าน	**ตำแหน่ง** `/etc/security/pscexpert/dodv2/chusrattrdod` **แอ็คชันความเข้ากันได้** ตรวจสอบให้แน่ใจว่า ไฟล์คอนฟิกูเรชันรหัสผ่านตรงกับข้อกำหนด
GEN000740	2	รหัสผ่านแอคเคาต์การประมวลผลแบบไม่โต้ตอบและเป็นแบบอัตโนมัติทั้งหมด ต้องถูกล็อก (GEN000280) การล็อกอินโดยตรงต้องไม่ได้รับอนุญาตให้แบ่งใช้ หรือทำเป็นค่าดีฟอลต์ หรือเป็นแอ็พพลิเคชัน หรือแอคเคาต์ยูทิลิตีใดๆ (GEN002640) แอคเคาต์ของระบบดีฟอลต์ต้องถูกปิดใช้งานหรือถูกลบทิ้ง	**ตำแหน่ง** `/etc/security/pscexpert/dodv2/loginout` `/etc/security/pscexpert/dodv2/lockacc_rlogin` **แอ็คชันความเข้ากันได้** ค่าติดตั้งนี้ถูกเปิดใช้งานแบบอัตโนมัติ

ตารางที่ 2. 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` **แอ็คชันความเข้ากันได้** ตรวจสอบให้แน่ใจว่า รหัสผ่านที่ระบุไว้ถูกเปลี่ยนทุกปีหรือถูกล็อก
GEN000750	2	กฎนี้ต้องการรหัสผ่านใหม่เพื่อให้มีอักขระอย่างน้อย 4 ตัวอักษรที่ไม่ได้อยู่ในรหัสผ่านเก่า	**ตำแหน่ง** `/etc/security/pscexpert/dodv2/chusrattrdod` **แอ็คชันความเข้ากันได้** ตั้งค่าจำนวนต่ำสุดของอักขระใหม่ที่ต้องการในรหัสผ่านใหม่ ให้มีค่า 4
GEN000760	2	แอคเคาต์ต้องถูกล็อกหลังจากที่ไม่ได้ใช้งาน 35 วัน	**ตำแหน่ง** `/etc/security/pscexpert/dodv2/disableacctdod` **แอ็คชันความเข้ากันได้** ล็อกแอคเคาต์หลังจากที่ไม่ได้ใช้งาน 35 วัน
GEN000790	2	ระบบต้องปกป้องการใช้คำในพจนานุกรม สำหรับรหัสผ่าน	**ตำแหน่ง** `/etc/security/pscexpert/dodv2/chuserstanzadod` **แอ็คชันความเข้ากันได้** ตรวจสอบให้แน่ใจว่า รหัสผ่านดีฟอลต์ที่ตั้งค่าไว้แข็งแรง
GEN000800	2	กฎนี้ทำให้มั่นใจได้ว่า รหัสผ่านห้าอันดับสุดท้าย ไม่ได้ถูกนำมาใช้ใหม่	**ตำแหน่ง** `/etc/security/pscexpert/dodv2/chusrattrdod` **แอ็คชันความเข้ากันได้** ตรวจสอบให้มั่นใจว่า รหัสผ่านใหม่ไม่ใช่รหัสผ่านที่ตรงกับรหัสผ่าน 5 อันดับสุดท้าย
GEN000880 (เกี่ยวข้องกับ GEN000300, GEN000320, GEN000380)	2	แอคเคาต์ทั้งหมดบนระบบต้องเป็นผู้ใช้หรือชื่อแอคเคาต์ที่ไม่ซ้ำกัน และรหัสผ่านผู้ใช้หรือรหัสผ่านแอคเคาต์ที่ไม่ซ้ำกัน	**ตำแหน่ง** `/etc/security/pscexpert/dodv2/grpusrpass_chk` **แอ็คชันความเข้ากันได้** ตรวจสอบให้แน่ใจว่า แอคเคาต์ทั้งหมดตรงกับข้อกำหนดที่ระบุไว้

ตารางที่ 2. 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` **แอ็คชันความเข้ากันได้** ตรวจสอบให้แน่ใจว่า ระบบตรงกับข้อกำหนดที่ระบุไว้ **หมายเหตุ:** ค่าติดตั้งนี้ไม่ได้ถูกเปลี่ยนโดยอัตโนมัติเมื่อรีเซ็ตนโยบายเป็น นโยบายดีฟอลต์ของ AIX โดยใช้ไฟล์ `DoDv2_to_AIXDefault.xml` คุณต้องเปลี่ยนค่าติดตั้งนี้แบบแมนวล
GEN000940	2	พาธการค้นหาที่สามารถเรียกทำงานได้ของแอคเคาต์ root ต้องเป็นค่าดีฟอลต์ของผู้จำหน่าย และต้องมีพาธสัมพันธ์เท่านั้น	**ตำแหน่ง** `/etc/security/pscexpert/dodv2/fixpathvars` **แอ็คชันความเข้ากันได้** ตรวจสอบให้แน่ใจว่า ระบบตรงกับข้อกำหนด ที่ระบุไว้ **หมายเหตุ:** ค่าติดตั้งนี้ไม่ได้ถูกเปลี่ยนโดยอัตโนมัติเมื่อรีเซ็ตนโยบายเป็น นโยบายดีฟอลต์ของ AIX โดยใช้ไฟล์ `DoDv2_to_AIXDefault.xml` คุณต้องเปลี่ยนค่าติดตั้งนี้แบบแมนวล
GEN000945	2	พาธการค้นหาไลบรารีของแอคเคาต์ root ต้องเป็นค่าดีฟอลต์ของระบบ และต้องมีเฉพาะพาธสัมบูรณ์เท่านั้น	**ตำแหน่ง** `/etc/security/pscexpert/dodv2/fixpathvars` **แอ็คชันความเข้ากันได้** ตรวจสอบให้แน่ใจว่า ระบบตรงกับข้อกำหนด ที่ระบุไว้ **หมายเหตุ:** ค่าติดตั้งนี้ไม่ได้ถูกเปลี่ยนโดยอัตโนมัติเมื่อรีเซ็ตนโยบายเป็น นโยบายดีฟอลต์ของ AIX โดยใช้ไฟล์ `DoDv2_to_AIXDefault.xml` คุณต้องเปลี่ยนค่าติดตั้งนี้แบบแมนวล

ตารางที่ 2. 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` **แอ็คชันความเข้ากันได้** ตรวจสอบให้แน่ใจว่า ระบบตรงกับข้อกำหนด ที่ระบุไว้ **หมายเหตุ:** ค่าติดตั้งนี้ไม่ได้ถูกเปลี่ยนโดยอัตโนมัติเมื่อรีเซ็ตนโยบายเป็น นโยบายดีฟอลต์ของ AIX โดยใช้ไฟล์ `DoDv2_to_AIXDefault.xml` คุณต้องเปลี่ยนค่าติดตั้งนี้แบบแมนวล
GEN000960 (เกี่ยวข้องกับ GEN003000, GEN003020, GEN003160, GEN003360, GEN003380)	2	แอคเคาต์ root ต้องมีไดเร็กทอรีที่สามารถเขียนได้ในพาธการค้นหาที่สามารถเรียกทำงานได้	**ตำแหน่ง** `/etc/security/pscexpert/dodv2/rmwwpaths` **แอ็คชันความเข้ากันได้** ตรวจสอบให้แน่ใจว่า ระบบตรงกับข้อกำหนด ที่ระบุไว้ **หมายเหตุ:** ค่าติดตั้งนี้ไม่ได้ถูกเปลี่ยนโดยอัตโนมัติเมื่อรีเซ็ตนโยบายเป็น นโยบายดีฟอลต์ของ AIX โดยใช้ไฟล์ `DoDv2_to_AIXDefault.xml` คุณต้องเปลี่ยนค่าติดตั้งนี้แบบแมนวล
GEN000980	2	ระบบต้องปกป้องแอคเคาต์ root จากการล็อกอินโดยตรง ยกเว้นจากคอนโซลของระบบ	**ตำแหน่ง** `/etc/security/pscexpert/dodv2/chuserstanzadod` **แอ็คชันความเข้ากันได้** ตรวจสอบให้แน่ใจว่า ระบบตรงกับข้อกำหนดที่ระบุไว้
GEN001000	2	คอนโซลแบบรีโมตต้องถูกปิดใช้งานหรือได้รับการปกป้อง จากการเข้าถึงที่ไม่ได้รับอนุญาต	**ตำแหน่ง** `/etc/security/pscexpert/dodv2/remoteconsole` **แอ็คชันความเข้ากันได้** ตรจสอบให้แน่ใจว่า คอนโซลที่ระบุไว้ถูกปิดใช้งาน
GEN001020	2	แอคเคาต์ root ต้องไม่ถูกใช้สำหรับ การล็อกอินโดยตรง	**ตำแหน่ง** `/etc/security/pscexpert/dodv2/sshDoDconfig` **แอ็คชันความเข้ากันได้** ปิดใช้งานแอคเคาต์ root จากการล็อกอินโดยตรง

ตารางที่ 2. 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` **แอ็คชันความเข้ากันได้** ตรวจสอบให้แน่ใจว่า ระบบตรงกับข้อกำหนดที่ระบุไว้
GEN001100	1	รหัสผ่าน root ต้องไม่ส่งผ่านเครือข่าย ในรูปของข้อความ	**ตำแหน่ง** `/etc/security/pscexpert/dodv2/chuserstanzadod` **แอ็คชันความเข้ากันได้** ตรวจสอบให้แน่ใจว่า ระบบตรงกับข้อกำหนดที่ระบุไว้
GEN001120	2	ระบบต้องไม่อนุญาตให้ใช้ล็อกอิน root โดยใช้โปรโตคอล SSH	**ตำแหน่ง** `/etc/security/pscexpert/dodv2/sshDoDconfig` **แอ็คชันความเข้ากันได้** ปิดใช้งานล็อกอิน root สำหรับ SSH
GEN001440	3	ผู้ใช้แบบโต้ตอบทั้งหมดต้องถูกกำหนดโฮมไดเร็กทอรี ไว้ในไฟล์ `/etc/passwd`	**ตำแหน่ง** `/etc/security/pscexpert/dodv2/grpusrpass_chk` **แอ็คชันความเข้ากันได้** ตรวจสอบให้แน่ใจว่า ผู้ใช้แบบโต้ตอบทั้งหมดมีไดเร็กทอรีที่ระบุเฉพาะ
GEN001475	2	ไฟล์ `/etc/group` ต้องไม่มีการแฮชรหัสผ่านแบบกลุ่มใดๆ	**ตำแหน่ง** `/etc/security/pscexpert/dodv2/passwdhash` **แอ็คชันความเข้ากันได้** ตรวจสอบให้แน่ใจว่า ไม่มีการแฮชรหัสผ่านแบบกลุ่มใน ไฟล์ที่ระบุเฉพาะ **หมายเหตุ:** ค่าติดตั้งนี้ไม่ได้ถูกเปลี่ยนโดยอัตโนมัติเมื่อรีเซ็ตนโยบายเป็น นโยบายดีฟอลต์ของ AIX โดยใช้ไฟล์ `DoDv2_to_AIXDefault.xml` คุณต้องเปลี่ยนค่าติดตั้งนี้แบบแมนวล

ตารางที่ 2. ข้อกำหนดทั่วไปของ DoD (ต่อ)

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

ตารางที่ 2. ข้อกำหนดทั่วไปของ DoD (ต่อ)

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

ตารางที่ 2. ข้อกำหนดทั่วไปของ DoD (ต่อ)

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

ตารางที่ 2. 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 **แอ็คชันความเข้ากันได้** ตรวจสอบให้แน่ใจว่า ไฟล์ที่ระบุไว้ตรงกับข้อกำหนดที่ระบุไว้
GEN002000	2	ต้องไม่มีไฟล์ .netrc บนระบบ	**ตำแหน่ง** /etc/security/pscexpert/dodv2/dodv2netrules **แอ็คชันความเข้ากันได้** ตรวจสอบให้มั่นใจว่า ไม่มีไฟล์ที่ระบุไว้บนระบบ **หมายเหตุ:** ค่าติดตั้งนี้ไม่ได้ถูกเปลี่ยนโดยอัตโนมัติเมื่อรีเซ็ตนโยบายเป็น นโยบายดีฟอลต์ของ AIX โดยใช้ไฟล์ DoDv2_to_AIXDefault.xml คุณต้องเปลี่ยนค่าติดตั้งนี้แบบแมนวล
GEN002020	2	ไฟล์ .rhosts, .shosts หรือ hosts.equiv ต้องมีคู่ของ โฮสต์–ผู้ใช้ที่เชื่อถือได้	**ตำแหน่ง** /etc/security/pscexpert/dodv2/dodv2netrules **แอ็คชันความเข้ากันได้** ตรวจสอบให้แน่ใจว่า ไฟล์ที่ระบุตรงกับข้อกำหนดนี้
GEN002040	1	กฎนี้ปิดใช้งานไฟล์ .rhosts, .shosts และ hosts.equiv หรือไฟล์ shosts.equiv	**ตำแหน่ง** /etc/security/pscexpert/dodv2/mvhostsfilesdod **แอ็คชันความเข้ากันได้** ปิดใช้งานไฟล์ที่ระบุไว้
GEN002120	1,2	กฎนี้ตรวจสอบและกำหนดคอนฟิกเชลล์ผู้ใช้	**ตำแหน่ง** /etc/security/pscexpert/dodv2/usershells **แอ็คชันความเข้ากันได้** สร้างเชลล์ที่ต้องการ **หมายเหตุ:** ค่าติดตั้งนี้ไม่ได้ถูกเปลี่ยนโดยอัตโนมัติเมื่อรีเซ็ตนโยบายเป็น นโยบายดีฟอลต์ของ AIX โดยใช้ไฟล์ DoDv2_to_AIXDefault.xml คุณต้องเปลี่ยนค่าติดตั้งนี้แบบแมนวล

ตารางที่ 2. 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` **แอ็คชันความเข้ากันได้** ตรวจสอบให้แน่ใจว่า เชลล์แสดงอยู่ในไฟล์ที่ถูกต้อง **หมายเหตุ:** ค่าติดตั้งนี้ไม่ได้ถูกเปลี่ยนโดยอัตโนมัติเมื่อรีเซ็ตนโยบายเป็น นโยบายดีฟอลต์ของ AIX โดยใช้ไฟล์ `DoDv2_to_AIXDefault.xml` คุณต้องเปลี่ยนค่าติดตั้งนี้แบบแมนวล
GEN002280	2	ไฟล์และไดเร็กทอรีอุปกรณ์ต้องสามารถเขียนได้โดยผู้ใช้ ที่มีแอคเคาต์ระบบเท่านั้น หรือเป็นระบบที่ถูกกำหนดคอฟนิกไว้โดยผู้จำหน่าย	**ตำแหน่ง** `/etc/security/pscexpert/dodv2/wwdevfiles` **แอ็คชันความเข้ากันได้** แสดงไฟล์อุปกรณ์ ไดเร็กทอรี และไฟล์อื่นใดที่สามารถเขียนได้ บนระบบที่อยู่ในไดเร็กทอรีที่ไม่ใช่พับลิก
GEN002300	2	ไฟล์อุปกรณ์ที่ใช้สำหรับการสำรองข้อมูล ต้องสามารถอ่านได้ สามารถเขียนได้ หรือทั้งสองอย่าง โดยผู้ใช้ root หรือผู้ใช้การสำรองข้อมูล เท่านั้น	**ตำแหน่ง** `/etc/security/pscexpert/dodv2/wwdevfiles` **แอ็คชันความเข้ากันได้** แสดงไฟล์อุปกรณ์ ไดเร็กทอรี และไฟล์อื่นใดที่สามารถเขียนได้ บนระบบที่อยู่ในไดเร็กทอรีที่ไม่ใช่พับลิก
GEN002400	2	ระบบต้องถูกตรวจสอบทุกสัปดาห์สำหรับไฟล์ `setuid` ที่ไม่ได้รับสิทธิ์ และโมดิฟิเคชันที่ไม่ได้รับสิทธิ์เพื่อให้สิทธิ์กับไฟล์ `setuid`	**ตำแหน่ง** `/etc/security/pscexpert/dodv2/trust` **แอ็คชันความเข้ากันได้** ตรวจสอบทุกสัปดาห์เพื่อระบุความเปลี่ยนแปลงกับไฟล์ ที่ระบุไว้ **หมายเหตุ:** เปรียบเทียบล็อกที่ใหม่ที่สุดรายสัปดาห์สองไฟล์ที่สร้างขึ้นในไดเร็กทอรี `/var/security/pscexpert` เพื่อตรวจสอบว่า ไม่มีกิจกรรมใดๆ ที่ไม่ได้รับอนุญาต

ตารางที่ 2. 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` **แอ็คชันความเข้ากันได้** ตรวจสอบให้แน่ใจว่า ระบบไฟล์ที่เมาท์แบบรีโมตมีอ็อพชัน ที่ระบุเฉพาะ **หมายเหตุ:** ค่าติดตั้งนี้ไม่ได้ถูกเปลี่ยนโดยอัตโนมัติเมื่อรีเซ็ตนโยบายเป็น นโยบายดีฟอลต์ของ AIX โดยใช้ไฟล์ `DoDv2_to_AIXDefault.xml` คุณต้องเปลี่ยนค่าติดตั้งนี้แบบแมนวล
GEN002430	2	สื่อบันทึกที่สามารถถอดออกได้ ระบบไฟล์แบบรีโมต และระบบไฟล์อื่นๆ ที่ไม่มีไฟล์อุปกรณ์ที่อนุมัติแล้วต้องถูกเมาท์โดยใช้อ็อพชัน *nodev*	**ตำแหน่ง** `/etc/security/pscexpert/dodv2/fsmntoptions` **แอ็คชันความเข้ากันได้** ตรวจสอบให้แน่ใจว่า ระบบไฟล์ที่เมาท์แบบรีโมตมีอ็อพชัน ที่ระบุเฉพาะ **หมายเหตุ:** ค่าติดตั้งนี้ไม่ได้ถูกเปลี่ยนโดยอัตโนมัติเมื่อรีเซ็ตนโยบายเป็น นโยบายดีฟอลต์ของ AIX โดยใช้ไฟล์ `DoDv2_to_AIXDefault.xml` คุณต้องเปลี่ยนค่าติดตั้งนี้แบบแมนวล
GEN002480	2	ไดเร็กทอรีแบบพับลิกต้องเป็นไดเร็กทอรีที่สามารถเขียนได้ และไฟล์ที่สามารถเขียนได้ต้องวางอยู่ในไดเร็กทอรี แบบพับลิกเท่านั้น	**ตำแหน่ง** `/etc/security/pscexpert/dodv2/wwdevfiles` `/etc/security/pscexpert/dodv2/fpmdodfiles` **แอ็คชันความเข้ากันได้** รายงานเมื่อไฟล์ที่สามารถเขียนได้ไม่ได้อยู่ในไดเร็กทอรีแบบพับลิก
GEN002640	2	แอคเคาต์ระบบดีฟอลต์ต้องถูกปิดใช้งาน หรือถอนออกได้	**ตำแหน่ง** `/etc/security/pscexpert/dodv2/lockacc_rlogin` `/etc/security/pscexpert/dodv2/loginout` **แอ็คชันความเข้ากันได้** ปิดใช้งานแอคเคาต์ระบบดีฟอลต์

ตารางที่ 2. ข้อกำหนดทั่วไปของ DoD (ต่อ)

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

ตารางที่ 2. ข้อกำหนดทั่วไปของ DoD (ต่อ)

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

ตารางที่ 2. 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 **แอ็คชันความเข้ากันได้** ตรวจสอบให้มั่นใจว่า ข้อจำกัดที่สอดคล้องกันถูกเปิดใช้งาน
GEN003000 (เกี่ยวข้องกับ GEN000960, GEN003020, GEN003160, GEN003360, GEN003380)	2	Cron ต้องไม่ได้รันโปรแกรมที่สามารถเขียนได้แบบกลุ่ม หรือโปรแกรมที่สามารถเขียนได้ทั่วไป	**ตำแหน่ง** /etc/security/pscexpert/dodv2/rmwwpaths **แอ็คชันความเข้ากันได้** ตรวจสอบให้มั่นใจว่า ข้อจำกัดที่สอดคล้องกันถูกเปิดใช้งาน **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 **แอ็คชันความเข้ากันได้** ถอนสิทธิที่สามารถเขียนได้จากไดเร็กทอรีโปรแกรม cron **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 **แอ็คชันความเข้ากันได้** ตรวจสอบให้แน่ใจว่า ระบบตรงกับข้อกำหนดที่ระบุไว้
GEN003160 (เกี่ยวข้องกับ GEN000960, GEN003000, GEN003020, GEN003360, GEN003380)	2	การสร้างล็อก Cron ต้องรันอยู่	**ตำแหน่ง** /etc/security/pscexpert/dodv2/rmwwpaths **แอ็คชันความเข้ากันได้** ตรวจสอบให้แน่ใจว่า ระบบตรงกับข้อกำหนดที่ระบุไว้

ตารางที่ 2. 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 **แอ็คชันความเข้ากันได้** ตรวจสอบให้แน่ใจว่า ระบบตรงกับข้อกำหนดที่ระบุไว้
GEN003300	2	ไฟล์ at.deny ต้องว่าง หากมีอยู่	**ตำแหน่ง** /etc/security/pscexpert/dodv2/chcronfilesdod **แอ็คชันความเข้ากันได้** ตรวจสอบให้แน่ใจว่า ระบบตรงกับข้อกำหนดที่ระบุไว้
GEN003320	2	แอคเคาต์ระบบดีฟอลต์ที่ไม่ใช่ root ต้องไม่แสดงอยู่ในไฟล์ at.allow หรือต้อง สอดแทรกในไฟล์ at.deny หากไฟล์ at.allow ไม่มีอยู่	**ตำแหน่ง** /etc/security/pscexpert/dodv2/chcronfilesdod **แอ็คชันความเข้ากันได้** ตรวจสอบให้แน่ใจว่า ระบบตรงกับข้อกำหนดที่ระบุไว้
GEN003360 (เกี่ยวข้องกับ GEN000960, GEN003000, GEN003020, GEN003160, GEN003380)	2	at daemon ต้องไม่รันโปรแกรมที่สามารถเขียนได้แบบกลุ่มหรือแบบทั่วไป	**ตำแหน่ง** /etc/security/pscexpert/dodv2/rmwwpaths **แอ็คชันความเข้ากันได้** ตรวจสอบให้แน่ใจว่า ระบบตรงกับข้อกำหนด ที่ระบุไว้ **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 **แอ็คชันความเข้ากันได้** ตรวจสอบให้แน่ใจว่า ระบบตรงกับข้อกำหนด ที่ระบุไว้ **หมายเหตุ:** ค่าติดตั้งนี้ไม่ได้ถูกเปลี่ยนโดยอัตโนมัติเมื่อรีเซ็ตนโยบายเป็น นโยบายดีฟอลต์ของ AIX โดยใช้ไฟล์ DoDv2_to_AIXDefault.xml คุณต้องเปลี่ยนค่าติดตั้งนี้แบบแมนวล

ตารางที่ 2. ข้อกำหนดทั่วไปของ DoD (ต่อ)

ID จุดตรวจสอบของ Department of Defense STIG	หมวดหมู่ของกฎ STIG	รายละเอียด	ตำแหน่งของสคริปต์ที่นิยามแอ็คชัน และผลลัพธ์ของแอ็คชันที่เปิดใช้งานความเข้ากันได้
GEN003510	2	ดัมพ์คอร์เคอร์เนลต้องถูกปิดใช้งาน ยกเว้นว่าจำเป็น	**ตำแหน่ง** `/etc/security/pscexpert/dodv2/coredumpdev` **แอ็คชันความเข้ากันได้** ปิดใช้งานดัมพ์คอร์เคอร์เนล
GEN003540	2	ระบบต้องใช้สแต็กโปรแกรม ที่ไม่สามารถเรียกทำงานได้	**ตำแหน่ง** `/etc/security/pscexpert/dodv2/sedconfigdod` **แอ็คชันความเข้ากันได้** บังคับใช้การใช้สแต็กโปรแกรมที่ไม่สามารถเรียกทำงานได้
GEN003600	2	ระบบต้องไม่ส่งต่อแพ็กเก็ตที่เราต์แหล่งที่มา IPv4	**ตำแหน่ง** `/etc/security/pscexpert/dodv2/ntwkoptsdod` **แอ็คชันความเข้ากันได้** ตั้งค่าอ็อพชันเครือข่าย `ipsrcforward` เป็น *0*
GEN003601	2	ขนาดคิวแบ็กล็อก TCP ต้องตั้งค่าไว้อย่างเหมาะสม	**ตำแหน่ง** `/etc/security/pscexpert/dodv2/ntwkoptsdod` **แอ็คชันความเข้ากันได้** 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` **แอ็คชันความเข้ากันได้** ตั้งค่าอ็อพชันเครือข่าย `bcastping` เป็น *0*
GEN003604	2	ระบบต้องไม่ตอบสนองกับคำร้องขอการประทับเวลา ICMP ที่ส่งไปยังแอดเดรสบอร์ดคาสก์	**ตำแหน่ง** `/etc/security/pscexpert/dodv2/ntwkoptsdod` **แอ็คชันความเข้ากันได้** ตั้งค่าอ็อพชันเครือข่าย `bcastping` เป็น *0*
GEN003605	2	ระบบต้องไม่นำการเราต์แหล่งที่มาที่สงวนไว้ไปยังการตอบสนอง TCP	**ตำแหน่ง** `/etc/security/pscexpert/dodv2/ntwkoptsdod` **แอ็คชันความเข้ากันได้** ตั้งค่าอ็อพชันเครือข่าย `nonlocsrcroute` เป็น *0*

ตารางที่ 2. ข้อกำหนดทั่วไปของ DoD (ต่อ)

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

ตารางที่ 2. ข้อกำหนดทั่วไปของ DoD (ต่อ)

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

ตารางที่ 2. 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` **แอ็คชันความเข้ากันได้** ตรวจสอบให้แน่ใจว่า ระบบตรงกับข้อกำหนดที่ระบุไว้
GEN004220	1	แอคเคาต์การดูแลจัดการต้องไม่รันเว็บเบราว์เซอร์ ยกเว้นว่าจำเป็นต้องมีสำหรับการดูแลจัดการเซอร์วิสโลคัล	**ตำแหน่ง** `/etc/security/pscexpert/dodv2/dodv2cat1` **แอ็คชันความเข้ากันได้** แสดงผลลัพธ์ของการทดสอบกฎที่ระบุเฉพาะ
GEN004460	2	กฎนี้ทำบันทึกข้อมูล `auth` และ `info`	**ตำแหน่ง** `/etc/security/pscexpert/dodv2/chsyslogdod` **แอ็คชันความเข้ากันได้** เปิดใช้งานการทำบันทึกข้อมูล `auth` และ `info`
GEN004540	2	กฎนี้ปิดใช้งานคำสั่งวิธีใช้ `sendmail`	**ตำแหน่ง** `/etc/security/pscexpert/dodv2/sendmailhelp` `/etc/security/pscexpert/dodv2/dodv2cmntrows` **แอ็คชันความเข้ากันได้** ปิดใช้งานคำสั่งที่ระบุเฉพาะ
GEN004580	2	ระบบต้องไม่ใช้ไฟล์ `.forward`	**ตำแหน่ง** `/etc/security/pscexpert/dodv2/forward` **แอ็คชันความเข้ากันได้** ปิดใช้งานไฟล์ที่ระบุ **หมายเหตุ:** ค่าติดตั้งนี้ไม่ได้ถูกเปลี่ยนโดยอัตโนมัติเมื่อรีเซ็ตนโยบายเป็น นโยบายดีฟอลต์ของ AIX โดยใช้ไฟล์ `DoDv2_to_AIXDefault.xml` คุณต้องเปลี่ยนค่าติดตั้งนี้แบบแมนวล

ตารางที่ 2. 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` **แอ็คชันความเข้ากันได้** ตรวจสอบให้แน่ใจว่าเวอร์ชันล่าสุดของเซอร์วิสที่ระบุไว้กำลังรันอยู่ **หมายเหตุ:** ค่าติดตั้งนี้ไม่ได้ถูกเปลี่ยนโดยอัตโนมัติเมื่อรีเซ็ตนโยบายเป็น นโยบายดีฟอลต์ของ AIX โดยใช้ไฟล์ `DoDv2_to_AIXDefault.xml` คุณต้องเปลี่ยนค่าติดตั้งนี้แบบแมนวล
GEN004620	2	เซิร์ฟเวอร์ `sendmail` ต้องปิดใช้งานคุณลักษณะการดีบัก	**ตำแหน่ง** `/etc/security/pscexpert/dodv2/SMTP_ver` **แอ็คชันความเข้ากันได้** ปิดใช้งานคุณสมบัติการดีบัก `sendmail`
GEN004640	1	เซอร์วิส SMTP ต้องไม่มี `uudecode` alias ที่แอ็คทีฟ	**ตำแหน่ง** `/etc/security/pscexpert/dodv2/SMTPuucode` **แอ็คชันความเข้ากันได้** ปิดใช้งาน `uudecode` alias
GEN004710	2	การรีเลย์เมลต้องเป็นข้อจำกัด	**ตำแหน่ง** `/etc/security/pscexpert/dodv2/sendmaildod` **แอ็คชันความเข้ากันได้** จำกัดการรีเลย์เมล
GEN004800	1,2,3	FTP ที่ไม่ได้เข้ารหัสไว้ต้องไม่ถูกใช้บน ระบบ	**ตำแหน่ง** `/etc/security/pscexpert/dodv2/inetdservices` **แอ็คชันความเข้ากันได้** ปิดใช้งาน daemons และเซอร์ที่จำเป็นโดยใส่คอมเมนต์ รายการในไฟล์ `/etc/inetd.conf`

ตารางที่ 2. 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` **แอ็คชันความเข้ากันได้** ปิดใช้งาน FTP แบบไม่ระบุชื่อบนระบบ **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` **แอ็คชันความเข้ากันได้** ตรวจสอบให้แน่ใจว่า FTP แบบไม่ระบุชื่อบนระบบอยู่บนเครือข่าย DMZ
GEN004880	2	ไฟล์ `ftpusers` ต้องมีอยู่	**ตำแหน่ง** `/etc/security/pscexpert/dodv2/chdodftpusers` **แอ็คชันความเข้ากันได้** ตรวจสอบให้แน่ใจว่า ไฟล์ที่ระบุอยู่บนระบบ
GEN004900	2	ไฟล์ `ftpusers` ต้องมีชื่อแอคเคาต์ที่ไม่อนุญาตให้ใช้โปรโตคอล FTP	**ตำแหน่ง** `/etc/security/pscexpert/dodv2/chdodftpusers` **แอ็คชันความเข้ากันได้** ตรวจสอบให้แน่ใจว่า ไฟล์มีชื่อแอคเคาต์ที่จำเป็นต้องมี

ตารางที่ 2. 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` **แอ็คชันความเข้ากันได้** ถอนเชลล์ออกจากแอคเคาต์ FTP ที่ไม่ระบุชื่อ **หมายเหตุ:** ค่าติดตั้งนี้ไม่ได้ถูกเปลี่ยนโดยอัตโนมัติเมื่อรีเซ็ตนโยบายเป็น นโยบายดีฟอลต์ของ AIX โดยใช้ไฟล์ `DoDv2_to_AIXDefault.xml` คุณต้องเปลี่ยนค่าติดตั้งนี้แบบแมนวล
GEN005080	1	`TFTP` daemon ต้องทำงาน ในโหมดความปลอดภัย ซึ่งจัดเตรียมการเข้าถึงไดเร็กทอรีเดี่ยว บนระบบโฮสต์ไฟล์เท่านั้น	**ตำแหน่ง** `/etc/security/pscexpert/dodv2/tftpdod` **แอ็คชันความเข้ากันได้** ตรวจสอบให้แน่ใจว่า daemon ตรงกับข้อกำหนดที่ระบุไว้
GEN005120	2	TFTP daemon ต้องถูกกำหนดไว้ให้กับข้อมูลจำเพาะของผู้จำหน่าย ซึ่งสอดแทรกแอคเคาต์ผู้ใช้ TFTP เฉพาะงาน เชลล์ที่ไม่มีการล็อกอิน เช่น `/bin/false` และโฮมไดเร็กทอรี ที่เป็นเจ้าของโดยผู้ใช้ TFTP	**ตำแหน่ง** `/etc/security/pscexpert/dodv2/tftpdod` **แอ็คชันความเข้ากันได้** ตรวจสอบให้แน่ใจว่า ระบบตรงกับข้อกำหนดที่ระบุไว้
GEN005140	1,2,3	TFTP daemon ที่แอ็คทีฟใดๆ ต้องได้รับสิทธิ์ และได้รับการอนุมัติในแพ็กเก็ตการรับรองระบบ	**ตำแหน่ง** `/etc/security/pscexpert/dodv2/inetdservices` **แอ็คชันความเข้ากันได้** ตรวจสอบให้แน่ใจว่า daemon ได้รับสิทธิ์
GEN005160	1,2	โฮสต์ X Window System ใดๆ ต้องเขียนไฟล์ `.Xauthority`	**ตำแหน่ง** `/etc/security/pscexpert/dodv2/dodv2disableX` **แอ็คชันความเข้ากันได้** ตรวจสอบให้แน่ใจว่า โฮสต์เขียนไฟล์ที่ระบุเฉพาะ
GEN005200	1,2	การแสดงผล X Window System ใดๆ ไม่สามารถเอ็กซ์พอร์ตไปยังพับลิกได้	**ตำแหน่ง** `/etc/security/pscexpert/dodv2/dodv2disableX` **แอ็คชันความเข้ากันได้** ปิดใช้งานการแพร่กระจายของโปรแกรม ที่ระบุเฉพาะ

ตารางที่ 2. 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 **แอ็คชันความเข้ากันได้** ตรวจสอบให้แน่ใจว่า ไฟล์ที่ระบุพร้อมใช้งานเพื่อจำกัดการเข้าถึงเซิร์ฟเวอร์
GEN005240	1,2	ยูทิลิตี .Xauthority ต้องอนุญาตให้เข้าถึงโฮสต์ที่ได้รับสิทธิ์เท่านั้น	**ตำแหน่ง** /etc/security/pscexpert/dodv2/dodv2disableX **แอ็คชันความเข้ากันได้** ตรวจสอบให้แน่ใจว่า สิทธิ์ถูกจำกัดในโฮสต์ที่ได้รับสิทธิ์
GEN005260	2	กฎนี้ปิดใช้งานการเชื่อมต่อ X Window System และโปรแกรมจัดการการล็อกอิน XServer	**ตำแหน่ง** /etc/security/pscexpert/dodv2/dodv2cmntrows **แอ็คชันความเข้ากันได้** ปิดใช้งานการเชื่อมต่อที่จำเป็นและโปรแกรมจัดการการล็อกอิน
GEN005280	1,2,3	ระบบต้องไม่มีเซอร์วิส UUCP ที่แอ็คทีฟ	**ตำแหน่ง** /etc/security/pscexpert/dodv2/inetdservices **แอ็คชันความเข้ากันได้** ปิดใช้งาน daemons และเซอร์ที่จำเป็นโดยใส่คอมเมนต์ รายการในไฟล์ /etc/inetd.conf
GEN005300	2	ชุมชน SNMP ต้องถูกเปลี่ยนจากค่าติดตั้ง ดีฟอลต์	**ตำแหน่ง** /etc/security/pscexpert/dodv2/chsnmp **แอ็คชันความเข้ากันได้** ตรวจสอบให้แน่ใจว่า ระบบตรงกับข้อกำหนดที่ระบุไว้
GEN005305	2	เซอร์วิส SNMP ต้องใช้เฉพาะ SNMPv3 หรือเวอร์ชัน ถัดมา	**ตำแหน่ง** /etc/security/pscexpert/dodv2/chsnmp **แอ็คชันความเข้ากันได้** ตรวจสอบให้แน่ใจว่า ระบบตรงกับข้อกำหนดที่ระบุไว้

ตารางที่ 2. 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` **แอ็คชันความเข้ากันได้** ตรวจสอบให้แน่ใจว่า ระบบตรงกับข้อกำหนดที่ระบุไว้
GEN005440	2	ระบบต้องใช้เซิร์ฟเวอร์ syslog แบบรีโมต (โฮสต์บันทึกการทำงาน)	**ตำแหน่ง** `/etc/security/pscexpert/dodv2/EnableTrustedLogging` **แอ็คชันความเข้ากันได้** ตรวจสอบให้แน่ใจว่าระบบกำลังใช้เซิร์ฟเวอร์ syslog แบบรีโมต
GEN005450	2	ระบบต้องใช้เซิร์ฟเวอร์ syslog แบบรีโมต (โฮสต์บันทึกการทำงาน)	**ตำแหน่ง** `/etc/security/pscexpert/dodv2/EnableTrustedLogging` **แอ็คชันความเข้ากันได้** ตรวจสอบให้แน่ใจว่าระบบกำลังใช้เซิร์ฟเวอร์ syslog แบบรีโมต
GEN005460	2	ระบบต้องใช้เซิร์ฟเวอร์ syslog แบบรีโมต (โฮสต์บันทึกการทำงาน)	**ตำแหน่ง** `/etc/security/pscexpert/dodv2/EnableTrustedLogging` **แอ็คชันความเข้ากันได้** ตรวจสอบให้แน่ใจว่าระบบกำลังใช้เซิร์ฟเวอร์ syslog แบบรีโมต
GEN005480	2	ระบบต้องใช้เซิร์ฟเวอร์ syslog แบบรีโมต (โฮสต์บันทึกการทำงาน)	**ตำแหน่ง** `/etc/security/pscexpert/dodv2/EnableTrustedLogging` **แอ็คชันความเข้ากันได้** ตรวจสอบให้แน่ใจว่าระบบกำลังใช้เซิร์ฟเวอร์ syslog แบบรีโมต
GEN005500	2	SSH daemon ต้องถูกกำหนดคอนฟิก เพื่อใช้เฉพาะโปรโตคอล Secure Shell เวอร์ชัน 2 (SSHv2)	**ตำแหน่ง** `/etc/security/pscexpert/dodv2/sshDoDconfig` **แอ็คชันความเข้ากันได้** ตรวจสอบให้แน่ใจว่า ระบบตรงกับข้อกำหนดที่ระบุไว้

ตารางที่ 2. 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` **แอ็คชันความเข้ากันได้** ตรวจสอบให้แน่ใจว่า ระบบตรงกับข้อกำหนดที่ระบุไว้
GEN005504	2	SSH daemon ต้อง listen แอดเดรสเครือข่ายการจัดการ ยกเว้นว่าได้รับสิทธิ์ให้ใช้ ที่นอกเหนือจากการจัดการ	**ตำแหน่ง** `/etc/security/pscexpert/dodv2/sshDoDconfig` **แอ็คชันความเข้ากันได้** ตรวจสอบให้แน่ใจว่า ระบบตรงกับข้อกำหนดที่ระบุไว้
GEN005505	2	SSH daemon ต้องถูกกำหนดคอนฟิกเพื่อใช้เฉพาะ ciphers ที่สอดคล้องกับมาตรฐาน Federal Information Processing Standards (FIPS) 140-2	**ตำแหน่ง** `/etc/security/pscexpert/dodv2/sshDoDconfig` **แอ็คชันความเข้ากันได้** ตรวจสอบให้แน่ใจว่า ระบบตรงกับข้อกำหนดที่ระบุไว้
GEN005506	2	SSH daemon ต้องถูกกำหนดคอนฟิก เพื่อใช้เฉพาะ ciphers ที่สอดคล้องกับมาตรฐาน FIPS 140-2	**ตำแหน่ง** `/etc/security/pscexpert/dodv2/sshDoDconfig` **แอ็คชันความเข้ากันได้** ตรวจสอบให้แน่ใจว่า ระบบตรงกับข้อกำหนดที่ระบุไว้
GEN005507	2	SSH daemon ต้องถูกกำหนดคอนฟิก เพื่อใช้เฉพาะ Message Authentication Codes (MACs) ด้วยอัลกอริทึมการแฮช ของการเข้ารหัสที่สอดคล้องกับมาตรฐาน FIPS 140-2	**ตำแหน่ง** `/etc/security/pscexpert/dodv2/sshDoDconfig` **แอ็คชันความเข้ากันได้** ตรวจสอบให้แน่ใจว่า ระบบตรงกับข้อกำหนดที่ระบุไว้
GEN005510	2	ไคลเอ็นต์ SSH ต้องถูกกำหนดคอนฟิก เพื่อใช้เฉพาะ MACs พร้อมกับ ciphers ที่สอดคล้องกับมาตรฐาน FIPS 140-2	**ตำแหน่ง** `/etc/security/pscexpert/dodv2/sshDoDconfig` **แอ็คชันความเข้ากันได้** ตรวจสอบให้แน่ใจว่า ระบบตรงกับข้อกำหนดที่ระบุไว้

ตารางที่ 2. 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` **แอ็คชันความเข้ากันได้** ตรวจสอบให้แน่ใจว่า ระบบตรงกับข้อกำหนดที่ระบุไว้
GEN005512	2	SSH daemon ต้องถูกกำหนดคอนฟิก เพื่อใช้เฉพาะ MACs ด้วยอัลกอริทึมการแฮชของการเข้ารหัส ที่สอดคล้องกับ FIPS 140-2 มาตรฐาน	**ตำแหน่ง** `/etc/security/pscexpert/dodv2/sshDoDconfig` **แอ็คชันความเข้ากันได้** ตรวจสอบให้แน่ใจว่า ระบบตรงกับข้อกำหนดที่ระบุไว้
GEN005521	2	SSH daemon ต้องจำกัดการล็อกอินแบบระบุผู้ใช้ กลุ่ม หรือทั้งสองแบบ	**ตำแหน่ง** `/etc/security/pscexpert/dodv2/sshDoDconfig` **แอ็คชันความเข้ากันได้** ตรวจสอบให้แน่ใจว่า ระบบตรงกับข้อกำหนดที่ระบุไว้
GEN005536	2	SSH daemon ต้องดำเนินการ ตรวจสอบโหมดแบบจำกัดของไฟล์คอนฟิกูเรชันโฮมไดเร็กทอรี	**ตำแหน่ง** `/etc/security/pscexpert/dodv2/sshDoDconfig` **แอ็คชันความเข้ากันได้** ตรวจสอบให้แน่ใจว่า ระบบตรงกับข้อกำหนดที่ระบุไว้
GEN005537	2	SSH daemon ต้องใช้การแยกสิทธิพิเศษ	**ตำแหน่ง** `/etc/security/pscexpert/dodv2/sshDoDconfig` **แอ็คชันความเข้ากันได้** ตรวจสอบให้แน่ใจว่า ระบบตรงกับข้อกำหนดที่ระบุไว้
GEN005538	2	SSH daemon ต้องไม่อนญาตให้ `rhosts` พิสูจน์ตัวตนโดยใช้ Rivest-Shamir-Adleman (RSA) cryptosystem	**ตำแหน่ง** `/etc/security/pscexpert/dodv2/sshDoDconfig` **แอ็คชันความเข้ากันได้** ตรวจสอบให้แน่ใจว่า ระบบตรงกับข้อกำหนดที่ระบุไว้

ตารางที่ 2. 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` **แอ็คชันความเข้ากันได้** ตรวจสอบให้แน่ใจว่า ระบบตรงกับข้อกำหนดที่ระบุไว้
GEN005550	2	SSH daemon ต้องถูกกำหนดคอนฟิก ด้วยแบนเนอร์ล็อกออน DoD	**ตำแหน่ง** `/etc/security/pscexpert/dodv2/sshDoDconfig` **แอ็คชันความเข้ากันได้** ตรวจสอบให้แน่ใจว่า ระบบตรงกับข้อกำหนดที่ระบุไว้
GEN005560	2	กำหนดว่ามีเกตเวย์ดีฟอลต์ ที่ถูกกำหนดคอนฟิกไว้สำหรับ IPv4	**ตำแหน่ง** `/etc/security/pscexpert/dodv2/chkgtway` **แอ็คชันความเข้ากันได้** ตรวจสอบให้แน่ใจว่า ระบบตรงกับข้อกำหนดที่ระบุไว้ **หมายเหตุ:** ค่าติดตั้งนี้ไม่ได้ถูกเปลี่ยนโดยอัตโนมัติเมื่อรีเซ็ตนโยบายเป็น นโยบายดีฟอลต์ของ AIX โดยใช้ไฟล์ `DoDv2_to_AIXDefault.xml` คุณต้องเปลี่ยนค่าติดตั้งนี้แบบแมนวล **หมายเหตุ:** ถ้าระบบของคุณ กำลังรันโปรโตคอล IPv6 ให้ตรวจสอบค่าติดตั้ง *ipv6_enabled* ในไฟล์ `/etc/security/pscexpert/ipv6.conf` ว่าตั้งค่า `yes` ไว้ ถ้าระบบไม่ได้ใช้ IPv6 ให้ตรวจสอบให้แน่ใจว่าค่า *ipv6_enabled* ถูกตั้งค่าเป็น `no`

ตารางที่ 2. 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` **แอ็คชันความเข้ากันได้** ตรวจสอบให้แน่ใจว่า ระบบตรงกับข้อกำหนดที่ระบุไว้ **หมายเหตุ:** ค่าติดตั้งนี้ไม่ได้ถูกเปลี่ยนโดยอัตโนมัติเมื่อรีเซ็ตนโยบายเป็น นโยบายดีฟอลต์ของ AIX โดยใช้ไฟล์ `DoDv2_to_AIXDefault.xml` คุณต้องเปลี่ยนค่าติดตั้งนี้แบบแมนวล **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` **แอ็คชันความเข้ากันได้** ตรวจสอบให้แน่ใจว่า ระบบตรงกับข้อกำหนดที่ระบุไว้
GEN005590	2	ระบบต้องไม่รัน daemons โปรโตคอลการเราต์ใดๆ ยกเว้นระบบคือเราเตอร์	**ตำแหน่ง** `/etc/security/pscexpert/dodv2/dodv2cmntrows` **แอ็คชันความเข้ากันได้** ตรวจสอบให้แน่ใจว่า ระบบตรงกับข้อกำหนดที่ระบุไว้
GEN005600	2	การส่งต่อ IP สำหรับ IPv4 ต้องไม่เปิดใช้งาน ยกเว้นว่าระบบคือเราเตอร์	**ตำแหน่ง** `/etc/security/pscexpert/dodv2/ntwkoptsdod` **แอ็คชันความเข้ากันได้** ตั้งค่าอ็อพชันเครือข่าย `ipforwarding` เป็น *0*

ตารางที่ 2. 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` **แอ็คชันความเข้ากันได้** ตั้งค่าอ็อพชันเครือข่าย `ip6forwarding` เป็น *1*
GEN005820	2	NFS anonymous UID และ GID ต้องถูกกำหนดคอนฟิก เป็นค่าที่ไม่มีการให้สิทธิ์	**ตำแหน่ง** `/etc/security/pscexpert/dodv2/nfsoptions` **แอ็คชันความเข้ากันได้** ตรวจสอบให้แน่ใจว่า ID ที่ระบุไว้ไม่มีการให้สิทธิ์
GEN005840	2	เซิร์ฟเวอร์ NFS ต้องถูกกำหนดคอนฟิกไว้เพื่อจำกัด การเข้าถึงระบบไฟล์ไปยังโลคัลโฮสต์	**ตำแหน่ง** `/etc/security/pscexpert/dodv2/nfsoptions` **แอ็คชันความเข้ากันได้** กำหนดคอนฟิกเซิร์ฟเวอร์ NFS เพื่อจำกัดการเข้าถึงโลคัลโฮสต์
GEN005880	2	เซิร์ฟเวอร์ NFS ต้องไม่ได้รับอนุญาตให้ใช้การเข้าถึง root แบบรีโมต	**ตำแหน่ง** `/etc/security/pscexpert/dodv2/nfsoptions` **แอ็คชันความเข้ากันได้** ปิดใช้งานการเข้าถึง root แบบรีโมตบนเซิร์ฟเวอร์ NFS
GEN005900	2	อ็อพชัน *nosuid* ต้องถูกเปิดใช้งานบนไคลเอ็นต์ NFS ที่เมาท์ทั้งหมด	**ตำแหน่ง** `/etc/security/pscexpert/dodv2/nosuid` **แอ็คชันความเข้ากันได้** เปิดใช้งานอ็อพชัน *nosuid* บนไคลเอ็นต์ NFS ที่เมาท์ทั้งหมด
GEN006060	2	ระบบต้องไม่รัน `Samba` ยกเว้นว่าจำเป็น	**ตำแหน่ง** `/etc/security/pscexpert/dodv2/dodv2services` **แอ็คชันความเข้ากันได้** ตรวจสอบให้แน่ใจว่า ระบบตรงกับข้อกำหนดที่ระบุไว้

ตารางที่ 2. 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` **แอ็คชันความเข้ากันได้** แสดงผลลัพธ์ของการทดสอบกฎที่ระบุเฉพาะ
GEN006400	2	โปรโตคอล Network Information System (NIS) ต้องไม่ถูกใช้	**ตำแหน่ง** `/etc/security/pscexpert/dodv2/nisplus` **แอ็คชันความเข้ากันได้** ปิดใช้งานโปรโตคอลที่ระบุเฉพาะ **หมายเหตุ:** ค่าติดตั้งนี้ไม่ได้ถูกเปลี่ยนโดยอัตโนมัติเมื่อรีเซ็ตนโยบายเป็น นโยบายดีฟอลต์ของ AIX โดยใช้ไฟล์ `DoDv2_to_AIXDefault.xml` คุณต้องเปลี่ยนค่าติดตั้งนี้แบบแมนวล
GEN006420	2	แม็พ NIS ต้องได้รับการปกป้องโดยใช้โดเมนเนมแบบ ยากที่จะเดา	**ตำแหน่ง** `/etc/security/pscexpert/dodv2/nisplus` **แอ็คชันความเข้ากันได้** ตรวจสอบให้แน่ใจว่า โดเมนเนมยากที่จะกำหนดได้
GEN006460	2	เซิร์ฟเวอร์ NIS+ ใดๆ ต้องทำงานที่ความปลอดภัยระดับ 2	**ตำแหน่ง** `/etc/security/pscexpert/dodv2/nisplus` **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` **แอ็คชันความเข้ากันได้** ตรวจสอบทุกสัปดาห์เพื่อระบุความเปลี่ยนแปลงกับไฟล์ ที่ระบุไว้

ตารางที่ 2. 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` **แอ็คชันความเข้ากันได้** ตรวจสอบทุกสัปดาห์เพื่อระบุความเปลี่ยนแปลงกับไฟล์ที่ระบุไว้
GEN006580	2	ระบบต้องใช้โปรแกรมควบคุมการเข้าถึง	**ตำแหน่ง** `/etc/security/pscexpert/dodv2/checktcpd` **แอ็คชันความเข้ากันได้** ตรวจสอบให้แน่ใจว่า ระบบตรงกับข้อกำหนดที่ระบุไว้
GEN006600	2	โปรแกรมควบคุมการเข้าถึงของระบบ ต้องจดบันทึกความพยายามในการเข้าถึงระบบแต่ละครั้ง	**ตำแหน่ง** `/etc/security/pscexpert/dodv2/chsyslogdod` **แอ็คชันความเข้ากันได้** ตรวจสอบให้แน่ใจว่าความพยายามในการเข้าถึงถูกจดบันทึกแล้ว
GEN006620	2	โปรแกรมควบคุมการเข้าถึงของระบบ ต้องถูกกำหนดคอนฟิกไว้เพื่อให้สิทธิ์หรือปฏิเสธระบบในการเข้าถึงโฮสต์ที่ระบุเฉพาะ	**ตำแหน่ง** `/etc/security/pscexpert/dodv2/chetchostsdod` **แอ็คชันความเข้ากันได้** กำหนดคอนฟิกไฟล์ `hosts.deny` และ `hosts.allow` เป็นค่าติดตั้งที่จำเป็น
GEN007020	2	Stream Control Transmission Protocol (SCTP) ต้องถูกปิดใช้งาน	**ตำแหน่ง** `/etc/security/pscexpert/dodv2/dodv2netrules` **แอ็คชันความเข้ากันได้** ปิดใช้งานโปรโตคอลที่ระบุเฉพาะ

ตารางที่ 2. 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` **แอ็คชันความเข้ากันได้** ปิดใช้งานตัวจัดการโปรโตคอล IPv6 จากสแต็กเครือข่าย ยกเว้นว่าโปรแกรมจัดการถูกระบุอยู่ในไฟล์ `/etc/ipv6.conf` **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` **แอ็คชันความเข้ากันได้** ปิดใช้งานท่อที่ระบุไว้ **หมายเหตุ:** ค่าติดตั้งนี้ไม่ได้ถูกเปลี่ยนโดยอัตโนมัติเมื่อรีเซ็ตนโยบายเป็น นโยบายดีฟอลต์ของ AIX โดยใช้ไฟล์ `DoDv2_to_AIXDefault.xml` คุณต้องเปลี่ยนค่าติดตั้งนี้แบบแมนวล
GEN007820	2	ระบบต้องไม่มี IP ที่ถูกกำหนดคอนฟิกไว้	**ตำแหน่ง** `/etc/security/pscexpert/dodv2/rmtunnel` **แอ็คชันความเข้ากันได้** ปิดใช้งานท่อ IP **หมายเหตุ:** ค่าติดตั้งนี้ไม่ได้ถูกเปลี่ยนโดยอัตโนมัติเมื่อรีเซ็ตนโยบายเป็น นโยบายดีฟอลต์ของ AIX โดยใช้ไฟล์ `DoDv2_to_AIXDefault.xml` คุณต้องเปลี่ยนค่าติดตั้งนี้แบบแมนวล

ตารางที่ 2. 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` **แอ็คชันความเข้ากันได้** ตรวจสอบให้แน่ใจว่า ระบบตรงกับข้อกำหนดที่ระบุไว้
GEN007850	2	ไคลเอ็นต์ DHCP ต้องไม่ส่งอัพเดต DNS แบบไดนามิก	**ตำแหน่ง** `/etc/security/pscexpert/dodv2/dodv2services` **แอ็คชันความเข้ากันได้** ตรวจสอบให้แน่ใจว่า ระบบตรงกับข้อกำหนดที่ระบุไว้
GEN007860	2	ระบบต้องละเว้นข้อความการเปลี่ยนทิศทาง IPv6 ICMP	**ตำแหน่ง** `/etc/security/pscexpert/dodv2/ntwkoptsdod` **แอ็คชันความเข้ากันได้** ตั้งค่าอ็อพชันเครือข่าย `ipignoreredirects` เป็น *1*
GEN007880	2	ระบบต้องไม่ส่งการเปลี่ยนทิศทาง IPv6 ICMP	**ตำแหน่ง** `/etc/security/pscexpert/dodv2/ntwkoptsdod` **แอ็คชันความเข้ากันได้** ตั้งค่าอ็อพชันเครือข่าย `ipsendredirects` เป็น *0*
GEN007900	2	ระบบต้องใช้ตัวกรอง reverse-path สำหรับทราฟฟิกเครือข่าย IPv6 หากระบบใช้ IPv6	**ตำแหน่ง** `/etc/security/pscexpert/dodv2/chuserstanzadod` **แอ็คชันความเข้ากันได้** ตรวจสอบให้แน่ใจว่า ระบบตรงกับข้อกำหนดที่ระบุไว้
GEN007920	2	ระบบต้องไม่ส่งต่อแพ็กเก็ตที่เราต์แหล่งที่มา IPv6	**ตำแหน่ง** `/etc/security/pscexpert/dodv2/ntwkoptsdod` **แอ็คชันความเข้ากันได้** ตั้งค่าอ็อพชันเครือข่าย `ip6srcrouteforward` เป็น *0*

ตารางที่ 2. 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` **แอ็คชันความเข้ากันได้** ตั้งค่าอ็อพชันเครือข่าย `ipsrcrouterecv` เป็น *0*
GEN007950	2	ระบบต้องไม่ตอบสนองต่อคำร้องขอ ICMPv6 echo ที่ส่งไปยังแอดเดรสบอร์ดคาสก์	**ตำแหน่ง** `/etc/security/pscexpert/dodv2/ntwkoptsdod` **แอ็คชันความเข้ากันได้** 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` **แอ็คชันความเข้ากันได้** ตรวจสอบให้แน่ใจว่า ระบบตรงกับข้อกำหนดที่ระบุไว้
GEN008020	2	ถ้าระบบกำลังใช้ LDAP สำหรับการพิสูจน์ตัวตน หรือข้อมูลแอคเคาต์ การเชื่อมต่อ LDAP Transport Layer Security (TLS) ต้องการให้เซิร์ฟเวอร์จัดเตรียมใบรับรองที่มีพาธที่เชื่อถือได้ที่ถูกต้อง	**ตำแหน่ง** `/etc/security/pscexpert/dodv2/ldap_config` **แอ็คชันความเข้ากันได้** ตรวจสอบให้แน่ใจว่า ระบบตรงกับข้อกำหนดที่ระบุไว้
GEN008050	2	ถ้าระบบกำลังใช้ LDAP สำหรับการพิสูจน์ตัวตน หรือข้อมูลแอคเคาต์ ไฟล์ `/etc/ldap.conf` (หรือเทียบเท่า) ต้องไม่มีรหัสผ่าน	**ตำแหน่ง** `/etc/security/pscexpert/dodv2/ldap_config` **แอ็คชันความเข้ากันได้** ตรวจสอบให้แน่ใจว่า ระบบตรงกับข้อกำหนดที่ระบุไว้
GEN008380	2	ระบบต้องถูกตรวจสอบทุกสัปดาห์สำหรับไฟล์ `setuid` ที่ไม่ได้รับสิทธิ์ และโมดิฟิเคชันที่ไม่ได้รับสิทธิ์เพื่อให้สิทธิ์กับไฟล์ `setuid`	**ตำแหน่ง** `/etc/security/pscexpert/dodv2/trust` **แอ็คชันความเข้ากันได้** ตรวจสอบทุกสัปดาห์เพื่อระบุความเปลี่ยนแปลงกับไฟล์ ที่ระบุไว้

ตารางที่ 2. 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` **แอ็คชันความเข้ากันได้** ตรวจสอบให้แน่ใจว่า ระบบตรงกับข้อกำหนดที่ระบุไว้
GEN008540	2	ไฟร์วอลล์โลคัลของระบบต้องใช้นโยบาย *deny-all*, *allow-by-exception*	**ตำแหน่ง** `/etc/security/pscexpert/dodv2/ipsecshunhosthls` **แอ็คชันความเข้ากันได้** ตรวจสอบให้แน่ใจว่า ระบบตรงกับข้อกำหนดที่ระบุไว้ **หมายเหตุ:** คุณสามารถ ป้อนกฎการกรองเพิ่มเติมในไฟล์ `/etc/security/aixpert/bin/filter.txt` กฎเหล่านี้ ถูกรวมไว้โดยสคริปต์ `ipsecshunhosthls.sh` เมื่อคุณใช้โปรไฟล์ รายการต่างๆ ควรอยู่ในรูปแบบ ต่อไปนี้: *`port_number`*`:`*`ip_address`*`:`*`action`* โดยที่ ค่าที่อาจเกิดขึ้นได้สำหรับ *action* คือ `Allow` หรือ `Deny`
GEN008600	1	ระบบต้องถูกกำหนดคอนฟิกไว้เพื่อเริ่มต้นจาก คอนฟิกูเรชันบูตระบบ	**ตำแหน่ง** `/etc/security/pscexpert/dodv2/dodv2cat1` **แอ็คชันความเข้ากันได้** ตรวจสอบให้แน่ใจว่าการเริ่มต้นระบบใช้คอนฟิกูเรชันบูตระบบ เท่านั้น
GEN008640	1	ระบบต้องไม่ใช้สื่อบันทึกที่สามารถถอดออกได้ เป็นโหลดเดอร์บูต	**ตำแหน่ง** `/etc/security/pscexpert/dodv2/dodv2cat1` **แอ็คชันความเข้ากันได้** ตรวจสอบให้แน่ใจว่า ระบบไม่ได้บูตจากไดรฟ์ที่สามารถถอดออกได้

ตารางที่ 2. 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 **แอ็คชันความเข้ากันได้** ปิดใช้งาน daemons และเซอร์ที่จำเป็นโดยใส่คอมเมนต์ รายการในไฟล์ /etc/inetd.conf
GEN009160	1,2,3	ระบบต้องไม่มีเซอร์วิส Calendar Management Service Daemon (CMSD) ที่แอ็คทีฟ	**ตำแหน่ง** /etc/security/pscexpert/dodv2/inetdservices **แอ็คชันความเข้ากันได้** ปิดใช้งาน daemons และเซอร์ที่จำเป็นโดยใส่คอมเมนต์ รายการในไฟล์ /etc/inetd.conf
GEN009180	1,2,3	ระบบต้องไม่มีเซอร์วิส tool-talk database server (ttdbserver) ที่แอ็คทีฟ	**ตำแหน่ง** /etc/security/pscexpert/dodv2/inetdservices **แอ็คชันความเข้ากันได้** ปิดใช้งาน daemons และเซอร์ที่จำเป็นโดยใส่คอมเมนต์ รายการในไฟล์ /etc/inetd.conf
GEN009190	1,2,3	ระบบต้องไม่มีเซอร์วิส comsat ที่แอ็คทีฟ	**ตำแหน่ง** /etc/security/pscexpert/dodv2/inetdservices **แอ็คชันความเข้ากันได้** ปิดใช้งาน daemons และเซอร์ที่จำเป็นโดยใส่คอมเมนต์ รายการในไฟล์ /etc/inetd.conf
GEN009200-9330	1,2,3	ระบบไม่สามารถมีเซอร์วิสอื่นๆ และ daemons ที่แอ็คทีฟ	**ตำแหน่ง** /etc/security/pscexpert/dodv2/inetdservices **แอ็คชันความเข้ากันได้** ปิดใช้งาน daemons และเซอร์ที่จำเป็นโดยใส่คอมเมนต์ รายการในไฟล์ /etc/inetd.conf
GEN009210	2	ระบบต้องไม่มีเซอร์วิส discard ที่แอ็คทีฟ	**ตำแหน่ง** /etc/security/pscexpert/dodv2/inetdservices **แอ็คชันความเข้ากันได้** ปิดใช้งาน daemons และเซอร์ที่จำเป็นโดยใส่คอมเมนต์ รายการในไฟล์ /etc/inetd.conf

ตารางที่ 2. 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 **แอ็คชันความเข้ากันได้** ปิดใช้งาน daemons และเซอร์ที่จำเป็นโดยใส่คอมเมนต์ รายการในไฟล์ /etc/inetd.conf
GEN009230	2	ระบบต้องไม่มีเซอร์วิส echo ที่แอ็คทีฟ	**ตำแหน่ง** /etc/security/pscexpert/dodv2/inetdservices **แอ็คชันความเข้ากันได้** ปิดใช้งาน daemons และเซอร์ที่จำเป็นโดยใส่คอมเมนต์ รายการในไฟล์ /etc/inetd.conf
GEN009240	2	ระบบต้องไม่มีเซอร์วิส Internet Message Access Protocol (IMAP) ที่แอ็คทีฟ	**ตำแหน่ง** /etc/security/pscexpert/dodv2/inetdservices **แอ็คชันความเข้ากันได้** ปิดใช้งาน daemons และเซอร์ที่จำเป็นโดยใส่คอมเมนต์ รายการในไฟล์ /etc/inetd.conf
GEN009250	2	ระบบต้องไม่มีเซอร์วิส PostOffice Protocol (POP3) ที่แอ็คทีฟ	**ตำแหน่ง** /etc/security/pscexpert/dodv2/inetdservices **แอ็คชันความเข้ากันได้** ปิดใช้งาน daemons และเซอร์ที่จำเป็นโดยใส่คอมเมนต์ รายการในไฟล์ /etc/inetd.conf
GEN009260	2	ระบบต้องไม่มีเซอร์วิส talk หรือ ntalk ที่แอ็คทีฟ	**ตำแหน่ง** /etc/security/pscexpert/dodv2/inetdservices **แอ็คชันความเข้ากันได้** ปิดใช้งาน daemons และเซอร์ที่จำเป็นโดยใส่คอมเมนต์ รายการในไฟล์ /etc/inetd.conf
GEN009270	2	ระบบต้องไม่มีเซอร์วิส netstat ที่แอ็คทีฟบนกระบวนการ InetD	**ตำแหน่ง** /etc/security/pscexpert/dodv2/inetdservices **แอ็คชันความเข้ากันได้** ปิดใช้งาน daemons และเซอร์ที่จำเป็นโดยใส่คอมเมนต์ รายการในไฟล์ /etc/inetd.conf

ตารางที่ 2. 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 **แอ็คชันความเข้ากันได้** ปิดใช้งาน daemons และเซอร์ที่จำเป็นโดยใส่คอมเมนต์ รายการในไฟล์ /etc/inetd.conf
GEN009290	2	ระบบต้องไม่มีเซอร์วิส systat ที่แอ็คทีฟ	**ตำแหน่ง** /etc/security/pscexpert/dodv2/inetdservices **แอ็คชันความเข้ากันได้** ปิดใช้งาน daemons และเซอร์ที่จำเป็นโดยใส่คอมเมนต์ รายการในไฟล์ /etc/inetd.conf
GEN009300	2	เซอร์วิส inetd time ต้อไม่แอ็คทีฟบนระบบบน inetd daemon	**ตำแหน่ง** /etc/security/pscexpert/dodv2/inetdservices **แอ็คชันความเข้ากันได้** ปิดใช้งาน daemons และเซอร์ที่จำเป็นโดยใส่คอมเมนต์ รายการในไฟล์ /etc/inetd.conf
GEN009310	2	ระบบต้องไม่มีเซอร์วิส rusersd ที่แอ็คทีฟ	**ตำแหน่ง** /etc/security/pscexpert/dodv2/inetdservices **แอ็คชันความเข้ากันได้** ปิดใช้งาน daemons และเซอร์ที่จำเป็นโดยใส่คอมเมนต์ รายการในไฟล์ /etc/inetd.conf
GEN009320	2	ระบบต้องไม่มีเซอร์วิส sprayd ที่แอ็คทีฟ	**ตำแหน่ง** /etc/security/pscexpert/dodv2/inetdservices **แอ็คชันความเข้ากันได้** ปิดใช้งาน daemons และเซอร์ที่จำเป็นโดยใส่คอมเมนต์ รายการในไฟล์ /etc/inetd.conf
GEN009330	2	ระบบต้องไม่มีเซอร์วิส rstatd ที่แอ็คทีฟ	**ตำแหน่ง** /etc/security/pscexpert/dodv2/inetdservices **แอ็คชันความเข้ากันได้** ปิดใช้งาน daemons และเซอร์ที่จำเป็นโดยใส่คอมเมนต์ รายการในไฟล์ /etc/inetd.conf

ตารางที่ 2. 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` **แอ็คชันความเข้ากันได้** กฎนี้ปิดใช้งานการเชื่อมต่อ X Window System และโปรแกรมจัดการการล็อกอิน XServer

ตารางที่ 3. ข้อกำหนดความเป็นเจ้าของ DoD

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

ตารางที่ 3. 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 **แอ็คชันความเข้ากันได้** ตรวจสอบให้แน่ใจว่า ไฟล์ที่ระบุไว้เป็นเจ้าของแบบกลุ่ม bin, sys หรือระบบ
GEN001160	ไฟล์และไดเร็กทอรีทั้งหมดต้องมี เจ้าของที่ถูกต้อง	**ตำแหน่ง** /etc/security/pscexpert/dodv2/chowndodfiles **แอ็คชันความเข้ากันได้** ตรวจสอบให้แน่ใจว่า ไฟล์และไดเร็กทอรีทั้งหมดมีเจ้าของที่ถูกต้อง
GEN001170	ไฟล์และไดเร็กทอรีทั้งหมดต้องมีเจ้าของกลุ่ม ที่ถูกต้อง	**ตำแหน่ง** /etc/security/pscexpert/dodv2/chowndodfiles **แอ็คชันความเข้ากันได้** ตรวจสอบให้แน่ใจว่า ไฟล์และไดเร็กทอรีทั้งหมดมีเจ้าของที่ถูกต้อง
GEN001220	ไฟล์ของระบบ โปรแกรม และไดเร็กทอรีทั้งหมด ต้องเป็นเจ้าของโดยแอคเคาต์ระบบ	**ตำแหน่ง** /etc/security/pscexpert/dodv2/chowndodfiles **แอ็คชันความเข้ากันได้** ตรวจสอบให้แน่ใจว่า ระบบไฟล์ โปรแกรม และไดเร็กทอรี เป็นเจ้าของโดยแอคเคาต์ระบบ
GEN001240	ระบบไฟล์ โปแกรม และไดเร็กทอรี ต้องเป็นเจ้าของแบบกลุ่มโดยกลุ่มของระบบ	**ตำแหน่ง** /etc/security/pscexpert/dodv2/chowndodfiles **แอ็คชันความเข้ากันได้** ระบบไฟล์ โปรแกรม และไดเร็กทอรีทั้งหมดต้องเป็นเจ้าของแบบกลุ่มโดย กลุ่มของระบบ
GEN001320	ไฟล์ Network Information Systems (NIS)/NIS+/yp ต้องเป็นเจ้าของโดย root, sys หรือ bin	**ตำแหน่ง** /etc/security/pscexpert/dodv2/chowndodfiles **แอ็คชันความเข้ากันได้** ตรวจสอบให้แน่ใจว่า ไฟล์ที่ระบุไว้เป็นเจ้าของโดย root, sys หรือ bin

ตารางที่ 3. 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` **แอ็คชันความเข้ากันได้** ตรวจสอบให้แน่ใจว่า ไฟล์ที่ระบุไว้เป็นเจ้าของโดย sys, bin, other หรือระบบ
GEN001362	ไฟล์ `/etc/resolv.conf` ต้องเป็นเจ้าของโดย root	**ตำแหน่ง** `/etc/security/pscexpert/dodv2/chowndodfiles` **แอ็คชันความเข้ากันได้** ตรวจสอบให้แน่ใจว่าไฟล์ที่ระบุไว้เป็นเจ้าของโดย root
GEN001363	ไฟล์ `/etc/resolv.conf` ต้องเป็นเจ้าของแบบกลุ่มโดย bin, sys หรือระบบ	**ตำแหน่ง** `/etc/security/pscexpert/dodv2/chowndodfiles` **แอ็คชันความเข้ากันได้** ตรวจสอบให้แน่ใจว่า ไฟล์ที่ระบุไว้เป็นเจ้าของแบบกลุ่ม bin, sys หรือระบบ
GEN001366	ไฟล์ `/etc/hosts` ต้องเป็นเจ้าของโดย root	**ตำแหน่ง** `/etc/security/pscexpert/dodv2/chowndodfiles` **แอ็คชันความเข้ากันได้** ตรวจสอบให้แน่ใจว่าไฟล์ที่ระบุไว้เป็นเจ้าของโดย root
GEN001367	ไฟล์ `/etc/hosts` ต้องเป็นเจ้าของแบบกลุ่มโดย bin, sys หรือระบบ	**ตำแหน่ง** `/etc/security/pscexpert/dodv2/chowndodfiles` **แอ็คชันความเข้ากันได้** ตรวจสอบให้แน่ใจว่า ไฟล์ที่ระบุไว้เป็นเจ้าของแบบกลุ่ม bin, sys หรือระบบ
GEN001371	ไฟล์ `/etc/nsswitch.conf` ต้องเป็นเจ้าของโดย root	**ตำแหน่ง** `/etc/security/pscexpert/dodv2/chowndodfiles` **แอ็คชันความเข้ากันได้** ตรวจสอบให้แน่ใจว่าไฟล์ที่ระบุไว้เป็นเจ้าของโดย root
GEN001372	ไฟล์ `/etc/nsswitch.conf` ต้องเป็นเจ้าของแบบกลุ่มโดย root, bin, sys หรือระบบ	**ตำแหน่ง** `/etc/security/pscexpert/dodv2/chowndodfiles` **แอ็คชันความเข้ากันได้** ตรวจสอบให้แน่ใจว่า ไฟล์ที่ระบุไว้เป็นเจ้าของแบบกลุ่มโดย root, bin, sys หรือระบบ

ตารางที่ 3. ข้อกำหนดความเป็นเจ้าของ DoD (ต่อ)

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

ตารางที่ 3. ข้อกำหนดความเป็นเจ้าของ DoD (ต่อ)

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

ตารางที่ 3. ข้อกำหนดความเป็นเจ้าของ DoD (ต่อ)

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

ตารางที่ 3. 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 **แอ็คชันความเข้ากันได้** ตรวจสอบให้แน่ใจว่า ไฟล์ที่ระบุไว้ไม่พร้อมใช้งานโดยใช้ PAM
GEN002200	ไฟล์เชลล์ทั้งหมดต้องเป็นเจ้าของ root หรือ bin	**ตำแหน่ง** /etc/security/pscexpert/dodv2/chowndodfiles **แอ็คชันความเข้ากันได้** ตรวจสอบให้แน่ใจว่า ไฟล์ที่ระบุไว้เป็นเจ้าของ root หรือ bin
GEN002210	ไฟล์เชลล์ทั้งหมดต้องเป็นเจ้าของแบบกลุ่มโดย root, bin, sys หรือระบบ	**ตำแหน่ง** /etc/security/pscexpert/dodv2/chowndodfiles **แอ็คชันความเข้ากันได้** ตรวจสอบให้แน่ใจ ไฟล์ที่ระบุไว้เป็นเจ้าของแบบกลุ่มโดย root, bin, sys หรือระบบ
GEN002340	อุปกรณ์ออดิโอต้องเป็นเจ้าของโดย root	**ตำแหน่ง** /etc/security/pscexpert/dodv2/chowndodfiles **แอ็คชันความเข้ากันได้** ตรวจสอบให้แน่ใจว่า อุปกรณ์ออดิโอทั้งหมดเป็นเจ้าของโดย root
GEN002360	อุปกรณ์ออดิโอต้องเป็นเจ้าของแบบกลุ่มโดย root, sys, bin หรือระบบ	**ตำแหน่ง** /etc/security/pscexpert/dodv2/chowndodfiles **แอ็คชันความเข้ากันได้** ตรวจสอบให้แน่ใจว่า อุปกรณ์ออดิโอทั้งหมดเป็นเจ้าของแบบกลุ่มโดย root, sys, bin หรือระบบ
GEN002520	ไดเร็กทอรีพับลิกทั้งหมดต้องเป็นเจ้าของโดย root หรือแอคเคาต์แอ็พพลิเคชัน	**ตำแหน่ง** /etc/security/pscexpert/dodv2/chowndodfiles **แอ็คชันความเข้ากันได้** ตรวจสอบให้แน่ใจว่า ไดเร็กทอรีพับลิกทั้งหมดเป็นเจ้าของโดย root หรือแอคเคาต์ แอ็พพลิเคชัน

ตารางที่ 3. ข้อกำหนดความเป็นเจ้าของ DoD (ต่อ)

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

ตารางที่ 3. ข้อกำหนดความเป็นเจ้าของ DoD (ต่อ)

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

ตารางที่ 3. 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` **แอ็คชันความเข้ากันได้** ตรวจสอบให้แน่ใจว่า ไฟล์ที่ระบุไว้เป็นเจ้าของแบบกลุ่มโดยระบบ, bin, sys หรือ cron
GEN003420	ไดเร็กทอรี `at` ต้องเป็นเจ้าของโดย root, bin, sys, daemon หรือ cron	**ตำแหน่ง** `/etc/security/pscexpert/dodv2/chowndodfiles` **แอ็คชันความเข้ากันได้** ตรวจสอบให้แน่ใจว่า ไดเร็กทอรีที่ระบุไว้เป็นเจ้าของโดย root, sys, daemon หรือ cron
GEN003430	ไดเร็กทอรี `at` ต้องเป็นเจ้าของแบบกลุ่มโดยระบบ, bin, sys หรือ cron	**ตำแหน่ง** `/etc/security/pscexpert/dodv2/chowndodfiles` **แอ็คชันความเข้ากันได้** ตรวจสอบให้แน่ใจว่า ไดเร็กทอรีที่ระบุไว้เป็นเจ้าของแบบกลุ่มโดยระบบ, bin, sys หรือ cron
GEN003460	ไฟล์ `at.allow` ต้องเป็นเจ้าของโดย root, bin หรือ sys	**ตำแหน่ง** `/etc/security/pscexpert/dodv2/chowndodfiles` **แอ็คชันความเข้ากันได้** ตรวจสอบให้แน่ใจว่า ไฟล์ที่ระบุไว้เป็นเจ้าของโดย root, bin หรือ sys
GEN003470	ไฟล์ `at.allow` ต้องเป็นเจ้าของแบบกลุ่มโดยระบบ bin, sys หรือ cron	**ตำแหน่ง** `/etc/security/pscexpert/dodv2/chowndodfiles` **แอ็คชันความเข้ากันได้** ตรวจสอบให้แน่ใจว่า ไฟล์ที่ระบุไว้เป็นเจ้าของแบบกลุ่มโดยระบบ, bin, sys หรือ cron
GEN003480	ไฟล์ `at.deny` ต้องเป็นเจ้าของโดย root, bin หรือ sys	**ตำแหน่ง** `/etc/security/pscexpert/dodv2/chowndodfiles` **แอ็คชันความเข้ากันได้** ตรวจสอบให้แน่ใจว่า ไฟล์ที่ระบุไว้เป็นเจ้าของโดย root, bin หรือ sys

ตารางที่ 3. 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` **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` **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` **แอ็คชันความเข้ากันได้** ตรวจสอบให้แน่ใจว่า ไฟล์และไดเร็กทอรีที่ระบุไว้เป็นเจ้าของแบบกลุ่มโดย bin, sys หรือระบบ
GEN003760	ไฟล์ `services` ต้องเป็นเจ้าของโดย root หรือ bin	**ตำแหน่ง** `/etc/security/pscexpert/dodv2/chowndodfiles` **แอ็คชันความเข้ากันได้** ตรวจสอบให้แน่ใจว่า ไฟล์ที่ระบุไว้เป็นเจ้าของโดย root หรือ bin
GEN003770	ไฟล์ `services` ต้องเป็น เจ้าของแบบกลุ่มโดย bin, sys หรือระบบ	**ตำแหน่ง** `/etc/security/pscexpert/dodv2/chowndodfiles` **แอ็คชันความเข้ากันได้** ตรวจสอบให้แน่ใจว่า ไฟล์ที่ระบุไว้เป็นเจ้าของแบบกลุ่ม bin, sys หรือระบบ
GEN003920	ไฟล์ `hosts.lpd` (หรือเทียบเท่า) ต้องเป็นเจ้าของโดย root, bin, sys หรือ lp	**ตำแหน่ง** `/etc/security/pscexpert/dodv2/chowndodfiles` **แอ็คชันความเข้ากันได้** ตรวจสอบให้แน่ใจว่า ไฟล์ที่ระบุไว้เป็นเจ้าของโดย root, bin, sys หรือ lp

ตารางที่ 3. 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` **แอ็คชันความเข้ากันได้** ตรวจสอบให้แน่ใจว่า ไฟล์ที่ระบุไว้เป็นเจ้าของแบบกลุ่ม bin, sys หรือระบบ
GEN003960	เจ้าของคำสั่ง **traceroute** ต้องเป็น root	**ตำแหน่ง** `/etc/security/pscexpert/dodv2/chowndodfiles` **แอ็คชันความเข้ากันได้** ตรวจสอบให้แน่ใจว่า เจ้าของคำสั่งเป็น root
GEN003980	คำสั่ง **traceroute** ต้องเป็นเจ้าของแบบกลุ่ม โดย sys, bin หรือระบบ	**ตำแหน่ง** `/etc/security/pscexpert/dodv2/chowndodfiles` **แอ็คชันความเข้ากันได้** ตรวจสอบให้แน่ใจว่า คำสั่งเป็นเจ้าของแบบกลุ่มโดย sys, bin หรือระบบ
GEN004360	ไฟล์ `alias` ต้องเป็นเจ้าของโดย root	**ตำแหน่ง** `/etc/security/pscexpert/dodv2/chowndodfiles` **แอ็คชันความเข้ากันได้** ตรวจสอบให้แน่ใจว่าไฟล์ที่ระบุไว้เป็นเจ้าของโดย root
GEN004370	ไฟล์ `aliases` ต้องเป็นเจ้าของแบบกลุ่มโดย sys, bin หรือระบบ	**ตำแหน่ง** `/etc/security/pscexpert/dodv2/chowndodfiles` **แอ็คชันความเข้ากันได้** ตรวจสอบให้แน่ใจว่า ไฟล์ที่ระบุไว้เป็นเจ้าของกลุ่มโดย sys, bin หรือระบบ
GEN004400	ไฟล์ที่รันผ่านไฟล์ `aliases` ต้องเป็นเจ้าของโดย root และต้องอยู่ภายในไดเร็กทอรีที่เป็นเจ้าของ และสามารถเขียนได้โดย root เท่านั้น	**ตำแหน่ง** `/etc/security/pscexpert/dodv2/chowndodfiles` **แอ็คชันความเข้ากันได้** ตรวจสอบให้แน่ใจว่า ไฟล์ต่างๆ ถูกรันผ่านไฟล์เมล `aliases` เป็นเจ้าของโดย root และต้องอยู่ภายในไดเร็กทอรีที่เป็นเจ้าของ และสามารถเขียนได้โดย root เท่านั้น

ตารางที่ 3. 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` **แอ็คชันความเข้ากันได้** 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` **แอ็คชันความเข้ากันได้** ตรวจสอบให้แน่ใจว่าไฟล์ที่ระบุไว้เป็นเจ้าของโดย root
GEN004920	ไฟล์ `ftpusers` ต้องเป็นเจ้าของโดย root	**ตำแหน่ง** `/etc/security/pscexpert/dodv2/chowndodfiles` **แอ็คชันความเข้ากันได้** ตรวจสอบให้แน่ใจว่าไฟล์ที่ระบุไว้เป็นเจ้าของโดย root
GEN004930	ไฟล์ `ftpusers` ต้องเป็นเจ้าของแบบกลุ่มตาม bin, sys หรือระบบ	**ตำแหน่ง** `/etc/security/pscexpert/dodv2/chowndodfiles` **แอ็คชันความเข้ากันได้** ตรวจสอบให้แน่ใจว่า ไฟล์ที่ระบุไว้เป็นเจ้าของแบบกลุ่ม bin, sys หรือระบบ
GEN005360	ไฟล์ `snmpd.conf` ต้องเป็นเจ้าของโดย root	**ตำแหน่ง** `/etc/security/pscexpert/dodv2/chowndodfiles` **แอ็คชันความเข้ากันได้** ตรวจสอบให้แน่ใจว่าไฟล์ที่ระบุไว้เป็นเจ้าของโดย root
GEN005365	ไฟล์ `snmpd.conf` ต้องเป็นเจ้าของแบบกลุ่มโดย bin, sys หรือระบบ	**ตำแหน่ง** `/etc/security/pscexpert/dodv2/chowndodfiles` **แอ็คชันความเข้ากันได้** ตรวจสอบให้แน่ใจว่า ไฟล์ที่ระบุไว้เป็นเจ้าของแบบกลุ่ม bin, sys หรือระบบ
GEN005400	ไฟล์ `/etc/syslog.conf` ต้องเป็นเจ้าของโดย root	**ตำแหน่ง** `/etc/security/pscexpert/dodv2/chowndodfiles` **แอ็คชันความเข้ากันได้** ตรวจสอบให้แน่ใจว่าไฟล์ที่ระบุไว้เป็นเจ้าของโดย root

ตารางที่ 3. 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 **แอ็คชันความเข้ากันได้** ตรวจสอบให้แน่ใจว่า ไฟล์ที่ระบุไว้เป็นเจ้าของแบบกลุ่ม bin, sys หรือระบบ
GEN005610	ระบบต้องไม่มีการส่งต่อ IP สำหรับ IPv6 ที่เปิดใช้งาน ยกเว้นว่าระบบเป็นเราเตอร์ IPv6	**ตำแหน่ง** /etc/security/pscexpert/dodv2/chowndodfiles **แอ็คชันความเข้ากันได้** ตรวจสอบให้แน่ใจว่า การส่งต่อ IP สำหรับ IPv6 ต้องไม่เปิดใช้งาน ยกเว้นว่า ระบบต้องถูกใช้เป็นเราเตอร์ IPv6
GEN005740	ไฟล์คอนฟิกูเรชันเอ็กซ์พอร์ต NFS ต้องเป็นเจ้าของโดย root	**ตำแหน่ง** /etc/security/pscexpert/dodv2/chowndodfiles **แอ็คชันความเข้ากันได้** ตรวจสอบให้แน่ใจว่าไฟล์ที่ระบุไว้เป็นเจ้าของโดย root
GEN005750	ไฟล์คอนฟิกูเรชันเอ็กซ์พอร์ต NFS ต้องเป็นเจ้าของแบบกลุ่มโดย root, bin, sys หรือระบบ	**ตำแหน่ง** /etc/security/pscexpert/dodv2/chowndodfiles **แอ็คชันความเข้ากันได้** ตรวจสอบให้แน่ใจว่า ไฟล์ที่ระบุไว้เป็นเจ้าของแบบกลุ่มโดย root, bin, sys หรือระบบ
GEN005800	ไฟล์ระบบที่เอ็กซ์พอร์ต NFS ทั้งหมดและไดเร็กทอรีระบบ ต้องเป็นเจ้าของโดย root	**ตำแหน่ง** /etc/security/pscexpert/dodv2/chowndodfiles **แอ็คชันความเข้ากันได้** ตรวจสอบให้แน่ใจว่าไฟล์ที่ระบุไว้เป็นเจ้าของโดย root
GEN005810	ไฟล์ระบบที่เอ็กซ์พอร์ต NFS ทั้งหมดและไดเร็กทอรีที่ระบบ ต้องเป็นเจ้าของแบบกลุ่มโดย root, bin, sys หรือระบบ	**ตำแหน่ง** /etc/security/pscexpert/dodv2/chowndodfiles **แอ็คชันความเข้ากันได้** ตรวจสอบให้แน่ใจว่า ไฟล์และไดเร็กทอรีที่ระบุไว้เป็นเจ้าของแบบกลุ่มโดย root, bin, sys หรือระบบ
GEN006100	ไฟล์ /usr/lib/smb.conf ต้องเป็นเจ้าของโดย root	**ตำแหน่ง** /etc/security/pscexpert/dodv2/chowndodfiles **แอ็คชันความเข้ากันได้** ตรวจสอบให้แน่ใจว่าไฟล์ที่ระบุไว้เป็นเจ้าของโดย root

ตารางที่ 3. 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 **แอ็คชันความเข้ากันได้** ตรวจสอบให้แน่ใจว่า ไฟล์ที่ระบุไว้เป็นเจ้าของแบบกลุ่ม bin, sys หรือระบบ
GEN006160	ไฟล์ /var/private/smbpasswd ต้องเจ้าของโดย root	**ตำแหน่ง** /etc/security/pscexpert/dodv2/chowndodfiles **แอ็คชันความเข้ากันได้** ตรวจสอบให้แน่ใจว่าไฟล์ที่ระบุไว้เป็นเจ้าของโดย root
GEN006180	ไฟล์ /var/private/smbpasswd ต้องเป็นเจ้าของแบบกลุ่มโดย sys หรือระบบ	**ตำแหน่ง** /etc/security/pscexpert/dodv2/chowndodfiles **แอ็คชันความเข้ากันได้** ตรวจสอบให้แน่ใจว่า ไฟล์ที่ระบุไว้เป็นเจ้าของแบบกลุ่มโดย sys หรือระบบ
GEN006340	ไฟล์ในไดเร็กทอรี /etc/news ต้องเป็นเจ้าของโดย root หรือข่าวสาร	**ตำแหน่ง** /etc/security/pscexpert/dodv2/chowndodfiles **แอ็คชันความเข้ากันได้** ตรวจสอบให้แน่ใจว่า ไดเร็กทอรีที่ระบุไว้เป็นเจ้าของโดย root หรือข่าวสาร
GEN006360	ไฟล์ใน /etc/news ต้องเป็นเจ้าของแบบกลุ่มโดยระบบหรือข่าวสาร	**ตำแหน่ง** /etc/security/pscexpert/dodv2/chowndodfiles **แอ็คชันความเข้ากันได้** ตรวจสอบให้แน่ใจว่า ไฟล์ที่ระบุไว้เป็นเจ้าของแบบกลุ่มโดยระบบหรือ ข่าวสาร
GEN008080	ถ้าระบบกำลังใช้ LDAP สำหรับการพิสูจน์ตัวตน หรือข้อมูลแอคเคาต์ไฟล์ /etc/ldap.conf (หรือ เทียบเท่า) ต้องเป็นเจ้าของโดย root	**ตำแหน่ง** /etc/security/pscexpert/dodv2/chowndodfiles **แอ็คชันความเข้ากันได้** ตรวจสอบให้แน่ใจว่าไฟล์ที่ระบุไว้เป็นเจ้าของโดย root
GEN008100	ถ้าระบบกำลังใช้ LDAP สำหรับการพิสูจน์ตัวตน หรือข้อมูลแอคเคาต์ไฟล์ /etc/ldap.conf (หรือ เทียบเท่า) ต้องเป็นเจ้าของแบบกลุ่มโดยความปลอดภัย, bin, sys หรือระบบ	**ตำแหน่ง** /etc/security/pscexpert/dodv2/chowndodfiles **แอ็คชันความเข้ากันได้** ตรวจสอบให้แน่ใจว่า ไฟล์ที่ระบุไว้เป็นเจ้าของแบบกลุ่ม bin, sys หรือระบบ

ตารางที่ 3. 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` **แอ็คชันความเข้ากันได้** ตรวจสอบให้แน่ใจว่าไฟล์ที่ระบุไว้เป็นเจ้าของโดย root
GEN008160	ถ้าระบบกำลังใช้ LDAP สำหรับการพิสูจน์ตัวตน หรือข้อมูลแอคเคาต์ ไฟล์การออกใบรับรอง TLS หรือไดเร็กทอรี ต้องเป็นเจ้าของแบบกลุ่มโดย root, bin, sys หรือระบบ	**ตำแหน่ง** `/etc/security/pscexpert/dodv2/chowndodfiles` **แอ็คชันความเข้ากันได้** ตรวจสอบให้แน่ใจว่า ไฟล์ที่ระบุไว้เป็นเจ้าของแบบกลุ่ม bin, sys หรือระบบ

ตารางที่ 4. 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` **แอ็คชันความเข้ากันได้** ตรวจสอบให้แน่ใจว่า ไฟล์ที่ถูกตั้งค่าเป็นโหมดการให้สิทธิ์ที่ระบุไว้ หรือเป็นค่าที่ได้รับสิทธิ์น้อย
AIX00340	ไฟล์ `/etc/ftpaccess.ctl` ต้องมีโหมด 0640 หรือโหมดที่ได้รับสิทธิ์น้อย	**ตำแหน่ง** `/etc/security/pscexpert/dodv2/fpmdodfiles` **แอ็คชันความเข้ากันได้** ตรวจสอบให้แน่ใจว่า ไฟล์ที่ถูกตั้งค่าเป็นโหมดการให้สิทธิ์ที่ระบุไว้ หรือเป็นค่าที่ได้รับสิทธิ์น้อย
GEN000252	ไฟล์คอนฟิกูเรชันการซิงโครไนซ์เวลา (เช่น `/etc/ntp.conf`) ต้องมีโหมด 0640 หรือโหมดที่ได้รับสิทธิ์น้อย	**ตำแหน่ง** `/etc/security/pscexpert/dodv2/fpmdodfiles` **แอ็คชันความเข้ากันได้** ตรวจสอบให้แน่ใจว่า ไฟล์ที่ถูกตั้งค่าเป็นโหมดการให้สิทธิ์ที่ระบุไว้ หรือเป็นค่าที่ได้รับสิทธิ์น้อย
GEN000920	โฮมไดเร็กทอรีของแอคเคาต์ root (นอกเหนือจาก /) ต้องมีโหมด 0700	**ตำแหน่ง** `/etc/security/pscexpert/dodv2/fpmdodfiles` **แอ็คชันความเข้ากันได้** ตรวจสอบให้แน่ใจว่า ไดเร็กทอรีถูกตั้งค่าเป็นโหมดการให้สิทธิ์ที่ระบุไว้ หรือเป็นค่าที่ได้รับสิทธิ์น้อย

ตารางที่ 4. DoD มาตรฐานสำหรับการให้สิทธิ์ไฟล์ (ต่อ)

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

ตารางที่ 4. 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` **แอ็คชันความเข้ากันได้** ตรวจสอบให้แน่ใจว่า ไฟล์ถูกตั้งค่าโหมดการให้สิทธิ์ที่ระบุไว้ หรือเป็นค่าที่ได้รับสิทธิ์น้อย
GEN001364	ไฟล์ `/etc/resolv.conf` ต้องมีโหมด 0644 หรือโหมดที่ได้รับสิทธิ์น้อย	**ตำแหน่ง** `/etc/security/pscexpert/dodv2/fpmdodfiles` **แอ็คชันความเข้ากันได้** ตรวจสอบให้แน่ใจว่า ไฟล์ที่ถูกตั้งค่าเป็นโหมดการให้สิทธิ์ที่ระบุไว้ หรือเป็นค่าที่ได้รับสิทธิ์น้อย
GEN001368	ไฟล์ `/etc/hosts` ต้องมีโหมด 0644 หรือโหมดที่ได้รับสิทธิ์น้อย	**ตำแหน่ง** `/etc/security/pscexpert/dodv2/fpmdodfiles` **แอ็คชันความเข้ากันได้** ตรวจสอบให้แน่ใจว่า ไฟล์ที่ถูกตั้งค่าเป็นโหมดการให้สิทธิ์ที่ระบุไว้ หรือเป็นค่าที่ได้รับสิทธิ์น้อย
GEN001373	ไฟล์ `/etc/nsswitch.conf` ต้องมีโหมด 0644 หรือโหมดที่ได้รับสิทธิ์น้อย	**ตำแหน่ง** `/etc/security/pscexpert/dodv2/fpmdodfiles` **แอ็คชันความเข้ากันได้** ตรวจสอบให้แน่ใจว่า ไฟล์ที่ถูกตั้งค่าเป็นโหมดการให้สิทธิ์ที่ระบุไว้ หรือเป็นค่าที่ได้รับสิทธิ์น้อย
GEN001380	ไฟล์ `/etc/passwd` ต้องมีโหมด 0644 หรือโหมดที่ได้รับสิทธิ์น้อย	**ตำแหน่ง** `/etc/security/pscexpert/dodv2/fpmdodfiles` **แอ็คชันความเข้ากันได้** ตรวจสอบให้แน่ใจว่า ไฟล์ที่ถูกตั้งค่าเป็นโหมดการให้สิทธิ์ที่ระบุไว้ หรือเป็นค่าที่ได้รับสิทธิ์น้อย
GEN001393	ไฟล์ `/etc/group` ต้องมีโหมด 0644 หรือโหมดที่ได้รับสิทธิ์น้อย	**ตำแหน่ง** `/etc/security/pscexpert/dodv2/fpmdodfiles` **แอ็คชันความเข้ากันได้** ตรวจสอบให้แน่ใจว่า ไฟล์ที่ถูกตั้งค่าเป็นโหมดการให้สิทธิ์ที่ระบุไว้ หรือเป็นค่าที่ได้รับสิทธิ์น้อย

ตารางที่ 4. 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 **แอ็คชันความเข้ากันได้** ตรวจสอบให้แน่ใจว่า ไฟล์ที่ถูกตั้งค่าเป็นโหมดการให้สิทธิ์ที่ระบุไว้ หรือเป็นค่าที่ได้รับสิทธิ์น้อย
GEN001480	โฮมไดเร็กทอรีของผู้ใช้ทั้งหมดต้องมีโหมด 0750 หรือได้รับสิทธิ์น้อย	**ตำแหน่ง** /etc/security/pscexpert/dodv2/fpmdodfiles **แอ็คชันความเข้ากันได้** ตรวจสอบให้แน่ใจว่า ไฟล์ที่ถูกตั้งค่าเป็นโหมดการให้สิทธิ์ที่ระบุไว้ หรือเป็นค่าที่ได้รับสิทธิ์น้อย
GEN001560	ไฟล์และไดเร็กทอรีทั้งหมดที่มีอยู่ในโฮมไดเร็กทอรีของผู้ใช้ต้องมีโหมด 0750 หรือโหมดที่มีการให้สิทธิ์ น้อย	**ตำแหน่ง** /etc/security/pscexpert/dodv2/fpmdodfiles **แอ็คชันความเข้ากันได้** ตรวจสอบให้แน่ใจว่า ไฟล์ถูกตั้งค่าโหมดการให้สิทธิ์ที่ระบุไว้ หรือเป็นค่าที่ได้รับสิทธิ์น้อย
GEN001580	สคริปต์การควบคุมการรันทั้งหมดต้องมีโหมด 0755 หรือโหมดที่ได้รับสิทธิ์น้อย	**ตำแหน่ง** /etc/security/pscexpert/dodv2/fpmdodfiles **แอ็คชันความเข้ากันได้** ตรวจสอบให้แน่ใจว่า ไฟล์ถูกตั้งค่าโหมดการให้สิทธิ์ที่ระบุไว้ หรือเป็นค่าที่ได้รับสิทธิ์น้อย
GEN001640	การรันสคริปต์การควบคุมต้องไม่รันโปรแกรมหรือสคริปต์ที่สามารถเขียนได้	**ตำแหน่ง** /etc/security/pscexpert/dodv2/fpmdodfiles **แอ็คชันความเข้ากันได้** ตรวจสอบโปรแกรม เช่น cron สำหรับโปรแกรมหรือสคริปต์ ที่สามารถเขียนได้
GEN001720	ไฟล์การเริ่มต้นทำงานแบบโกลบอลทั้งหมดต้องมีโหมด 0644 หรือโหมดที่ได้รับสิทธิ์น้อย	**ตำแหน่ง** /etc/security/pscexpert/dodv2/fpmdodfiles **แอ็คชันความเข้ากันได้** ตรวจสอบให้แน่ใจว่า ไฟล์ถูกตั้งค่าโหมดการให้สิทธิ์ที่ระบุไว้ หรือเป็นค่าที่ได้รับสิทธิ์น้อย

ตารางที่ 4. 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` **แอ็คชันความเข้ากันได้** ตรวจสอบให้แน่ใจว่า ไฟล์ถูกตั้งค่าโหมดการให้สิทธิ์ที่ระบุไว้ หรือเป็นค่าที่ได้รับสิทธิ์น้อย
GEN001880	ไฟล์การเริ่มต้นทำงานแบบโลคัลทั้งหมดต้องมีโหมด 0740 หรือโหมดที่ได้รับสิทธิ์น้อย	**ตำแหน่ง** `/etc/security/pscexpert/dodv2/fpmdodfiles` **แอ็คชันความเข้ากันได้** ตรวจสอบให้แน่ใจว่า ไฟล์ถูกตั้งค่าโหมดการให้สิทธิ์ที่ระบุไว้ หรือเป็นค่าที่ได้รับสิทธิ์น้อย
GEN002220	ไฟล์เชลล์ทั้งหมดต้องมีโหมด 0755 หรือโหมด ที่ได้รับสิทธิ์น้อย	**ตำแหน่ง** `/etc/security/pscexpert/dodv2/fpmdodfiles` **แอ็คชันความเข้ากันได้** ตรวจสอบให้แน่ใจว่า ไฟล์ถูกตั้งค่าโหมดการให้สิทธิ์ที่ระบุไว้ หรือเป็นค่าที่ได้รับสิทธิ์น้อย
GEN002320	อุปกรณ์ออดิโอต้องมีโหมด 0660 หรือโหมด ที่ได้รับสิทธิ์น้อย	**ตำแหน่ง** `/etc/security/pscexpert/dodv2/fpmdodfiles` **แอ็คชันความเข้ากันได้** ตรวจสอบให้แน่ใจว่า อุปกรณ์ออดิโอถูกตั้งค่าเป็นโหมดการให้สิทธิ์ ที่ระบุเฉพาะ หรือเป็นค่าที่ได้สิทธิ์น้อย
GEN002560	ดีฟอลต์ของระบบและดีฟอลต์ของผู้ใช้ `umask` ต้องเป็น 077	**ตำแหน่ง** `/etc/security/pscexpert/dodv2/fpmdodfiles` **แอ็คชันความเข้ากันได้** ตรวจสอบให้แน่ใจว่า ค่าติดตั้งที่ระบุไว้เป็น *077*
GEN002700	ไฟล์การบันทึกของระบบต้องมีโหมด 0640 หรือโหมด ที่ได้รับสิทธิ์น้อย	**ตำแหน่ง** `/etc/security/pscexpert/dodv2/fpmdodfiles` **แอ็คชันความเข้ากันได้** ตรวจสอบให้แน่ใจว่า ไฟล์ถูกตั้งค่าโหมดการให้สิทธิ์ที่ระบุไว้ หรือเป็นค่าที่ได้รับสิทธิ์น้อย

ตารางที่ 4. DoD มาตรฐานสำหรับการให้สิทธิ์ไฟล์ (ต่อ)

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

ตารางที่ 4. 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` **แอ็คชันความเข้ากันได้** ตรวจสอบให้แน่ใจว่า ไฟล์ที่ถูกตั้งค่าเป็นโหมดการให้สิทธิ์ที่ระบุไว้ หรือเป็นค่าที่ได้รับสิทธิ์น้อย
GEN003252	ไฟล์ `at.deny` ต้องมีโหมด 0640 หรือโหมดที่ได้รับสิทธิ์น้อย	**ตำแหน่ง** `/etc/security/pscexpert/dodv2/fpmdodfiles` **แอ็คชันความเข้ากันได้** ตรวจสอบให้แน่ใจว่า ไฟล์ที่ถูกตั้งค่าเป็นโหมดการให้สิทธิ์ที่ระบุไว้ หรือเป็นค่าที่ได้รับสิทธิ์น้อย
GEN003340	ไฟล์ `at.allow` ต้องมีโหมด 0600 หรือโหมดที่ได้รับสิทธิ์น้อย	**ตำแหน่ง** `/etc/security/pscexpert/dodv2/fpmdodfiles` **แอ็คชันความเข้ากันได้** ตรวจสอบให้แน่ใจว่า ไฟล์ที่ถูกตั้งค่าเป็นโหมดการให้สิทธิ์ที่ระบุไว้ หรือเป็นค่าที่ได้รับสิทธิ์น้อย
GEN003400	ไดเร็กทอรี `at` ต้องมีโหมด 0755 หรือโหมดที่ได้รับสิทธิ์น้อย	**ตำแหน่ง** `/etc/security/pscexpert/dodv2/fpmdodfiles` **แอ็คชันความเข้ากันได้** ตรวจสอบให้แน่ใจว่า ไดเร็กทอรีถูกตั้งค่าเป็นโหมดการให้สิทธิ์ที่ระบุไว้ หรือเป็นค่าที่ได้รับสิทธิ์น้อย
GEN003440	งาน `At` ต้องไม่ตั้งค่าพารามิเตอร์ `umask` เป็นค่าที่น้อยกว่า 077	**ตำแหน่ง** `/etc/security/pscexpert/dodv2/fpmdodfiles` **แอ็คชันความเข้ากันได้** ตรวจสอบให้แน่ใจว่า พารามิเตอร์ถูกตั้งค่าเป็นโหมดการให้สิทธิ์ที่ระบุไว้ หรือเป็นค่าที่ได้รับสิทธิ์น้อย
GEN003740	ไฟล์ `inetd.conf` และ `xinetd.conf` ต้องมีโหมด 0440 หรือโหมดที่ได้รับสิทธิ์น้อย	**ตำแหน่ง** `/etc/security/pscexpert/dodv2/fpmdodfiles` **แอ็คชันความเข้ากันได้** ตรวจสอบให้แน่ใจว่า ไฟล์ถูกตั้งค่าโหมดการให้สิทธิ์ที่ระบุไว้ หรือเป็นค่าที่ได้รับสิทธิ์น้อย

ตารางที่ 4. DoD มาตรฐานสำหรับการให้สิทธิ์ไฟล์ (ต่อ)

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

ตารางที่ 4. DoD มาตรฐานสำหรับการให้สิทธิ์ไฟล์ (ต่อ)

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

ตารางที่ 4. DoD มาตรฐานสำหรับการให้สิทธิ์ไฟล์ (ต่อ)

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

ตารางที่ 4. 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 **แอ็คชันความเข้ากันได้** ตรวจสอบให้แน่ใจว่า ไฟล์ที่ถูกตั้งค่าเป็นโหมดการให้สิทธิ์ที่ระบุไว้ หรือเป็นค่าที่ได้รับสิทธิ์น้อย
GEN006320	ไฟล์ /etc/news/passwd.nntp (หรือเทียบเท่า) ต้องมีโหมด 0600 หรือโหมดที่ได้รับสิทธิ์น้อย	**ตำแหน่ง** /etc/security/pscexpert/dodv2/fpmdodfiles **แอ็คชันความเข้ากันได้** ตรวจสอบให้แน่ใจว่า ไฟล์ที่ถูกตั้งค่าเป็นโหมดการให้สิทธิ์ที่ระบุไว้ หรือเป็นค่าที่ได้รับสิทธิ์น้อย
GEN008060	ถ้าระบบกำลังใช้ LDAP สำหรับการพิสูจน์ตัวตน หรือข้อมูลแอคเคาต์ไฟล์ /etc/ldap.conf (หรือ เทียบเท่า) ต้องมีโหมด 0644 หรือได้รับสิทธิ์น้อย	**ตำแหน่ง** /etc/security/pscexpert/dodv2/fpmdodfiles **แอ็คชันความเข้ากันได้** ตรวจสอบให้แน่ใจว่า ไฟล์ที่ถูกตั้งค่าเป็นโหมดการให้สิทธิ์ที่ระบุไว้ หรือเป็นค่าที่ได้รับสิทธิ์น้อย
GEN008180	ถ้าระบบกำลังใช้ LDAP สำหรับการพิสูจน์ตัวตน หรือข้อมูลแอคเคาต์ไฟล์การออกใบรับรอง TLS ไดเร็กทอรี หรือทั้งสองต้องมีโหมด 0644 (0755 สำหรับไดเร็กทอรี) หรือได้รับสิทธิ์น้อย	**ตำแหน่ง** /etc/security/pscexpert/dodv2/fpmdodfiles **แอ็คชันความเข้ากันได้** ตรวจสอบให้แน่ใจว่า ไฟล์ไดเร็กทอรีที่ระบุเฉพาะ หรือทั้งสอง ถูกตั้งค่าเป็นโหมดการให้สิทธิ์ที่ระบุเฉพาะ หรือเป็นค่าที่ได้รับสิทธิ์น้อย

ตารางที่ 5. 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 **แอ็คชันความเข้ากันได้** ปิดใช้งาน ACL ที่ขยายเพิ่มที่ระบุไว้ **หมายเหตุ:** ค่าติดตั้งนี้ไม่ได้ถูกเปลี่ยนโดยอัตโนมัติเมื่อรีเซ็ตนโยบายเป็น นโยบายดีฟอลต์ของ AIX โดยใช้ไฟล์ DoDv2_to_AIXDefault.xml คุณต้องเปลี่ยนค่าติดตั้งนี้แบบแมนวล

ตารางที่ 5. 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 **แอ็คชันความเข้ากันได้** ปิดใช้งาน ACL ที่ขยายเพิ่มที่ระบุไว้ **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 **แอ็คชันความเข้ากันได้** ปิดใช้งาน ACL ที่ขยายเพิ่มที่ระบุไว้ **หมายเหตุ:** ค่าติดตั้งนี้ไม่ได้ถูกเปลี่ยนโดยอัตโนมัติเมื่อรีเซ็ตนโยบายเป็น นโยบายดีฟอลต์ของ AIX โดยใช้ไฟล์ DoDv2_to_AIXDefault.xml คุณต้องเปลี่ยนค่าติดตั้งนี้แบบแมนวล
GEN000930	โฮมไดเร็กทอรีของแอคเคาต์ root ต้องไม่มี ACL ที่ขยายเพิ่ม	**ตำแหน่ง** /etc/security/pscexpert/dodv2/acldodfiles **แอ็คชันความเข้ากันได้** ปิดใช้งาน ACL ที่ขยายเพิ่มที่ระบุไว้ **หมายเหตุ:** ค่าติดตั้งนี้ไม่ได้ถูกเปลี่ยนโดยอัตโนมัติเมื่อรีเซ็ตนโยบายเป็น นโยบายดีฟอลต์ของ AIX โดยใช้ไฟล์ DoDv2_to_AIXDefault.xml คุณต้องเปลี่ยนค่าติดตั้งนี้แบบแมนวล
GEN001190	ไฟล์ daemon เซอร์วิสเครือข่ายทั้งหมดไม่มี ACLs ที่ขยายเพิ่ม	**ตำแหน่ง** /etc/security/pscexpert/dodv2/acldodfiles **แอ็คชันความเข้ากันได้** ปิดใช้งาน ACL ที่ขยายเพิ่มที่ระบุไว้ **หมายเหตุ:** ค่าติดตั้งนี้ไม่ได้ถูกเปลี่ยนโดยอัตโนมัติเมื่อรีเซ็ตนโยบายเป็น นโยบายดีฟอลต์ของ AIX โดยใช้ไฟล์ DoDv2_to_AIXDefault.xml คุณต้องเปลี่ยนค่าติดตั้งนี้แบบแมนวล

ตารางที่ 5. 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` **แอ็คชันความเข้ากันได้** ปิดใช้งาน ACL ที่ขยายเพิ่มที่ระบุไว้ **หมายเหตุ:** ค่าติดตั้งนี้ไม่ได้ถูกเปลี่ยนโดยอัตโนมัติเมื่อรีเซ็ตนโยบายเป็น นโยบายดีฟอลต์ของ AIX โดยใช้ไฟล์ `DoDv2_to_AIXDefault.xml` คุณต้องเปลี่ยนค่าติดตั้งนี้แบบแมนวล
GEN001270	ไฟล์การทำบันทึกระบบต้องไม่มี ACLs ที่ขยายเพิ่ม ยกเว้นว่าจำเป็นต่อการสนับสนุนซอฟต์แวร์ที่ได้รับสิทธิ์	**ตำแหน่ง** `/etc/security/pscexpert/dodv2/acldodfiles` **แอ็คชันความเข้ากันได้** ปิดใช้งาน ACL ที่ขยายเพิ่มที่ระบุไว้ **หมายเหตุ:** ค่าติดตั้งนี้ไม่ได้ถูกเปลี่ยนโดยอัตโนมัติเมื่อรีเซ็ตนโยบายเป็น นโยบายดีฟอลต์ของ AIX โดยใช้ไฟล์ `DoDv2_to_AIXDefault.xml` คุณต้องเปลี่ยนค่าติดตั้งนี้แบบแมนวล
GEN001310	ไฟล์ไลบรารีทั้งหมดต้องไม่มี ACLs ที่ขยายเพิ่ม	**ตำแหน่ง** `/etc/security/pscexpert/dodv2/acldodfiles` **แอ็คชันความเข้ากันได้** ปิดใช้งาน ACL ที่ขยายเพิ่มที่ระบุไว้ **หมายเหตุ:** ค่าติดตั้งนี้ไม่ได้ถูกเปลี่ยนโดยอัตโนมัติเมื่อรีเซ็ตนโยบายเป็น นโยบายดีฟอลต์ของ AIX โดยใช้ไฟล์ `DoDv2_to_AIXDefault.xml` คุณต้องเปลี่ยนค่าติดตั้งนี้แบบแมนวล
GEN001361	ไฟล์คำสั่ง NIS/NIS+/yp ต้องไม่มี ACLs ที่ขยายเพิ่ม	**ตำแหน่ง** `/etc/security/pscexpert/dodv2/acldodfiles` **แอ็คชันความเข้ากันได้** ปิดใช้งาน ACL ที่ขยายเพิ่มที่ระบุไว้ **หมายเหตุ:** ค่าติดตั้งนี้ไม่ได้ถูกเปลี่ยนโดยอัตโนมัติเมื่อรีเซ็ตนโยบายเป็น นโยบายดีฟอลต์ของ AIX โดยใช้ไฟล์ `DoDv2_to_AIXDefault.xml` คุณต้องเปลี่ยนค่าติดตั้งนี้แบบแมนวล

ตารางที่ 5. 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 **แอ็คชันความเข้ากันได้** ปิดใช้งาน ACL ที่ขยายเพิ่มที่ระบุไว้ **หมายเหตุ:** ค่าติดตั้งนี้ไม่ได้ถูกเปลี่ยนโดยอัตโนมัติเมื่อรีเซ็ตนโยบายเป็น นโยบายดีฟอลต์ของ AIX โดยใช้ไฟล์ DoDv2_to_AIXDefault.xml คุณต้องเปลี่ยนค่าติดตั้งนี้แบบแมนวล
GEN001369	ไฟล์ /etc/hosts ต้องไม่มี ACL ที่ขยายเพิ่ม	**ตำแหน่ง** /etc/security/pscexpert/dodv2/acldodfiles **แอ็คชันความเข้ากันได้** ปิดใช้งาน ACL ที่ขยายเพิ่มที่ระบุไว้ **หมายเหตุ:** ค่าติดตั้งนี้ไม่ได้ถูกเปลี่ยนโดยอัตโนมัติเมื่อรีเซ็ตนโยบายเป็น นโยบายดีฟอลต์ของ AIX โดยใช้ไฟล์ DoDv2_to_AIXDefault.xml คุณต้องเปลี่ยนค่าติดตั้งนี้แบบแมนวล
GEN001374	ไฟล์ /etc/nsswitch.conf ต้องไม่มี ACL ที่ขยายเพิ่ม	**ตำแหน่ง** /etc/security/pscexpert/dodv2/acldodfiles **แอ็คชันความเข้ากันได้** ปิดใช้งาน ACL ที่ขยายเพิ่มที่ระบุไว้ **หมายเหตุ:** ค่าติดตั้งนี้ไม่ได้ถูกเปลี่ยนโดยอัตโนมัติเมื่อรีเซ็ตนโยบายเป็น นโยบายดีฟอลต์ของ AIX โดยใช้ไฟล์ DoDv2_to_AIXDefault.xml คุณต้องเปลี่ยนค่าติดตั้งนี้แบบแมนวล
GEN001390	ไฟล์ /etc/passwd ต้องไม่มี ACL ที่ขยายเพิ่ม	**ตำแหน่ง** /etc/security/pscexpert/dodv2/acldodfiles **แอ็คชันความเข้ากันได้** ปิดใช้งาน ACL ที่ขยายเพิ่มที่ระบุไว้ **หมายเหตุ:** ค่าติดตั้งนี้ไม่ได้ถูกเปลี่ยนโดยอัตโนมัติเมื่อรีเซ็ตนโยบายเป็น นโยบายดีฟอลต์ของ AIX โดยใช้ไฟล์ DoDv2_to_AIXDefault.xml คุณต้องเปลี่ยนค่าติดตั้งนี้แบบแมนวล

ตารางที่ 5. 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` **แอ็คชันความเข้ากันได้** ปิดใช้งาน ACL ที่ขยายเพิ่มที่ระบุไว้ **หมายเหตุ:** ค่าติดตั้งนี้ไม่ได้ถูกเปลี่ยนโดยอัตโนมัติเมื่อรีเซ็ตนโยบายเป็น นโยบายดีฟอลต์ของ AIX โดยใช้ไฟล์ `DoDv2_to_AIXDefault.xml` คุณต้องเปลี่ยนค่าติดตั้งนี้แบบแมนวล
GEN001430	ไฟล์ `/etc/security/passwd` ต้องไม่มี ACL ที่ขยายเพิ่ม	**ตำแหน่ง** `/etc/security/pscexpert/dodv2/acldodfiles` **แอ็คชันความเข้ากันได้** ปิดใช้งาน ACL ที่ขยายเพิ่มที่ระบุไว้ **หมายเหตุ:** ค่าติดตั้งนี้ไม่ได้ถูกเปลี่ยนโดยอัตโนมัติเมื่อรีเซ็ตนโยบายเป็น นโยบายดีฟอลต์ของ AIX โดยใช้ไฟล์ `DoDv2_to_AIXDefault.xml` คุณต้องเปลี่ยนค่าติดตั้งนี้แบบแมนวล
GEN001570	ไฟล์และไดเร็กทอรีทั้งหมดที่มี อยู่ในโฮมไดเร็กทอรีต้องไม่มี ACLs ที่ขยายเพิ่ม	**ตำแหน่ง** `/etc/security/pscexpert/dodv2/acldodfiles` **แอ็คชันความเข้ากันได้** ปิดใช้งาน ACL ที่ขยายเพิ่มที่ระบุไว้ **หมายเหตุ:** ค่าติดตั้งนี้ไม่ได้ถูกเปลี่ยนโดยอัตโนมัติเมื่อรีเซ็ตนโยบายเป็น นโยบายดีฟอลต์ของ AIX โดยใช้ไฟล์ `DoDv2_to_AIXDefault.xml` คุณต้องเปลี่ยนค่าติดตั้งนี้แบบแมนวล
GEN001590	การรันสคริปต์การควบคุมทั้งหมดต้องไม่มี ACLs ที่ขยายเพิ่ม	**ตำแหน่ง** `/etc/security/pscexpert/dodv2/acldodfiles` **แอ็คชันความเข้ากันได้** ปิดใช้งาน ACL ที่ขยายเพิ่มที่ระบุไว้ **หมายเหตุ:** ค่าติดตั้งนี้ไม่ได้ถูกเปลี่ยนโดยอัตโนมัติเมื่อรีเซ็ตนโยบายเป็น นโยบายดีฟอลต์ของ AIX โดยใช้ไฟล์ `DoDv2_to_AIXDefault.xml` คุณต้องเปลี่ยนค่าติดตั้งนี้แบบแมนวล

ตารางที่ 5. 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` **แอ็คชันความเข้ากันได้** ปิดใช้งาน ACL ที่ขยายเพิ่มที่ระบุไว้ **หมายเหตุ:** ค่าติดตั้งนี้ไม่ได้ถูกเปลี่ยนโดยอัตโนมัติเมื่อรีเซ็ตนโยบายเป็น นโยบายดีฟอลต์ของ AIX โดยใช้ไฟล์ `DoDv2_to_AIXDefault.xml` คุณต้องเปลี่ยนค่าติดตั้งนี้แบบแมนวล
GEN001810	ไฟล์ Skeleton ต้องไม่มี ACLs ที่ขยายเพิ่ม	**ตำแหน่ง** `/etc/security/pscexpert/dodv2/acldodfiles` **แอ็คชันความเข้ากันได้** ปิดใช้งาน ACL ที่ขยายเพิ่มที่ระบุไว้ **หมายเหตุ:** ค่าติดตั้งนี้ไม่ได้ถูกเปลี่ยนโดยอัตโนมัติเมื่อรีเซ็ตนโยบายเป็น นโยบายดีฟอลต์ของ AIX โดยใช้ไฟล์ `DoDv2_to_AIXDefault.xml` คุณต้องเปลี่ยนค่าติดตั้งนี้แบบแมนวล
GEN001890	ไฟล์การเริ่มต้นทำงานแบบโลคัลต้องไม่มี ACLs ที่ขยายเพิ่ม	**ตำแหน่ง** `/etc/security/pscexpert/dodv2/acldodfiles` **แอ็คชันความเข้ากันได้** ปิดใช้งาน ACL ที่ขยายเพิ่มที่ระบุไว้ **หมายเหตุ:** ค่าติดตั้งนี้ไม่ได้ถูกเปลี่ยนโดยอัตโนมัติเมื่อรีเซ็ตนโยบายเป็น นโยบายดีฟอลต์ของ AIX โดยใช้ไฟล์ `DoDv2_to_AIXDefault.xml` คุณต้องเปลี่ยนค่าติดตั้งนี้แบบแมนวล
GEN002230	ไฟล์เชลล์ทั้งหมดต้องไม่มี ACLs ที่ขยายเพิ่ม	**ตำแหน่ง** `/etc/security/pscexpert/dodv2/acldodfiles` **แอ็คชันความเข้ากันได้** ปิดใช้งาน ACL ที่ขยายเพิ่มที่ระบุไว้ **หมายเหตุ:** ค่าติดตั้งนี้ไม่ได้ถูกเปลี่ยนโดยอัตโนมัติเมื่อรีเซ็ตนโยบายเป็น นโยบายดีฟอลต์ของ AIX โดยใช้ไฟล์ `DoDv2_to_AIXDefault.xml` คุณต้องเปลี่ยนค่าติดตั้งนี้แบบแมนวล

ตารางที่ 5. 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` **แอ็คชันความเข้ากันได้** ปิดใช้งาน ACL ที่ขยายเพิ่มที่ระบุไว้ **หมายเหตุ:** ค่าติดตั้งนี้ไม่ได้ถูกเปลี่ยนโดยอัตโนมัติเมื่อรีเซ็ตนโยบายเป็น นโยบายดีฟอลต์ของ AIX โดยใช้ไฟล์ `DoDv2_to_AIXDefault.xml` คุณต้องเปลี่ยนค่าติดตั้งนี้แบบแมนวล
GEN002710	ไฟล์การตรวจสอบระบบทั้งหมดต้องไม่มี ACLs ที่ขยายเพิ่ม	**ตำแหน่ง** `/etc/security/pscexpert/dodv2/acldodfiles` **แอ็คชันความเข้ากันได้** ปิดใช้งาน ACL ที่ขยายเพิ่มที่ระบุไว้ **หมายเหตุ:** ค่าติดตั้งนี้ไม่ได้ถูกเปลี่ยนโดยอัตโนมัติเมื่อรีเซ็ตนโยบายเป็น นโยบายดีฟอลต์ของ AIX โดยใช้ไฟล์ `DoDv2_to_AIXDefault.xml` คุณต้องเปลี่ยนค่าติดตั้งนี้แบบแมนวล
GEN002990	ACLs ที่ขยายเพิ่มควรปิดใช้งานสำหรับไฟล์ `cron.allow` และ `cron.deny`	**ตำแหน่ง** `/etc/security/pscexpert/dodv2/acldodfiles` **แอ็คชันความเข้ากันได้** ปิดใช้งาน ACL ที่ขยายเพิ่มที่ระบุไว้ **หมายเหตุ:** ค่าติดตั้งนี้ไม่ได้ถูกเปลี่ยนโดยอัตโนมัติเมื่อรีเซ็ตนโยบายเป็น นโยบายดีฟอลต์ของ AIX โดยใช้ไฟล์ `DoDv2_to_AIXDefault.xml` คุณต้องเปลี่ยนค่าติดตั้งนี้แบบแมนวล
GEN003090	ไฟล์ Crontab ต้องไม่มี ACLs ที่ขยายเพิ่ม	**ตำแหน่ง** `/etc/security/pscexpert/dodv2/acldodfiles` **แอ็คชันความเข้ากันได้** ปิดใช้งาน ACL ที่ขยายเพิ่มที่ระบุไว้ **หมายเหตุ:** ค่าติดตั้งนี้ไม่ได้ถูกเปลี่ยนโดยอัตโนมัติเมื่อรีเซ็ตนโยบายเป็น นโยบายดีฟอลต์ของ AIX โดยใช้ไฟล์ `DoDv2_to_AIXDefault.xml` คุณต้องเปลี่ยนค่าติดตั้งนี้แบบแมนวล

ตารางที่ 5. 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` **แอ็คชันความเข้ากันได้** ปิดใช้งาน ACL ที่ขยายเพิ่มที่ระบุไว้ **หมายเหตุ:** ค่าติดตั้งนี้ไม่ได้ถูกเปลี่ยนโดยอัตโนมัติเมื่อรีเซ็ตนโยบายเป็น นโยบายดีฟอลต์ของ AIX โดยใช้ไฟล์ `DoDv2_to_AIXDefault.xml` คุณต้องเปลี่ยนค่าติดตั้งนี้แบบแมนวล
GEN003190	ไฟล์การทำบันทึก cron ต้องไม่มี ACLs ที่ขยายเพิ่ม	**ตำแหน่ง** `/etc/security/pscexpert/dodv2/acldodfiles` **แอ็คชันความเข้ากันได้** ปิดใช้งาน ACL ที่ขยายเพิ่มที่ระบุไว้ **หมายเหตุ:** ค่าติดตั้งนี้ไม่ได้ถูกเปลี่ยนโดยอัตโนมัติเมื่อรีเซ็ตนโยบายเป็น นโยบายดีฟอลต์ของ AIX โดยใช้ไฟล์ `DoDv2_to_AIXDefault.xml` คุณต้องเปลี่ยนค่าติดตั้งนี้แบบแมนวล
GEN003210	ไฟล์ `cron.deny` ต้องไม่มี ACL ที่ขยายเพิ่ม	**ตำแหน่ง** `/etc/security/pscexpert/dodv2/acldodfiles` **แอ็คชันความเข้ากันได้** ปิดใช้งาน ACL ที่ขยายเพิ่มที่ระบุไว้ **หมายเหตุ:** ค่าติดตั้งนี้ไม่ได้ถูกเปลี่ยนโดยอัตโนมัติเมื่อรีเซ็ตนโยบายเป็น นโยบายดีฟอลต์ของ AIX โดยใช้ไฟล์ `DoDv2_to_AIXDefault.xml` คุณต้องเปลี่ยนค่าติดตั้งนี้แบบแมนวล
GEN003245	ไฟล์ `at.allow` ต้องไม่มี ACL ที่ขยายเพิ่ม	**ตำแหน่ง** `/etc/security/pscexpert/dodv2/acldodfiles` **แอ็คชันความเข้ากันได้** ปิดใช้งาน ACL ที่ขยายเพิ่มที่ระบุไว้ **หมายเหตุ:** ค่าติดตั้งนี้ไม่ได้ถูกเปลี่ยนโดยอัตโนมัติเมื่อรีเซ็ตนโยบายเป็น นโยบายดีฟอลต์ของ AIX โดยใช้ไฟล์ `DoDv2_to_AIXDefault.xml` คุณต้องเปลี่ยนค่าติดตั้งนี้แบบแมนวล

ตารางที่ 5. 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` **แอ็คชันความเข้ากันได้** ปิดใช้งาน ACL ที่ขยายเพิ่มที่ระบุไว้ **หมายเหตุ:** ค่าติดตั้งนี้ไม่ได้ถูกเปลี่ยนโดยอัตโนมัติเมื่อรีเซ็ตนโยบายเป็น นโยบายดีฟอลต์ของ AIX โดยใช้ไฟล์ `DoDv2_to_AIXDefault.xml` คุณต้องเปลี่ยนค่าติดตั้งนี้แบบแมนวล
GEN003410	ไดเร็กทอรี `at` ต้องไม่มี ACL ที่ขยายเพิ่ม	**ตำแหน่ง** `/etc/security/pscexpert/dodv2/acldodfiles` **แอ็คชันความเข้ากันได้** ปิดใช้งาน ACL ที่ขยายเพิ่มที่ระบุไว้ **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` **แอ็คชันความเข้ากันได้** ปิดใช้งาน ACL ที่ขยายเพิ่มที่ระบุไว้ **หมายเหตุ:** ค่าติดตั้งนี้ไม่ได้ถูกเปลี่ยนโดยอัตโนมัติเมื่อรีเซ็ตนโยบายเป็น นโยบายดีฟอลต์ของ AIX โดยใช้ไฟล์ `DoDv2_to_AIXDefault.xml` คุณต้องเปลี่ยนค่าติดตั้งนี้แบบแมนวล
GEN003790	ไฟล์เซอร์วิสต้องไม่มี ACL ที่ขยายเพิ่ม	**ตำแหน่ง** `/etc/security/pscexpert/dodv2/acldodfiles` **แอ็คชันความเข้ากันได้** ปิดใช้งาน ACL ที่ขยายเพิ่มที่ระบุไว้ **หมายเหตุ:** ค่าติดตั้งนี้ไม่ได้ถูกเปลี่ยนโดยอัตโนมัติเมื่อรีเซ็ตนโยบายเป็น นโยบายดีฟอลต์ของ AIX โดยใช้ไฟล์ `DoDv2_to_AIXDefault.xml` คุณต้องเปลี่ยนค่าติดตั้งนี้แบบแมนวล

ตารางที่ 5. 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` **แอ็คชันความเข้ากันได้** ปิดใช้งาน ACL ที่ขยายเพิ่มที่ระบุไว้ **หมายเหตุ:** ค่าติดตั้งนี้ไม่ได้ถูกเปลี่ยนโดยอัตโนมัติเมื่อรีเซ็ตนโยบายเป็น นโยบายดีฟอลต์ของ AIX โดยใช้ไฟล์ `DoDv2_to_AIXDefault.xml` คุณต้องเปลี่ยนค่าติดตั้งนี้แบบแมนวล
GEN004010	ไฟล์ `traceroute` ต้องไม่มี ACL ที่ขยายเพิ่ม	**ตำแหน่ง** `/etc/security/pscexpert/dodv2/acldodfiles` **แอ็คชันความเข้ากันได้** ปิดใช้งาน ACL ที่ขยายเพิ่มที่ระบุไว้ **หมายเหตุ:** ค่าติดตั้งนี้ไม่ได้ถูกเปลี่ยนโดยอัตโนมัติเมื่อรีเซ็ตนโยบายเป็น นโยบายดีฟอลต์ของ AIX โดยใช้ไฟล์ `DoDv2_to_AIXDefault.xml` คุณต้องเปลี่ยนค่าติดตั้งนี้แบบแมนวล
GEN004390	ไฟล์ `alias` ต้องไม่มี ACL ที่ขยายเพิ่ม	**ตำแหน่ง** `/etc/security/pscexpert/dodv2/acldodfiles` **แอ็คชันความเข้ากันได้** ปิดใช้งาน ACL ที่ขยายเพิ่มที่ระบุไว้ **หมายเหตุ:** ค่าติดตั้งนี้ไม่ได้ถูกเปลี่ยนโดยอัตโนมัติเมื่อรีเซ็ตนโยบายเป็น นโยบายดีฟอลต์ของ AIX โดยใช้ไฟล์ `DoDv2_to_AIXDefault.xml` คุณต้องเปลี่ยนค่าติดตั้งนี้แบบแมนวล
GEN004430	ไฟล์ที่รันผ่านไฟล์เมล `aliases` ต้องไม่มี ACLs ที่ขยายเพิ่ม	**ตำแหน่ง** `/etc/security/pscexpert/dodv2/acldodfiles` **แอ็คชันความเข้ากันได้** ปิดใช้งาน ACL ที่ขยายเพิ่มที่ระบุไว้ **หมายเหตุ:** ค่าติดตั้งนี้ไม่ได้ถูกเปลี่ยนโดยอัตโนมัติเมื่อรีเซ็ตนโยบายเป็น นโยบายดีฟอลต์ของ AIX โดยใช้ไฟล์ `DoDv2_to_AIXDefault.xml` คุณต้องเปลี่ยนค่าติดตั้งนี้แบบแมนวล

ตารางที่ 5. 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` **แอ็คชันความเข้ากันได้** ปิดใช้งาน ACL ที่ขยายเพิ่มที่ระบุไว้ **หมายเหตุ:** ค่าติดตั้งนี้ไม่ได้ถูกเปลี่ยนโดยอัตโนมัติเมื่อรีเซ็ตนโยบายเป็น นโยบายดีฟอลต์ของ AIX โดยใช้ไฟล์ `DoDv2_to_AIXDefault.xml` คุณต้องเปลี่ยนค่าติดตั้งนี้แบบแมนวล
GEN004950	ไฟล์ `ftpusers` ต้องไม่มี ACL ที่ขยายเพิ่ม	**ตำแหน่ง** `/etc/security/pscexpert/dodv2/acldodfiles` **แอ็คชันความเข้ากันได้** ปิดใช้งาน ACL ที่ขยายเพิ่มที่ระบุไว้ **หมายเหตุ:** ค่าติดตั้งนี้ไม่ได้ถูกเปลี่ยนโดยอัตโนมัติเมื่อรีเซ็ตนโยบายเป็น นโยบายดีฟอลต์ของ AIX โดยใช้ไฟล์ `DoDv2_to_AIXDefault.xml` คุณต้องเปลี่ยนค่าติดตั้งนี้แบบแมนวล
GEN005190	ไฟล์ `.Xauthority` ต้องไม่มี ACLs ที่ขยายเพิ่ม	**ตำแหน่ง** `/etc/security/pscexpert/dodv2/acldodfiles` **แอ็คชันความเข้ากันได้** ปิดใช้งาน ACL ที่ขยายเพิ่มที่ระบุไว้ **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` **แอ็คชันความเข้ากันได้** ปิดใช้งาน ACL ที่ขยายเพิ่มที่ระบุไว้ **หมายเหตุ:** ค่าติดตั้งนี้ไม่ได้ถูกเปลี่ยนโดยอัตโนมัติเมื่อรีเซ็ตนโยบายเป็น นโยบายดีฟอลต์ของ AIX โดยใช้ไฟล์ `DoDv2_to_AIXDefault.xml` คุณต้องเปลี่ยนค่าติดตั้งนี้แบบแมนวล

ตารางที่ 5. 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` **แอ็คชันความเข้ากันได้** ปิดใช้งาน ACL ที่ขยายเพิ่มที่ระบุไว้ **หมายเหตุ:** ค่าติดตั้งนี้ไม่ได้ถูกเปลี่ยนโดยอัตโนมัติเมื่อรีเซ็ตนโยบายเป็น นโยบายดีฟอลต์ของ AIX โดยใช้ไฟล์ `DoDv2_to_AIXDefault.xml` คุณต้องเปลี่ยนค่าติดตั้งนี้แบบแมนวล
GEN005395	ไฟล์ `/etc/syslog.conf` ต้องไม่มี ACL ที่ขยายเพิ่ม	**ตำแหน่ง** `/etc/security/pscexpert/dodv2/acldodfiles` **แอ็คชันความเข้ากันได้** ปิดใช้งาน ACL ที่ขยายเพิ่มที่ระบุไว้ **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` **แอ็คชันความเข้ากันได้** ปิดใช้งาน ACL ที่ขยายเพิ่มที่ระบุไว้ **หมายเหตุ:** ค่าติดตั้งนี้ไม่ได้ถูกเปลี่ยนโดยอัตโนมัติเมื่อรีเซ็ตนโยบายเป็น นโยบายดีฟอลต์ของ AIX โดยใช้ไฟล์ `DoDv2_to_AIXDefault.xml` คุณต้องเปลี่ยนค่าติดตั้งนี้แบบแมนวล
GEN006210	ไฟล์ `/var/private/smbpasswd` ต้องไม่มี ACL ที่ขยายเพิ่ม	**ตำแหน่ง** `/etc/security/pscexpert/dodv2/acldodfiles` **แอ็คชันความเข้ากันได้** ปิดใช้งาน ACL ที่ขยายเพิ่มที่ระบุไว้ **หมายเหตุ:** ค่าติดตั้งนี้ไม่ได้ถูกเปลี่ยนโดยอัตโนมัติเมื่อรีเซ็ตนโยบายเป็น นโยบายดีฟอลต์ของ AIX โดยใช้ไฟล์ `DoDv2_to_AIXDefault.xml` คุณต้องเปลี่ยนค่าติดตั้งนี้แบบแมนวล

ตารางที่ 5. 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 **แอ็คชันความเข้ากันได้** ปิดใช้งาน ACL ที่ขยายเพิ่มที่ระบุไว้ **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 **แอ็คชันความเข้ากันได้** ปิดใช้งาน ACL ที่ขยายเพิ่มที่ระบุไว้ **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 **แอ็คชันความเข้ากันได้** ปิดใช้งาน ACL ที่ขยายเพิ่มที่ระบุไว้ **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 **แอ็คชันความเข้ากันได้** ปิดใช้งาน ACL ที่ขยายเพิ่มที่ระบุไว้ **หมายเหตุ:** ค่าติดตั้งนี้ไม่ได้ถูกเปลี่ยนโดยอัตโนมัติเมื่อรีเซ็ตนโยบายเป็น นโยบายดีฟอลต์ของ AIX โดยใช้ไฟล์ DoDv2_to_AIXDefault.xml คุณต้องเปลี่ยนค่าติดตั้งนี้แบบแมนวล

ตารางที่ 5. ข้อกำหนดเกี่ยวกับ DoD access control list (ACL) (ต่อ)

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

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 ถูกปรับใช้โดยการปิดใช้เซอร์วิสที่ไม่จำเป็น และเซอร์วิสที่ไม่ปลอดภัย

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

ข้อกำหนดที่ 2: อย่าใช้ค่าดีฟอลต์ที่กำหนดโดยผู้จำหน่ายสำหรับ รหัสผ่านของระบบและพารามิเตอร์ความปลอดภัยอื่นๆ

ส่วนที่ 2.1: เปลี่ยนค่าดีฟอลต์ที่กำหนดโดยผู้จำหน่ายเสมอ ก่อนที่คุณจะติดตั้งระบบบนเครือข่าย 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 AIXPert ที่จะสมบูรณ์เมื่อรันคำสั่ง เช่น คำสั่ง `pscxpert -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: จำกัดการเข้าถึงทางกายภาพต่อข้อมูลสมาชิก

จัดเก็บที่เก็บข้อมูลที่มีข้อมูลสมาชิกที่สำคัญ ในห้องที่มีการจำกัดการเข้าถึง

ข้อกำหนดที่ 10: ติดตามและเฝ้าดูการเข้าถึงรีซอร์สเครือข่าย และข้อมูลสมาชิกทั้งหมด

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

ตารางที่ 6. 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`

ตารางที่ 6. การตั้งค่าที่เกี่ยวข้องกับมาตรฐานการปฏิบัติตามข้อกำหนด PCI DSS 2.0 (ต่อ)

การปรับใช้มาตรฐาน PCI DSS เหล่านี้	ข้อมูลจำเพาะการนำไปปฏิบัติ	การปรับใช้ AIX Security Expert	ตำแหน่งของค่าและการตั้งค่าที่ จำเป็นสำหรับการปฏิบัติตาม (ถ้ามี)
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
8.5.12	ไม่อนุญาตให้แต่ละบุคคลส่งรหัสผ่านใหม่ ที่เป็นรหัสผ่านเดียวกับรหัสผ่านสี่ตัวที่ใช้ก่อนหน้านี้	ตั้งค่าจำนวนสัปดาห์ก่อนที่จะสามารถนำรหัสผ่าน กลับมาใช้ใหม่เท่ากับ 52	**ตำแหน่ง** /etc/security/pscexpert/bin/chusrattr **ค่ามาตรฐาน** histexpire=52

ตารางที่ 6. การตั้งค่าที่เกี่ยวข้องกับมาตรฐานการปฏิบัติตามข้อกำหนด PCI DSS 2.0 (ต่อ)

การปรับใช้มาตรฐาน PCI DSS เหล่านี้	ข้อมูลจำเพาะการนำไปปฏิบัติ	การปรับใช้ AIX Security Expert	ตำแหน่งของค่าและการตั้งค่าที่ จำเป็นสำหรับการปฏิบัติตาม (ถ้ามี)
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 ครั้งสำหรับแต่ละแอคเคาต์ผู้ใช้ 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 ผู้จำหน่าย และหุ้นส่วนทางธุรกิจเฉพาะเมื่อจำเป็นต้องใช้โดยผู้จำหน่ายและหุ้นส่วน 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
10.2	เปิดใช้งานการตรวจสอบบนระบบ	เปิดใช้งานการตรวจสอบไฟล์ไลบรารีบน ระบบ	**ตำแหน่ง** `/etc/security/pscexpert/bin/pciaudit` **ค่ามาตรฐาน** h

ตารางที่ 6. 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 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
2.1	เปลี่ยนค่าดีฟอลต์ที่กำหนดโดยผู้จำหน่ายก่อนการติดตั้ง ระบบบนเครือข่าย ซึ่งรวมถึงการปิดใช้งาน HOSTMIBD daemon	ปิดใช้งาน HOSTMIBD daemon	**ตำแหน่ง** /etc/security/pscexpert/bin/rctcpip **ค่ามาตรฐาน** hostmibd d

ตารางที่ 6. 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 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
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

ตารางที่ 6. 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 `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
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

ตารางที่ 6. 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 `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
1.1.5 2.2.2	ปิดใช้งานเซอร์วิสที่ไม่ปลอดภัยและเซอร์วิสที่ไม่จำเป็น ซึ่ง รวมถึงเซอร์วิส `TCP daytime`	หยุดและปิดใช้งานอินสแตนซ์ทั้งหมดของเซอร์วิส `daytime(tcp)` ยูทิลิตี้ AIX Security Expert ยังคอมเม้นต์รายการที่เกี่ยวข้อง ในไฟล์ `/etc/inetd.conf` ที่สตาร์ท เซอร์วิสโดยอัตโนมัติ	**ตำแหน่ง** `/etc/security/pscexpert/bin/cominetdconf` **ค่ามาตรฐาน** daytime tcp d

ตารางที่ 6. 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 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
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

ตารางที่ 6. 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 `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
2.2.3	กำหนดค่าคอนฟิกพารามิเตอร์การรักษาความปลอดภัยของระบบเพื่อป้องกัน ความผิดพลาด	ปรับเปลี่ยนโปรโตคอล Network File System ด้วยค่าติดตั้งที่จำกัด ซึ่งสอดคล้องกับข้อกำหนดด้านความปลอดภัย PCI ค่าติดตั้งที่จำกัดเหล่านี้ประกอบด้วยการปิดใช้งานการเข้าถึงแบบ roote แบบรีโมต และการเข้าถึง UID และ GID แบบไม่ระบุชื่อ	**ตำแหน่ง** `/etc/security/pscexpert/bin/nfsconfig` **ค่ามาตรฐาน** e

ตารางที่ 6. การตั้งค่าที่เกี่ยวข้องกับมาตรฐานการปฏิบัติตามข้อกำหนด PCI DSS 2.0 (ต่อ)

การปรับใช้มาตรฐาน PCI DSS เหล่านี้	ข้อมูลจำเพาะการนำไปปฏิบัติ	การปรับใช้ AIX Security Expert	ตำแหน่งของค่าและการตั้งค่าที่ จำเป็นสำหรับการปฏิบัติตาม (ถ้ามี)
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 6. 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 **หมายเหตุ:** คุณสามารถป้อนกฎการกรองเพิ่มเติมใน ไฟล์ `/etc/security/aixpert/bin/filter.txt` กฎนี้ถูกรวมไว้โดยสคริปต์ `ipsecshunhosthls.sh` เมื่อคุณใช้กับโปรไฟล์ รายการต่างๆ ควรอยู่ในรูปแบบ ต่อไปนี้: *port_number*:*ip_address*:*action (การดำเนินการ)* โดยที่ ค่าที่อาจเกิดขึ้นได้สำหรับ *action* คือ `Allow` หรือ `Deny`
	ปกป้องโฮสต์จากการสแกนพอร์ต	ตั้งค่าระบบเพื่อหลบหลีกพอร์ตที่มีช่องโหว่ เป็นเวลา 5 นาที ซึ่งจะป้องกันการสแกนพอร์ต	**ตำแหน่ง** `/etc/security/pscexpert/bin/ipsecshunports` **ค่ามาตรฐาน** ไม่ต้องมีค่ามาตรฐาน **หมายเหตุ:** คุณสามารถป้อนกฎการกรองเพิ่มเติมในไฟล์ `/etc/security/aixpert/bin/filter.txt` กฎเหล่านี้ถูกรวมไว้โดยสคริปต์ `ipsecshunhosthls.sh` เมื่อคุณใช้โปรไฟล์ รายการต่างๆ ควรอยู่ในรูปแบบ ต่อไปนี้: *port_number*:*ip_address*:*action (การดำเนินการ)* โดยที่ ค่าที่อาจเกิดขึ้นได้สำหรับ *action* คือ `Allow` หรือ `Deny`
	จำกัดสิทธิ์การสร้างอ็อบเจ็กต์	ตั้งค่าสิทธิ์การสร้างอ็อบเจ็กต์ดีฟอลต์เป็น 22	**ตำแหน่ง** `/etc/security/pscexpert/bin/chusrattr` **ค่ามาตรฐาน** umask=22
	จำกัดการเข้าถึงระบบ	ให้มีเฉพาะ ID รูทที่แสดง ในไฟล์ `cron.allow` และลบไฟล์ `cron.deny` ออกจากระบบ	**ตำแหน่ง** `/etc/security/pscexpert/bin/limitsysacc` **ค่ามาตรฐาน** h

ตารางที่ 6. การตั้งค่าที่เกี่ยวข้องกับมาตรฐานการปฏิบัติตามข้อกำหนด PCI DSS 2.0 (ต่อ)

การปรับใช้มาตรฐาน PCI DSS เหล่านี้	ข้อมูลจำเพาะการนำไปปฏิบัติ	การปรับใช้ AIX Security Expert	ตำแหน่งของค่าและการตั้งค่าที่ จำเป็นสำหรับการปฏิบัติตาม (ถ้ามี)
	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`
	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`

ตารางที่ 6. การตั้งค่าที่เกี่ยวข้องกับมาตรฐานการปฏิบัติตามข้อกำหนด PCI DSS 2.0 (ต่อ)

การปรับใช้มาตรฐาน PCI DSS เหล่านี้	ข้อมูลจำเพาะการนำไปปฏิบัติ	การปรับใช้ AIX Security Expert	ตำแหน่งของค่าและการตั้งค่าที่ จำเป็นสำหรับการปฏิบัติตาม (ถ้ามี)
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`
	รักษาการเชื่อมต่อที่ปลอดภัยเมื่อโอนย้าย ข้อมูล	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
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 และ

การรักษาความปลอดภัย 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 และการใช้งานที่ไม่ถูกต้องและการเปิดเผยที่คาดการณ์อย่าง 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 7. 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** **ค่าส่งคืน:** ถ้าสำเร็จ คำสั่งนี้ออกโดยมีค่าเป็น 0 ถ้าไม่สำเร็จ คำสั่ง ออกโดยมีค่า 1
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

ตารางที่ 7. กฎ HIPAA และรายละเอียด การนำไปปฏิบัติ (ต่อ)

ส่วนของกฎการรักษาความปลอดภัย HIPAA	ข้อมูลจำเพาะการนำไปปฏิบัติ	การนำไปปฏิบัติ aixpert	คำสั่ง และค่าส่งคืน
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 หนึ่งในนั้นต้องเป็นตัวพิมพ์ใหญ่	**คำสั่ง:** **chsec -f /etc/security/user -s user -a minalpha=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	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	ให้แน่ใจว่ารหัสผ่านทั้งหมดไม่มีอักขระซ้ำกัน	**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

ตารางที่ 7. 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	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
164.308 (a) (5) (ii) (D) 164.312 (a) (2) (i)	การจัดการรหัสผ่าน (A) :ประยุกต์ใช้ กระบวนการสำหรับการสร้าง การเปลี่ยนแปลง และการป้องกันรหัสผ่าน	ระบุจำนวนอักขระขั้นต่ำที่ ไม่สามารถมีซ้ำจากรหัสผ่านคือ 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

ตารางที่ 7. 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	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
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	ระบุช่วงเวลาเพื่อพิมพ์รหัสผ่าน เป็น 30 วินาที	**คำสั่ง:** **chsec -f /etc/security/login.cfg -s usw -a logintimeout=30** **ค่า ส่งคืน:** ถ้าสำเร็จ สคริปต์นี้ออกโดยมีค่าเป็น 0 ถ้าไม่สำเร็จ คำสั่งออกโดยมีโค้ดระบุความผิดพลาดเป็น 1

ตารางที่ 7. 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	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 8. 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

ตารางที่ 8. ฟังก์ชัน HIPAA และรายละเอียด การนำไปปฏิบัติ (ต่อ)

ฟังก์ชัน HIPAA	ข้อมูลจำเพาะการนำไปปฏิบัติ	การนำไปปฏิบัติ aixpert	คำสั่ง และค่าส่งคืน
การเปิดใช้งาน FPM	เปลี่ยนแปลงสิทธิ์ไฟล์	เปลี่ยนแปลงสิทธิของไฟล์จากราย การ สิทธิ์ และไฟล์โดยใช้คำสั่ง **fpm**	**คำสั่ง**: **# fpm -l <level> -f <commands file>** **ค่าส่งคืน**: ถ้าสำเร็จ คำสั่งนี้ออกโดยมีค่าเป็น 0 ถ้าไม่สำเร็จ คำสั่ง ออกโดยมีค่า 1
การเปิดใช้งาน RBAC	สร้างผู้ใช้ **isso, so** และ **sa** และกำหนดบทบาทที่เหมาะสมให้กับผู้ใช้	แนะนำให้คุณสร้างผู้ใช้ **isso, so** และ **sa** กำหนดค่า บทบาทที่เหมาะสมให้แก่ผู้ใช้	**คำสั่ง**: **/etc/security/pscexpert/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
```

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 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 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) อยู่ ในไดเร็กทอรี `/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 9. 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 10. 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 114
ศึกษาเกี่ยวกับขั้นตอนการวางแผนและนำโปรไฟล์ความปลอดภัยและความเข้ากันได้อัตโนมัติของ PowerSC บนกลุ่มระบบตาม 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 หนึ่งเมธอดคือ ใช้คำสั่ง **pscxpert** และอีกหนึ่งเมธอดคือ ใช้ AIX Profile Manager กับ IBM Systems Director

เมื่อโปรไฟล์ความเข้ากันได้ถูกระบุ คุณสามารถเพิ่มไฟล์ เพิ่มเติมในรายการไฟล์เพื่อมอนิเตอร์โดยการรวมไฟล์ เพิ่มเติมในไฟล์ `/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

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

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

หมายเหตุ: รันคำสั่ง **pscxpert** อีกครั้งหลังจากการเปลี่ยนแปลงระบบหลักใดๆ เช่น การติดตั้ง หรือ อัพเดตซอฟต์แวร์ หาก รายการคอนฟิกูเรชันการรักษาความปลอดภัยเฉพาะ ไม่ถูกเลือกเมื่อรันคำสั่ง **pscxpert** อีกครั้ง รายการคอนฟิกูเรชันนั้นจะถูก ข้าม

แฟล็ก

รายการ	คำอธิบาย
-a	การตั้งค่าที่มีอ็อพชันของระดับการรักษาความปลอดภัย ที่เกี่ยวข้องจะถูกเขียนไปยังไฟล์ที่ระบุโดยแฟล็ก **-o** ในรูปแบบตัวย่อ คุณต้องระบุอ็อพชัน **-o** เมื่อคุณระบุอ็อพชัน**-a**
-c	ตรวจสอบการตั้งค่าการรักษาความปลอดภัยกับชุดของกฎ ที่ปรับใช้ก่อนหน้านี้ หากการตรวจสอบกฎล้มเหลว เวอร์ชันก่อนหน้า ของกฎจะถูกตรวจสอบ กระบวนการนี้จะดำเนินการต่อจนกว่า การตรวจสอบจะผ่าน หรือจนกว่าอินสแตนซ์ทั้งหมดของกฎที่ล้มหลว 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** เปลี่ยนแปลงค่าติดตั้งไปเป็นค่าติดตั้งดีฟอลต์ของ AIX **DoDv2.xml** ไฟล์นี้มาข้อกำหนดสำหรับเวอร์ชัน 2 ของค่าติดตั้ง Department of Defense Security Technical Implementation Guide (STIG) **DoDv2_to_AIXDefault.xml** เปลี่ยนแปลงค่าติดตั้งไปเป็นค่าติดตั้งดีฟอลต์ของ AIX **Hipaa.xml** ไฟล์นี้จะมีข้อกำหนดสำหรับการตั้งค่า Health Insurance Portability and Accountability Act (HIPAA) **PCI.xml** ไฟล์นี้จะมีข้อกำหนดสำหรับการตั้งค่า Payment card industry Data Security Standard **PCIv3.xml** ไฟล์นี้มีข้อกำหนดสำหรับค่าติดตั้ง Payment card industry Data Security Standard Version 3 **PCI_to_AIXDefault.xml** ไฟล์นี้จะเปลี่ยนแปลงการตั้งค่าเป็นการตั้งค่า AIX ดีฟลอต์ **PCIv3_to_AIXDefault.xml** ไฟล์นี้จะเปลี่ยนแปลงการตั้งค่าเป็นการตั้งค่า AIX ดีฟลอต์ **SOX-COBIT.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**

รายการ	คำอธิบาย
-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
-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 **หมายเหตุ:** คุณไม่สามารถใช้แฟล็ก `-u` เพื่อถอยกลับแอ็พพลิเคชันของ โปรไฟล์ Department of Defense Version 2 หรือโปรไฟล์ Payment Card Industry Version 3 เมื่อต้องการถอนโปรไฟล์เหล่านี้หลังจากที่คุณเพิ่มแล้ว ให้ใช้โปรไฟล์ที่มีไฟล์ `DoDv2_to_AIXDefault.xml` หรือไฟล์ `PCIv3_to_AIXDefault.xml` ตามลำดับ

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	มีบันทึกการติดตามของการตั้งค่าการรักษาความปลอดภัยที่ปรับใช้ ซึ่งไม่ได้ใช้มาตรฐาน 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

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

UNIX เป็นเครื่องหมายการค้าที่จดทะเบียนของ The Open Group ในสหรัฐฯ และประเทศอื่นๆ

ดัชนี

P

R

S

ก

ข

ค

ภ

ม

ร

พิมพ์ในสหรัฐอเมริกา