IBM

eserver

iSeries

คำแนะนำและทูลในการรักษาความปลอดภัยให้กับเซิร์ฟเวอร์ iSeries

เวอร์ชัน 5

SC09-3448-03

IBM

@server

iSeries

คำแนะนำและทูลในการรักษาความปลอดภัยให้กับเซิร์ฟเวอร์ iSeries

เวอร์ชัน 5

SC09-3448-03

หมายเหตุ

ก่อนใช้ข้อมูลนี้และผลิตภัณฑ์ที่ข้อมูลนี้สนับสนุน, โปรดแน่ใจว่าได้อ่านข้อมูลในหัวข้อ “ประกาศ” ในหน้า 183.

พิมพ์ครั้งที่แปด (เมษายน 2004)

| การพิมพ์ครั้งนี้ใช้กับเวอร์ชัน 5, รีลีส 3, โมดิฟิเคชัน 0 ของ IBM Operating System/400 (หมายเลขผลิตภัณฑ์ 5722-SS1) และใช้กับรี
| ลีส และโมดิฟิเคชันถัดจากนี้ไปจนกว่าจะมีการระบุเป็นอย่างอื่นในการพิมพ์ครั้งใหม่. เวอร์ชันนี้ไม่สามารถรันบนโมเดล RISC (reduced
| instruction set computer) และโมเดล CISC ได้ทุกรุ่น.

การพิมพ์ครั้งนี้ใช้แทนที่ SC09-3448-02.

สารบัญ

รูป

ตาราง

คำแนะนำและทูลในการรักษาความปลอดภัยให้กับเซิร์ฟเวอร์ iSeries (SC09-3448-03)

บทบาทของคอมพิวเตอร์ในองค์กรมีการเปลี่ยนแปลงอย่างรวดเร็ว. ผู้จัดการไอที, ผู้จัดทำซอฟต์แวร์, ผู้บริหารความปลอดภัย, และผู้ตรวจสอบมีความจำเป็นที่ต้องมีมุมมองใหม่ๆ ในหลายๆ สาขาซึ่งไม่เคยให้ความสำคัญมาก่อนในอดีตที่ผ่านมา. การรักษาความปลอดภัยของ iSeries ก็สมควรที่จะเป็นหนึ่งในจำนวนนั้น.

ระบบมีฟังก์ชันใหม่ๆ หลายอย่างที่แตกต่างจากแอ็พพลิเคชันด้านบัญชีแบบเดิมๆ เป็นอย่างมาก. ผู้ใช้สามารถเข้าสู่ระบบโดยวิธีใหม่ๆ อันได้แก่: ระบบเครือข่ายท้องถิ่น (LAN), ระบบสลับสาย (โทรศัพท์), ระบบไร้สาย, รวมไปถึงเครือข่ายทุกชนิด. บ่อยครั้ง, ที่ผู้ใช้ไม่เคยเห็นหน้าจอ sign-on. องค์กรหลายๆ แห่งมีการขยายตัวจนกลายเป็นองค์กรแบบขยาย “extended enterprise”, ที่ใช้เครือข่ายของตัวเอง หรือ ใช้อินเตอร์เน็ตอย่างใดอย่างหนึ่ง.

ทันใดนั้น, ดูเหมือนว่าระบบจะมีประตูทางเข้าหรือหน้าต่างติดต่อที่เปลี่ยนใหม่หมด ผู้จัดการระบบและผู้บริหารระบบความปลอดภัยจึงสมควรที่จะให้ความสนใจในการปกป้องทรัพย์สินข้อมูล ในสภาวะแวดล้อมที่เปลี่ยนแปลงอย่างรวดเร็วนี้.

ข้อมูลนี้ประกอบไปด้วยชุดคำแนะนำในการปฏิบัติ สำหรับการใช้คุณลักษณะพิเศษในการรักษาความปลอดภัยของ iSeries และสำหรับการจัดทำขั้นโพรซีเดอร์ในการปฏิบัติการที่คำนึงถึงการรักษาความปลอดภัยเป็นหลัก. คำแนะนำที่อยู่ในข้อมูลเหล่านี้สามารถใช้ได้กับการติดตั้งที่มีความจำเป็นในการรักษาความปลอดภัยและจำกัดช่องโหว่ในระดับทั่วไป. ข้อมูลเหล่านี้จะไม่ได้กล่าวถึงรายละเอียดโดยสมบูรณ์ของคุณลักษณะพิเศษในการรักษาความปลอดภัยที่มีอยู่ใน iSeries . ถ้าคุณต้องการอ่านเกี่ยวกับตัวเลือกเพิ่มเติม หรือต้องการทราบข้อมูลแบ็กกราวน์ที่สมบูรณ์ยิ่งขึ้น, สามารถศึกษาได้จากเอกสารที่ได้ให้รายละเอียดเอาไว้ใน บทที่ 17, “ข้อมูลที่เกี่ยวข้อง”, ในหน้า 179.

ข้อมูลเหล่านี้สามารถอธิบายถึงวิธีในการติดตั้งและใช้ทูลสำหรับการรักษาความปลอดภัยซึ่งเป็นส่วนหนึ่งของ OS/400. บทที่ 4, “การปรับแต่งค่าของ iSeries เพื่อใช้งาน Security Tools”, ในหน้า 31 และ “คำสั่งและเมนูสำหรับคำสั่งที่เกี่ยวกับความปลอดภัย” ในหน้า 32 โดยจะให้ข้อมูลอ้างอิงเกี่ยวกับทูลในการรักษาความปลอดภัยต่างๆ ไว้. ข้อมูลเหล่านี้จะมีตัวอย่างสำหรับการใช้งานทูลต่างๆ อยู่ด้วย.

ใครควรอ่านหนังสือเล่มนี้

เจ้าหน้าดูแลความปลอดภัย (secty officer) หรือ **ผู้บริหารความปลอดภัย (security administrator)** ที่รับผิดชอบในการรักษาความปลอดภัยบนระบบ. ซึ่งความรับผิดชอบนั้นโดยทั่วไปจะประกอบไปด้วยภารกิจดังต่อไปนี้:

- การตั้งค่าและการจัดการโปรไฟล์ผู้ใช้ (user profile)
- การตั้งค่าโดยทั่วไปที่มีผลต่อความปลอดภัยของระบบ

- การบริหารสิทธิในการใช้งาน (authority) ไปยังอ็อบเจ็กต์ต่างๆ
- การควบคุมและการตรวจสอบนโยบายด้านการรักษาความปลอดภัย (security policy)

ถ้าคุณต้องรับผิดชอบในการบริหารการรักษาความปลอดภัยของระบบ iSeries ระบบหนึ่งหรือหลายๆ ระบบ, ข้อมูลเหล่านี้มีไว้เพื่อคุณ. วิธีการในข้อมูลเหล่านี้จะมีการสมมติให้เป็นไปดังต่อไปนี้:

- คุณมีความคุ้นเคยกับขั้นตอนการปฏิบัติงานในระดับต้นของระบบ iSeries เช่น การ sign-on และการใช้คำสั่งต่างๆ .
- คุณมีความคุ้นเคยกับองค์ประกอบด้านการรักษาความปลอดภัยของ iSeries ได้แก่: ระดับความปลอดภัย, ค่าความปลอดภัยของระบบ, โปรไฟล์ผู้ใช้, และความปลอดภัยของอ็อบเจ็กต์.

  หมายเหตุ: บทที่ 1, "องค์ประกอบพื้นฐานของการรักษาความปลอดภัยแบบ iSeries", ในหน้า 3 มีการทบทวนเกี่ยวกับองค์ประกอบเหล่านี้. ถ้าองค์ประกอบระดับต้นเหล่านี้ยังใหม่สำหรับคุณ, ให้อ่านในหัวข้อ *Basic security and planning* ใน iSeries Information Center. โปรดดูที่ "สิ่งที่ต้องรู้ก่อนและข้อมูลที่เกี่ยวข้อง" ในหน้า xiii สำหรับรายละเอียดเพิ่มเติม.
- คุณได้ทำการเรียกการทำงานของการรักษาความปลอดภัยบนระบบของคุณ โดยการกำหนดค่าระดับความปลอดภัย (QSECURITY) ซึ่งเป็นค่ากำหนดของระบบให้มีค่าอย่างน้อยเท่ากับ 30.

IBM® ได้พัฒนาขีดความสามารถด้านการรักษาความปลอดภัยของ iSeries ให้ดีขึ้นอย่างต่อเนื่อง. เพื่อใช้ประโยชน์ในส่วนที่ดีขึ้นนี้, คุณควรจะประเมินแพ็กเกจโปรแกรมฟิกซ์ซึ่งเพิ่มขึ้น ที่มีอยู่ในปัจจุบันสำหรับรีลีสของคุณอย่างสม่ำเสมอ . เพื่อดูว่ามีโปรแกรมฟิกซ์ที่เกี่ยวข้องกับการรักษาความปลอดภัยหรือไม่.

จะใช้ข้อมูลนี้อย่างไร

ถ้าคุณยังไม่ได้จัดเตรียมระบบของคุณเพื่อใช้ทูลในการรักษาความปลอดภัย หรือถ้าคุณมี Security ToolKit for OS/400 ติดตั้งอยู่สำหรับรีลีสก่อนหน้านี้, ให้ปฏิบัติดังต่อไปนี้:

1. เริ่มต้นด้วย บทที่ 2, "iSeries Security Wizard และ eServer Security Planner", ในหน้า 11. ซึ่งจะอธิบายและแนะนำวิธีการใช้คุณลักษณะพิเศษเหล่านี้ในการเลือก security tools และวิธีในการเริ่มต้นใช้งาน tool นั้น.
2. สำหรับข้อมูลเกี่ยวกับการรักษาความปลอดภัยในระดับต้น, คุณสามารถทบทวนข้อมูลจาก Security Reference, ซึ่งมีออนไลน์อยู่ใน iSeries™ Information Center.

ข้อสังเกต

ข้อมูลเหล่านี้มีคำแนะนำ *มากมาย* สำหรับการรักษาความปลอดภัยให้กับ iSeries. ระบบของคุณอาจต้องการการปกป้องกันในเพียงบางส่วนเท่านั้น. ใช้ข้อมูลเหล่านี้ในการให้ความรู้กับตัวคุณเองเกี่ยวกับช่องโหว่ในการรักษาความปลอดภัยที่เป็นไปได้ และวิธีแก้ไข. จากนั้นให้มุ่งเน้นความพยายามไปยังส่วนที่วิกฤตที่สุดสำหรับระบบของคุณ.

สิ่งที่ต้องรู้ก่อนและข้อมูลที่เกี่ยวข้อง

ใช้ iSeries Information Center เป็นจุดเริ่มต้นในการค้นดูข้อมูลด้าน technical ของ iSeries .

คุณสามารถเข้าถึง Information Center ได้สองทาง คือ:

- จากเว็บไซต์ดังต่อไปนี้:

  `http://www.ibm.com/eserver/iseries/infocenter`

- สำหรับ *iSeries Information Center*, SK3T-4091-04 CD-ROM. CD-ROM นี้ จะมากับฮาร์ดแวร์ iSeries ใหม่ของคุณ หรือซอฟแวร์อัพเดต IBM Operating System/400 . คุณสามารถสั่งซื้อ CD-ROM ได้จาก IBM Publications Center:

  `http://www.ibm.com/shop/publications/order`

iSeries Information Center ประกอบด้วยข้อมูลใหม่และอัพเดตของ iSeries เช่นการติดตั้งซอฟต์แวร์ และฮาร์ดแวร์, Linux, WebSphere®, Java™, high availability, ฐานข้อมูล, โลจิคัลพาร์ติชัน, คำสั่ง CL และ application programming interfaces (APIs) ของระบบ. นอกจากนี้, ยังประกอบไปด้วยตัวแนะนำ และตัวค้นหา เพื่อช่วยในการวางแผน, แก้ปัญหาข้อบกพร่อง, และการตั้งค่าฮาร์ดแวร์ และซอฟต์แวร์ iSeries ของคุณ.

ทุกครั้งที่มีการสั่งซื้อฮาร์ดแวร์ใหม่, คุณจะได้รับซีดีรอมต่อไปนี้: *iSeries Setup and Operations CD-ROM*, SK3T-4098-02. CD-ROM นี้ประกอบด้วย IBM @server IBM e(logo)server iSeries Access for Windows และ EZ-Setup wizard. iSeries Access Family จะให้ชุดไคลเอ็นต์และเซิร์ฟเวอร์ที่มีประสิทธิภาพสูงสำหรับเชื่อมต่อพีซีไปยังเซิร์ฟเวอร์ iSeries. EZ-Setup wizard ช่วยทำงานในส่วนการติดตั้งของ iSeries โดยอัตโนมัติ.

วิธีการส่งความคิดเห็นของคุณ

การตอบกลับมาของท่านจะมีความสำคัญในการช่วยจัดเตรียมข้อมูลที่ถูกต้องและมีคุณภาพสูง. ถ้าคุณมีความคิดเห็นเกี่ยวกับหนังสือนี้หรือเอกสารคู่มืออื่นๆ ของ iSeries , สามารถกรอกแบบฟอร์มแสดงความคิดเห็นของผู้อ่านที่อยู่ด้านหลังของหนังสือนี้แล้วส่งกลับมา.

- ถ้าคุณต้องการที่จะส่งความคิดเห็นมาทางไปรษณีย์, ให้ใช้แบบฟอร์มแสดงความคิดเห็นของผู้อ่านแล้วส่งมาตามที่อยู่ที่พิมพ์อยู่บนด้านหลัง. ถ้าคุณส่งความคิดเห็นจากนอกประเทศสหรัฐอเมริกา, คุณสามารถให้แบบฟอร์มนั้นกับสำนักงานสาขาของ IBM หรือตัวแทนของIBM เพื่อให้ส่งต่อให้.
- ถ้าคุณต้องการส่งความคิดเห็นทาง FAX ให้ใช้หมายเลขดังต่อไปนี้หมายเลขใดหมายเลขหนึ่ง:
  - United States, Canada, และ Puerto Rico: 1-800-937-3430
  - ประเทศอื่นๆ : 1-507-253-5192
- หากคุณต้องการที่จะส่งทางอีเล็กทรอนิกส์, สามารถเลือกใช้อีเมล์แอดเดรสอันใดอันหนึ่งจากอีเมล์แอดเดรสดังต่อไปนี้:
  - ความคิดเห็นเกี่ยวกับหนังสือ:

    RCHCLERK@us.ibm.com

– ความคิดเห็นเกี่ยวกับศูนย์กลางข้อมูลของ iSeries :

RCHINFOC@us.ibm.com

ตรวจดูให้แน่ใจว่าได้ทำการรวมเอาสิ่งต่างๆ ดังต่อไปนี้ไว้ด้วยแล้ว :

- ชื่อของหนังสือหรือ หัวข้อเกี่ยวกับศูนย์กลางข้อมูลของ iSeries .
- ตัวเลขกำกับเอกสารของหนังสือ.
- เลขที่หน้า หรือหัวข้อของหนังสือที่คุณต้องการแสดงความคิดเห็น.

ส่วนที่ 1. ความปลอดภัยระดับต้น ของiSeries

บทที่ 1. องค์ประกอบพื้นฐานของการรักษาความปลอดภัยแบบ iSeries

ในบทนี้จะเป็นการทบทวนอย่างย่อๆ เกี่ยวกับส่วนประกอบพื้นฐานที่ทำงานประกอบกัน เป็นระบบความปลอดภัยของ iSeries. ในส่วนอื่นๆ ของหนังสือเล่มนี้ จะเป็นการเข้าสู่รายละเอียด ซึ่งจะมีคำแนะนำสำหรับการใช้ส่วนประกอบของระบบความปลอดภัย เพื่อที่จะสนองตอบต่อความต้องการขององค์กรของคุณ.

ระดับความปลอดภัย

คุณสามารถเลือกระดับความปลอดภัยที่คุณต้องการให้ระบบของคุณบังคับใช้โดยการตั้งค่า ระดับความปลอดภัยของระบบ (QSECURITY). ซึ่งจะมี 5 ระดับ ต่อไปนี้:

ระดับ 10:

ระบบจะไม่บังคับใช้เรื่องความปลอดภัยใดๆ . ไม่จำเป็นต้องมีรหัสผ่าน. ระบบจะทำการสร้างโปรไฟล์ใหม่ให้, หากไม่มีโปรไฟล์ผู้ใช้ที่ระบุอยู่ในระบบ เมื่อมีผู้ใดผู้หนึ่ง sign-on เข้ามา.

ข้อควรระวัง:

เริ่มต้นใน V4R3 และในรีลีสถัดไป, คุณไม่สามารถตั้งค่า QSECURITY เป็น 10. ถ้าระบบของคุณมีระดับความปลอดภัยปัจจุบันเป็น 10 มันจะยังคงค่าเป็น 10 เมื่อคุณติดตั้งเวอร์ชัน 4 รีลีส 3. แต่ถ้าคุณเปลี่ยนระดับความปลอดภัยเป็นค่าอื่นๆ, คุณจะไม่สามารถเปลี่ยนค่ากลับมาเป็นระดับ 10 ได้อีก. เนื่องจากระดับ 10 ไม่มีการป้องกันด้านความปลอดภัยใดๆ , จึงเป็นค่าที่ IBM ไม่แนะนำให้ใช้. **IBM จะไม่ให้การสนับสนุนต่อปัญหาที่เกิดขึ้นที่ระดับความปลอดภัย 10 นอกจากว่า ปัญหานั้นจะเกิดขึ้นได้ในระดับความปลอดภัยที่สูงขึ้นด้วย.**

ระดับ 20:

ระบบต้องการ user ID และรหัสผ่านในการ sign on. ระดับความปลอดภัย 20 มักถูกเรียกว่า **ความปลอดภัยของการ sign-on**.โดยดีฟอลต์, ผู้ใช้ทุกคนสามารถเข้าถึงทุกอ็อบเจ็กต์ได้ เนื่องจากผู้ใช้ทุกคนมีสิทธิพิเศษ *ALLOBJ.

ระดับ 30:

ระบบต้องการ user ID และรหัสผ่านในการ sign on. ผู้ใช้จะต้องมีสิทธิในการใช้อ็อบเจ็กต์เนื่องจากผู้ใช้ไม่มีสิทธิโดยดีฟอลต์. ระดับความปลอดภัยนี้เรียกว่า **ความปลอดภัยของรีซอร์ส**.

ระดับ 40:

ระบบต้องการ user ID และรหัสผ่านในการ sign on. นอกเหนือจาก ความปลอดภัยของรีซอร์ส, ระบบยังมีฟังก์ชัน **integrity protection**. ฟังก์ชัน Integrity protection ต่างๆ, อาทิ เช่น การตรวจสอบพารามิเตอร์ที่ใช้กับอินเตอร์เฟสเพื่อส่งไปยังระบบปฏิบัติการ, และมีไว้เพื่อปกป้องทั้งระบบของคุณ และอ็อบเจ็กต์ที่อยู่บนระบบจากการแทรกแซงของผู้ใช้ที่มี

ประสบการณ์. การติดตั้งโดยส่วนใหญ่, ระดับ 40 จะเป็นระดับความปลอดภัยที่แนะนำให้ใช้. เมื่อคุณได้รับระบบ iSeries ใหม่พร้อมกับรีลีส V4R5 หรือหลังจากนั้น, ระดับความปลอดภัยจะถูกตั้งค่าให้เป็น 40.

ระดับ 50:

ระบบต้องการ user ID และรหัสผ่านในการ sign on. ระบบบังคับใช้ทั้งความปลอดภัยของรีซอร์ส และ integrity protection ของระดับ 40, แต่เพิ่ม **integrity protection ที่ได้รับการพัฒนาแล้ว** , อาทิเช่น ข้อบังคับของการจัดการข้อความระหว่างโปรแกรมสถานะของระบบกับโปรแกรมสถานะของผู้ใช้. ความปลอดภัยระดับ 50 จะถูกใช้กับระบบ iSeries ที่ต้องการความปลอดภัยในระดับสูง.

หมายเหตุ: ระดับ 50 เป็นระดับที่เป็นที่ต้องการสำหรับการรับรองความปลอดภัย C2 (และการรับรองความปลอดภัย FIPS-140).

ในบทที่ 2 ของหนังสือ *iSeries Security Reference* จะมีข้อมูลเพิ่มเติมเกี่ยวกับระดับความปลอดภัย และอธิบายถึงการย้ายจากระดับความปลอดภัยหนึ่งไปยังอีกระดับหนึ่ง.

ค่าติดตั้งโกลบอล

ระบบของคุณมีค่าติดตั้งโกลบอลที่มีผลกระทบ ต่อการเข้าไปในระบบ และการที่ระบบปรากฏต่อผู้ใช้ในระบบอื่นๆ . ค่าติดตั้งเหล่านี้ประกอบด้วยค่าต่างๆ ดังนี้:

ค่ากำหนดของระบบในการรักษาความปลอดภัย:

ค่ากำหนดของระบบSecurity system values are used to control security on your system. โดยค่าเหล่านี้จะถูกแบ่งออกเป็นสี่กลุ่ม:

- ค่าความปลอดภัยของระบบโดยทั่วไป (general security system values)
- ค่าอื่นๆ ของระบบที่เกี่ยวกับความปลอดภัย (other system values related to security)
- ค่ากำหนดของระบบที่ควบคุมรหัสผ่าน (system values that control passwords)
- ค่ากำหนดของระบบที่ควบคุมระบบตรวจสอบ (system values that control auditing)

หลายหัวข้อใน book จะอธิบายถึงผลโดยนัยต่อความปลอดภัยจากค่าของระบบเหล่านี้. บทที่ 3 ในหนังสือ *iSeries Security Reference* จะอธิบายเกี่ยวกับค่าของระบบทุกตัวที่เกี่ยวข้องกับความปลอดภัย.

เน็ตเวิร์กแอ็ตทริบิวต์ (network attributes):

เน็ตเวิร์คแอ็ตทริบิวต์ควบคุมวิธีการที่ระบบของคุณมีส่วนร่วม (หรือเลือกที่จะไม่มีส่วนร่วม) กับระบบอื่นๆ ในเครือข่ายหนึ่ง. คุณสามารถอ่านเพิ่มเติมเกี่ยวกับแอตทริบิวต์ ของเครือข่ายได้ จากหนังสือ *Work Management* .

Subsystem descriptions และส่วนประกอบการจัดการระบบงานอื่นๆ :

ส่วนประกอบการจัดการระบบงาน จะพิจารณาถึงวิธีที่งานจะเข้าสู่ระบบ และสภาพแวดล้อมใดที่งานจะรันอยู่ภายในนั้น. มีหลายๆ หัวข้อในข้อมูลนี้กล่าวถึงความปลอดภัยโดยนัยอันเนื่องมาจากคุณค่าในการจัดการระบบงาน. ในหนังสือ *Work Management* จะมีข้อมูลที่สมบูรณ์.

Communications configuration:

communications configuration ของคุณจะส่งผลกระทบกับงานที่เข้าสู่ระบบคุณ. มีหลายๆ หัวข้อในข้อมูลนี้ที่มีคำแนะนำสำหรับการปกป้องระบบของคุณเมื่อต้องเข้าไปทำงานอยู่ในเครือข่าย.

โปรไฟล์ผู้ใช้

ผู้ใช้ระบบทุกคน **ต้อง** มีโปรไฟล์ผู้ใช้. คุณจะต้องสร้างโปรไฟล์ผู้ใช้ก่อนที่จะสามารถ sign on ได้. โปรไฟล์ผู้ใช้ยังสามารถถูกนำไปใช้ในการควบคุมการเข้าถึงเซอร์วิสทูล อาทิเช่น DASD และดัมพ์ของหน่วยความจำหลักได้อีกด้วย. ดู "การจัดการเซอร์วิสทูลต่างๆ" ในหน้า 67 สำหรับข้อมูลเพิ่มเติม.

โปรไฟล์ผู้ใช้เป็นเครื่องมือที่ทรงพลังและมีความยืดหยุ่น. มันควบคุมสิ่งที่ผู้ใช้สามารถทำได้ และปรับแต่งวิธีที่ระบบปรากฏแก่ผู้ใช้. หนังสือ *iSeries Security Reference* จะอธิบายถึงพารามิเตอร์ทุกตัวในโปรไฟล์ผู้ใช้.

โปรไฟล์กลุ่ม

โปรไฟล์กลุ่มเป็นโปรไฟล์ผู้ใช้ชนิดพิเศษ. คุณสามารถใช้โปรไฟล์กลุ่มในการกำหนดสิทธิสำหรับกลุ่มของผู้ใช้, แทนที่จะกำหนดสิทธิให้ผู้ใช้แต่ละราย. คุณยังสามารถใช้โปรไฟล์กลุ่มเป็นรูปแบบเมื่อทำการสร้าง โปรไฟล์ผู้ใช้ส่วนบุคคลโดยการใช้ฟังก์ชัน copy-profile หรือถ้าคุณใช้ iSeries Navigator คุณสามารถใช้เมนูของนโยบายเกี่ยวกับความปลอดภัย (security policy) ในการแก้ไขสิทธิผู้ใช้ .

ในบทที่ 5 และบทที่ 7 ของหนังสือ *iSeries Security Reference* จะมีข้อมูลเกี่ยวกับการวางแผนและการใช้โปรไฟล์กลุ่ม.

ความปลอดภัยของรีซอร์ส

ความปลอดภัยของรีซอร์ส (resource security) ในระบบอนุญาตให้คุณสามารถกำหนดว่าผู้ใดสามารถใช้อ็อบเจ็กต์ และอ็อบเจ็กต์เหล่านี้จะถูกใช้อย่างไร. ความสามารถในการเข้าถึงอ็อบเจ็กต์เรียกว่า **สิทธิ (authority)**. เมื่อคุณกำหนดสิทธิอ็อบเจ็กต์, คุณจะต้องให้สิทธิ ให้อำนาจแก่ผู้ใช้ของคุณอย่างพอเพียงเพื่อที่จะได้ทำงานได้โดยไม่ต้องให้อำนาจในการบราวซ์ (browse) และเปลี่ยนแปลง (change) ระบบ. สิทธิอ็อบเจ็กต์จะให้อนุญาตผู้ใช้สำหรับอ็อบเจ็กต์ที่จำเพาะเจาะจงและสามารถระบุว่าผู้ใช้สามารถทำอะไรได้บ้างกับอ็อบเจ็กต์นั้น. การจำกัดรีซอร์สของอ็อบเจ็กต์ทำได้โดยผ่านรายละเอียดของสิทธิผู้ใช้ (user authority), เช่น การเพิ่มเร็กคอร์ดหรือการเปลี่ยนแปลงเร็กคอร์ด. การใช้รีซอร์สของระบบทำได้โดย การให้ผู้ใช้เข้าถึงบางกลุ่มย่อย (subset) ของสิทธิที่ถูกกำหนดโดยระบบ เช่น: *ALL, *CHANGE, *USE, และ *EXCLUDE.

ไฟล์, โปรแกรม, ไลบรารี, และไดเร็กทอรี เป็นอ็อบเจ็กต์พื้นฐานของระบบที่ต้องการการป้องกันความปลอดภัยของรีซอร์ส, แต่คุณสามารถระบุสิทธิเป็นการเฉพาะสำหรับอ็อบเจ็กต์ใดๆ ในระบบได้.

บทที่ 5, “ปกป้องข้อมูลทรัพย์สินด้วยสิทธิอ็อบเจ็กต์”อธิบายเกี่ยวกับความสำคัญของการจัดเตรียมสิทธิอ็อบเจ็กต์ในระบบของคุณ. ในบทที่ 5 ของหนังสือ *iSeries Security Reference* อธิบายถึงอ็อพชันในการกำหนดความปลอดภัยของรีซอร์ส.

ขอบเขตของการเข้าไปใช้ Program Function

ขอบเขตของการเข้าไปใช้ Program Function อนุญาตให้คุณเตรียมการรักษาความปลอดภัยสำหรับโปรแกรมในกรณีที่คุณไม่มีอ็อบเจ็กต์ iSeries ในการรักษาความปลอดภัยให้กับโปรแกรม. ก่อนที่จะมีการเพิ่มการจำกัดการเข้าถึงโปรแกรมฟังก์ชันไว้ใน V4R3, คุณสามารถทำเช่นนี้ได้โดยการสร้าง authorization list หรืออ็อบเจ็กต์อื่นๆ , และตรวจสอบสิทธิในอ็อบเจ็กต์ เพื่อควบคุมการเข้าถึงโปรแกรมฟังก์ชัน. ขณะนี้คุณสามารถใช้การจำกัดการเข้าถึงโปรแกรมฟังก์ชัน เพื่อควบคุมการเข้าถึง แอ็พพลิเคชัน, ส่วนหนึ่งของแอ็พพลิเคชัน, หรือฟังก์ชันต่างๆ ภายในโปรแกรมได้ง่ายขึ้นกว่าเดิม.

มีวิธีสองวิธีด้วยกันที่คุณสามารถใช้ในการควบคุมการเข้าไปใช้แอ็พพลิเคชันฟังก์ชันผ่านทางเนวิเกเตอร์ iSeries. วิธีแรกใช้การสนับสนุนของ Application Administration:

1. คลิ๊กปุ่มขวามือบนระบบที่มีฟังก์ชันที่คุณต้องการจะเปลี่ยนค่าในการเข้าไปใช้ฟังก์ชันของมัน.
2. เลือก **Application Administration**.
3. ถ้าคุณอยู่บนระบบ administration, เลือก **Local Settings**. หรือไม่, ก็ดำเนินการในขั้นต่อไป.
4. เลือกฟังก์ชันที่สามารถบริหารได้.
5. เลือก **Default Access**, ถ้าสามารถใช้ได้. โดยการเลือกดังนี้, คุณอนุญาตให้ผู้ใช้ทั้งหมดเข้าไปใช้ฟังก์ชันโดยดีฟอลต์.
6. เลือก **All Object Access**, ถ้าสามารถใช้ได้. โดยการเลือกดังนี้, คุณอนุญาตให้ผู้ใช้ทั้งหมดที่มีสิทธิพิเศษของระบบในอ็อบเจ็กต์ทั้งหมดเพื่อเข้าไปใช้ฟังก์ชันนี้.
7. เลือก **Customize**, ถ้าสามารถใช้ได้. ใช้ปุ่ม **Add** และ**Remove** ที่อยู่บนไดอะล็อก **Customize Access** เพื่อทำการเพิ่มหรือลบผู้ใช้หรือกลุ่มในรายการ **Access allowed** และ **Access denied** .
8. เลือก **Remove Customization**, ถ้าสามารถใช้ได้. โดยการเลือกดังนี้, คุณลบความสามารถในการเข้าไปใช้งานใดๆ ที่ตั้งค่าเอาไว้ตามความต้องการสำหรับฟังก์ชันที่ถูกเลือกไว้แล้ว.
9. กดปุ่ม **OK** เพื่อปิดไดอะล็อก **Application Administration** .

วิธีที่สองของการควบคุมการเข้าไปใช้งานของผู้ใช้ซึ่งจะเกี่ยวข้องกับการสนับสนุนผู้ใช้และกลุ่มของเนวิเกเตอร์ iSeries :

1. ในเนวิเกเตอร์ iSeries , ขยาย **ผู้ใช้และเนวิเกเตอร์** .
2. เลือก **All Users**, **Groups**, หรือ **Users Not in a Group** เพื่อแสดงรายชื่อของผู้ใช้และกลุ่ม.
3. กดปุ่มขวามือเลือกผู้ใช้ หรือกลุ่ม, และเลือก **Properties**.
4. กด **Capabilities**.
5. กดที่แท็บ **Applications**.
6. ใช้หน้านี้ในการเปลี่ยนแปลงค่าที่ตั้งไว้ในการเข้าไปใช้งานสำหรับผู้ใช้หรือกลุ่ม.
7. กดเลือก **OK** สองครั้งเพื่อปิดไดอะล็อก**Properties**.

โปรดดูที่ “iSeries Navigator security” ในหน้า 169 สำหรับข้อมูลเพิ่มเติมในฉบับที่เกี่ยวกับการรักษาความปลอดภัยของเนวิเกเตอร์ iSeries .

หากคุณเป็นผู้เขียนแอ็พพลิเคชัน, คุณสามารถใช้ APIs ของการจำกัดการเข้าถึงโปรแกรมฟังก์ชันทำสิ่งต่อไปนี้:

- ลงทะเบียน (register) ฟังก์ชัน
- เรียกข้อมูลเกี่ยวกับฟังก์ชัน
- กำหนดผู้ที่สามารถหรือไม่สามารถใช้ฟังก์ชัน
- ตรวจสอบว่าผู้ใช้ได้รับอนุญาตให้ใช้ฟังก์ชันหรือไม่

หมายเหตุ: การสนับสนุนนี้ **ไม่ได้** มาแทนที่ ความปลอดภัยของรีซอร์ส. การจำกัดการเข้าถึงโปรแกรมฟังก์ชันไม่ได้ป้องกันผู้ใช้จากการเข้าถึงรีซอร์ส (เช่น ไฟล์ หรือโปรแกรม) จากส่วนอินเตอร์เฟสอื่นๆ .

เพื่อที่จะใช้การสนับสนุนนี้ภายในแอ็พพลิเคชัน, ผู้จัดทำแอ็พพลิเคชัน จะต้องลงทะเบียนฟังก์ชันเมื่อแอ็พพลิเคชันถูกติดตั้ง. ฟังก์ชันที่ลงทะเบียนไว้ คือ บล็อกของรหัสคำสั่ง (code block) ที่ทำงานบางอย่างในแอ็พพลิเคชัน. เมื่อมีการรัน แอ็พพลิเคชันโดยผู้ใช้, แอ็พพลิเคชันนั้นจะเรียก API ก่อนที่แอ็พพลิเคชันเรียกบล็อกของรหัสคำสั่ง. API จะเรียก check usage API เพื่อตรวจสอบดูว่าผู้ใช้ได้รับอนุญาตให้ใช้ฟังก์ชันนั้นหรือไม่. ถ้าผู้ใช้ได้รับอนุญาตให้ใช้ฟังก์ชันที่ลงทะเบียน, บล็อกของรหัสคำสั่งนั้นจะทำงาน. ถ้าผู้ใช้นั้นไม่ได้รับอนุญาตให้ใช้ฟังก์ชันนั้น, ผู้ใช้จะถูกป้องกันไม่ให้ใช้บล็อกของ รหัสคำสั่งนั้น.

หมายเหตุ: API ทำการลงทะเบียน ID ขนาด 30 อักขระของแต่ละฟังก์ชัน ลงในฐานข้อมูลของการลงทะเบียน (WRKREGINF). แม้ว่าจะไม่มี exit point ที่สัมพันธ์กับ ฟังก์ชัน ID ที่ถูกใช้โดย APIs จำกัดการเข้าถึงฟังก์ชัน, แต่ก็จำเป็นจะต้องมี exit point. เพื่อลงทะเบียนทุกอย่างในรีจิสตรี้ (registry), คุณจำเป็น **จำเป็นต้อง** ให้ชื่อรูปแบบจุดทางออก (exit point format name). การทำฟังก์ชันลงทะเบียน API นี้ทำให้เกิดชื่อที่เป็นแบบดัมมีฟอร์แม็ตและจะใช้ดัมมีฟอร์แม็ตนี้สำหรับฟังก์ชันทั้งหมดที่ได้รับการลงทะเบียน. ทำให้ไม่มีการเรียกจุดทางออกของโปรแกรม, เนื่องจากชื่อเป็นแบบดัมมีฟอร์แม็ต.

ในการกำหนดผู้ที่ได้รับอนุญาตหรือไม่ได้รับอนุญาตให้เข้าถึงฟังก์ชัน. ผู้ดูแลสามารถเลือกใช้ API ในการควบคุมการเข้าไปใช้งาน Program Function หรือใช้ GUI ของ Application Administration ที่เป็นของเนวิเกเตอร์ iSeries อย่างใดอย่างหนึ่ง. หนังสือคู่มือ *iSeries server API Reference* มีข้อมูลที่เกี่ยวกับขอบเขตของการเข้าไปใช้งาน program function ที่เป็น API. และสำหรับข้อมูลเพิ่มเติมเกี่ยวกับ การควบคุมการเข้าไปใช้ฟังก์ชัน, ดูได้ใน “iSeries Navigator security” ในหน้า 169.

การตรวจสอบความปลอดภัย

เหตุผลที่ต้องมีการตรวจสอบความปลอดภัยของระบบ ได้แก่:

- เพื่อประเมินว่าแผนความปลอดภัยสมบูรณ์หรือไม่.
- เพื่อให้แน่ใจว่าการควบคุมความปลอดภัยที่วางแผนไว้ยังทำงานได้ดี. การตรวจสอบประเภทนี้มักจะกระทำโดยเจ้าหน้าที่รักษาความปลอดภัยระบบ โดยเป็นส่วนหนึ่งของการจัดการความ

ปลอดภัยประจำวัน. การตรวจสอบที่ทำ, โดยมีรายละเอียดมากขึ้นในบางครั้ง, เป็นส่วนหนึ่งของการตรวจสอบด้านความปลอดภัยเป็นครั้งคราว ที่กระทำโดยผู้ตรวจสอบภายในหรือภายนอกองค์กร.

- เพื่อให้แน่ใจว่าระบบยังอยู่ในสภาพเดิมภายใต้การเปลี่ยนแปลงของสภาพแวดล้อม ของระบบ. ตัวอย่างของการเปลี่ยนแปลงที่มีผลกระทบต่อความปลอดภัย ได้แก่:
  - อ็อบเจ็กต์ที่สร้างโดยผู้ใช้ระบบ
  - ผู้ใช้ใหม่ที่เพิ่มขึ้นในระบบ
  - การเปลี่ยนความเป็นเจ้าของอ็อบเจ็กต์ (โดยไม่ปรับการให้สิทธิ)
  - การเปลี่ยนความรับผิดชอบ (เปลี่ยนกลุ่มผู้ใช้)
  - สิทธิชั่วคราว (เวลาที่ถอนสิทธิไม่เหมาะสม)
  - ผลิตภัณฑ์ใหม่ที่ติดตั้ง
- การเตรียมรับเหตุการณ์ในอนาคต, เช่น การติดตั้งแอ็พพลิเคชันใหม่, การย้าย ไปสู่ระดับความปลอดภัยที่สูงขึ้น, หรือการจัดเตรียมเครือข่ายการสื่อสาร.

เทคนิคที่อธิบายนี้เหมาะสมกับทุกสถานการณ์ที่กล่าวมา. สิ่งที่คุณจะตรวจสอบ และความถี่ในการตรวจสอบนั้น จะขึ้นกับขนาดและความต้องการด้านความปลอดภัยขององค์กรของคุณ.

การตรวจสอบความปลอดภัย ทำงานโดยใช้คำสั่งในระบบของคุณและเข้าไปในบันทึกการทำงานและข้อมูลเจอร์นัล. คุณสามารถสร้างโปรไฟล์พิเศษเพื่อถูกนำไปใช้โดยใครคนใดคนหนึ่งที่ทำการตรวจสอบความปลอดภัยของระบบของคุณ. โปรไฟล์ของผู้ตรวจสอบจำเป็นจะต้องใช้สิทธิพิเศษที่เป็น *AUDIT ในการเปลี่ยนแปลงคุณสมบัติของระบบตรวจสอบในระบบนั้นๆ. งานในการตรวจสอบงานส่วนที่ได้แนะนำไว้ในบทนี้ต้องการโปรไฟล์ผู้ใช้ที่มีสิทธิพิเศษ *ALLOBJ และ *SECADM. ตั้งรหัสผ่านสำหรับโปรไฟล์ผู้ที่ทำการตรวจสอบให้เป็น *NONE เมื่อระยะเวลาของการตรวจสอบสิ้นสุดลง.

สำหรับรายละเอียดเพิ่มเติมเกี่ยวกับการตรวจสอบความปลอดภัย ดูได้ในบทที่ 9, ในหนังสือ *Security Reference*.

ตัวอย่าง: รายงานเกี่ยวกับแอ็ตทริบิวต์ของความปลอดภัยในระบบ

รูปที่ 1 ในหน้า 9 แสดงตัวอย่างของเอาต์พุตจากคำสั่ง Print System Security Attributes (PRTSYSSECA). รายงานแสดงถึงค่าที่กำหนดไว้สำหรับค่ากำหนดของระบบที่เกี่ยวข้องกับความปลอดภัย และเน็ตเวิร์กแอ็ตทริบิวต์ที่แนะนำให้ใช้กับระบบที่มีความต้องการด้านความปลอดภัยแบบปกติ. และยังแสดงถึงค่าติดตั้งปัจจุบันในระบบของคุณ.

หมายเหตุ: คอลัมน์ *Current Value* ในรายงานแสดงถึงค่าติดตั้งปัจจุบันในระบบของคุณ.เปรียบเทียบค่านี้กับค่าที่แนะนำให้เพื่อดูว่า ที่ใดที่คุณอาจมีจุดอ่อนด้านความปลอดภัย.

```
System Security Attributes

System Value
Name            Current value          Recommended value
QALWOBJRST      *NONE                  *NONE
QALWUSRDMN      *ALL                   QTEMP
QATNPGM         QEZMAIN   QSYS         *NONE
QAUDENDACN      *NOTIFY                *NOTIFY
QAUDFRCLVL      *SYS                   *SYS
QAUDCTL         *AUDLVL                *AUDLVL   *OBJAUD
QAUDLVL         *SECURITY              *AUTFAIL  *CREATE
                                       *DELETE   *SECURITY
                                       *SAVRST   *NOQTEMP
```

รูปที่ 1. System Security Attributes Report - ตัวอย่าง (ส่วนที่ 1 ของ 4)

```
QAUTOCFG        0                      0
QAUTORMT        1                      0
QAUTOVRT        9999                   0
QCMNRCYLMT      0 0                    0 0
QCRTAUT         *CHANGE                Control at library level.
QCRTOBJAUD      *NONE                  Control at library level.
QDEVRCYACN      *DSCMSG                *DSCMSG
QDSCJOBITV      120                    120
QDSPSGNINF      1                      1
QINACTITV       60                     60
QINACTMSGQ      *ENDJOB                *ENDJOB
QLMTDEVSSN      0                      1
QLMTSECOFR      0                      1
QMAXSGNACN      2                      3
QMAXSIGN        3                      3
```

รูปที่ 1. System Security Attributes Report - ตัวอย่าง (ส่วนที่ 2 ของ 4)

```
QPWDEXPITV      60                  60
QPWDLMTAJC      1                   1
QPWDLMTCHR      *NONE               AEIOU@$#
QPWDLMTREP      1                   2
QPWDLVL         0
QPWDMAXLEN      8                   8
QPWDMINLEN      6                   6
QPWDPOSDIF      1                   1
QPWDRQDDGT      1                   1
QPWDRQDDIF      0                   1
QPWDVLDPGM      *NONE               *NONE
QRETSVRSEC      0                   0
QRMTIPL         0                   0
QRMTSIGN        *FRCSIGNON          *FRCSIGNON
QSECURITY       50                  50
QSHRMEMCTL      1                   0
QSRVDMP         *DMPUSRJOB          *NONEQUSEADPAUT      *NONE                  CRTAUTL AUTL(QUSEADPAUT
                                    CHGOBJOWN OBJ(QUSEADPAUT) OBJTYPE(*AUTL)
                                    CHGSYSVAL SYSVAL(QUSEADPAUT) VALUE(QUSEADPAUT)
QVFYOBJRST      1                   3
```

รูปที่ 1. System Security Attributes Report - ตัวอย่าง (ส่วนที่ 3 ของ 4)

```
แอ็ตทริบิวต์ของความปลอดภัยในระบบ
เน็ตเวิร์กแอ็ตทริบิวต์
 ชื่อ                        ค่าปัจจุบัน                    ค่าที่แนะนำให้ใช้
DDMACC          *OBJAUT             *REJECT
JOBACN          *FILE               *REJECT
PCSACC          *OBJAUT             *REJECT
```

รูปที่ 1. System Security Attributes Report - ตัวอย่าง (ส่วนที่ 4 ของ 4)

บทที่ 2. iSeries Security Wizard และ eServer Security Planner

iSeries server Security Wizard และ eServer Security Planner tools สามารถช่วยคุณ ตัดสินใจได้ว่าค่าความปลอดภัยค่าใดที่จะถูกนำมาใช้ให้เกิดผลกับเซิร์ฟเวอร์ iSeries. การใช้ iSeries server Security Wizard ใน iSeries Navigator ทำให้คุณสร้างรายงานแสดงความต้องการใน ด้านการรักษาความปลอดภัยของคุณ โดยอาศัยคำตอบที่คุณเลือก. จากนั้นคุณยังสามารถใช้รายงานนี้ ในการปรับตั้งค่าความปลอดภัยของระบบของคุณ.

การใช้ iSeries Security Wizard หรือ eServer Security Planner เพื่อช่วยให้คุณวางแผนรับมือ และใช้นโยบายเกี่ยวกับความปลอดภัยในระดับต้นสำหรับเซิร์ฟเวอร์ iSeries ของคุณ. จุดมุ่งหมายของทูลทั้งสองก็คือการอำนวยความสะดวกในการนำมาปฏิบัติใช้ และการควบคุมการรักษาความปลอดภัยบนระบบของคุณ. ส่ว ของ wizard, ซึ่งมีอยู่ในส่วนของ OS/400®, จะถามคำถามระดับสูงหลายคำถามเกี่ยวกับสภาวะแวดล้อมเซิร์ฟเวอร์ของคุณ, และจากคำตอบของคุณ, wizard จะให้คำแนะนำกับคุณที่ wizard สามารถนำมาใช้กับระบบของคุณได้ในทันที.

eServer Security Planner เป็นเวอร์ชันออนไลน์ของ Security Wizard. ซึ่งยอมให้คุณเลือกตัวเลือกต่างๆ ตามความต้องการด้านความปลอดภัยของคุณ และจากนั้น จะสร้างรายงานในการแนะนำว่าคุณต้องการฟีเจอร์อะไรบ้างในการรักษาความปลอดภัยให้กับระบบของคุณ.

eServer Security Planner เป็นเวอร์ชันบนเว็บของวิซาร์ด. มันจะให้คำแนะนำในการนำการรักษาความปลอดภัยมาปฏิบัติใช้บนระบบของคุณ, เหมือนกับว่ามีผู้วิเศษคอยช่วยเหลือ. อย่างไรก็ตาม, ผู้ที่ให้คำแนะนำไม่สามารถทำตามคำแนะนำเหล่านี้ด้วยตัวเองได้. เรียกได้ว่า, มันส่งเอาต์พุตรายการที่เป็นค่าของการรักษาความปลอดภัยของระบบและแอ็ตทริบิวต์อื่นๆ ที่คุณสมควรที่จะประยุกต์ใช้บนระบบของคุณ, โดยปฏิบัติตามคำตอบที่คุณได้ตอบคำถามของ advisor.

Security Wizard

ทำการตัดสินใจว่าค่ากำหนดของระบบเกี่ยวกับความปลอดภัยของ iSeries ใดที่คุณสมควรใช้กับงานของคุณ ที่สามารถก่อให้เกิดความสับสนได้. ถ้าคุณยังใหม่ต่อการนำการรักษาความปลอดภัยมาปฏิบัติบนเซิร์ฟเวอร์ iSeries , หรือสภาวะแวดล้อมที่คุณรันเซิร์ฟเวอร์ iSeries เพิ่งจะมีการเปลี่ยนแปลงเกิดขึ้น, Security Wizard สามารถช่วยคุณในการตัดสินใจได้

wizard คืออะไร?

- wizard คือ เครื่องมือที่ออกแบบมาให้กับผู้ใช้งานระดับเริ่มต้นในการติดตั้ง หรือปรับแต่งค่าบางอย่างของระบบ.
- wizard จะทำการขอข้อมูลจากผู้ใช้โดยการตั้งคำถาม. คำตอบของแต่ละคำถามจะเป็นหลักในการตัดสินใจว่าคำถามใดจะถูกถามถัดไป.
- เมื่อ wizard ได้ถามทุกคำถามแล้ว, หน้าจอจะมีการแสดงไดอะล็อกสิ้นสุด. ผู้ใช้สามารถกดปุ่ม **Finish** เพื่อติดตั้งและปรับค่ารายการนั้นๆ .

จุดมุ่งหมายของ Security Wizard

จุดมุ่งหมายของ Security Wizard คือการปรับแต่งค่า, ซึ่งจะขึ้นอยู่กับการตอบรับของผู้ใช้ดังต่อไปนี้เป็นหลัก.

- ค่ากำหนดของระบบที่เกี่ยวกับความปลอดภัยและเน็ตเวิร์กแอ็ตทริบิวต์.
- การรักษาความปลอดภัยที่เกี่ยวข้องการรายงานผลสำหรับการมอนิเตอร์ระบบ.
- การTo generate an Administrator Information Report and a User Information Report:
  - Administrator Information Report ประกอบด้วยคำแนะนำเกี่ยวกับค่าติดตั้ง ความปลอดภัยและขั้นตอนที่จะต้องทำ เพื่อที่จะทำให้คำแนะนำนั้นเป็นผล.
  - User Information Report ประกอบด้วยข้อมูลที่สามารถใช้ในนโยบายความปลอดภัย ของธุรกิจ (Business Security Policy). ตัวอย่างเช่น, กฎในการสร้างรหัสผ่าน จะถูกรวมอยู่ในรายงานนี้ด้วย.
- การเตรียมค่าติดตั้งที่แนะนำให้ใช้กับหัวข้อเกี่ยวกับการรักษาควมที่แตกต่างกันไปภายในระบบ.

จุดมุ่งหมายของ Security Wizard

- จุดมุ่งหมายของ Security Wizard คือ:
  - ตัดสินใจเกี่ยวกับการตั้งความปลอดภัยของระบบที่ควรเป็น, โดยอาศัยคำตอบของผู้ใช้จากคำถามของ Wizard, จากนั้นปรับแต่งค่าเหล่านั้นเมื่อเหมาะสม.
  - wizard สร้างรายงานที่มีข้อมูลโดยละเอียด โดยมีรายการดังนี้.
    - รายงานอธิบายเกี่ยวกับคำแนะนำของ Wizard.
    - รายงานที่มีรายละเอียดขั้นตอนที่จะต้องทำตามก่อนที่จะนำไปปฏิบัติ.
    - รายงานที่มีรายการข้อมูลที่เกี่ยวข้อง เพื่อกระจายให้กับผู้ใช้ของระบบ.
- ทำหน้าที่วางนโยบายความปลอดภัยขั้นพื้นฐานให้ทำงานในระบบของคุณ.
- Wizard แนะนำรายงานการตรวจสอบรายเดือน (audit journal report) ที่คุณควร จะตั้งเวลาใช้งานไว้อย่างสม่ำเสมอ. เมื่อใช้งานสม่ำเสมอ, รายงานเหล่านี้จะช่วยในเรื่อง:
  - ทำให้มั่นใจว่านโยบายความปลอดภัยได้รับการทำตาม.
  - ทำให้มั่นใจว่านโยบายความปลอดภัยถูกเปลี่ยนแปลงโดยการอนุญาตของคุณเท่านั้น.
  - รายงานที่มีเป็นระยะๆ จะช่วยให้คุณมองเห็นเหตุการณ์ที่เกี่ยวข้องกับความปลอดภัยในระบบของคุณ.
- Wizard อนุญาตให้คุณบันทึกคำแนะนำหรือประยุกต์คำแนะนำบางส่วนหรือทั้งหมดของระบบของคุณ.

หมายเหตุ: Security Wizard สามารถใช้มากกว่าหนึ่งครั้งในระบบเดียวกัน เพื่อให้ผู้ใช้ที่อาจมีการติดตั้งครั้งก่อนๆ ตรวจสอบความปลอดภัยที่ใช้อยู่ในปัจจุบัน. Security Wizard สามารถถูกเรียกใช้ได้จากระบบ V3R7 (เมื่อเนวิเกเตอร์ iSeries ได้รับการแนะนำ) แต่นั้นเป็นต้นมา.

การใช้ iSeries Navigator, คุณต้องมี IBM iSeries Access for Windows® ติดตั้งบนเครื่องพีซี Windows 95/NT และมีการเชื่อมต่อจากพีซีเครื่องนั้นไปที่เซิร์ฟเวอร์ iSeries . ผู้ใช้ของ Wizard ต้องถูกเชื่อมต่อไปยังเซิร์ฟเวอร์ iSeries . และผู้ใช้จะต้องมี user ID ที่มีสิทธิพิเศษ *ALLOBJ, *SECADM, *AUDIT และ *IOSYSCFG. สำหรับความช่วยเหลือในการเชื่อมต่อพีซี Windows

95/NT ของคุณเข้ากับระบบ iSeries ของคุณ, ให้ศึกษาจากหัวข้อ IBM iSeries Access for Windows ใน Information Center (โปรดดูที่ “สิ่งที่ต้องรู้ก่อนและข้อมูลที่เกี่ยวข้อง” ในหน้า xiii สำหรับรายละเอียด).

เพื่อที่จะใช้งาน Security Wizard, ให้ทำตามขั้นตอนต่อไปนี้:

1. ในเนวิเกเตอร์ iSeries, ให้ทำการขยายเนื้อที่เซิร์ฟเวอร์ของคุณ.
2. คลิ๊กขวาบน **Security**, และเลือก **Configure**.
   - เมื่อผู้ใช้เริ่มการทำงานของตัวเลือก **Security** ของเนวิเกเตอร์ iSeries คำร้องขอจะถูกส่งไปยังเซิร์ฟเวอร์ iSeries เพื่อตรวจสอบสิทธิพิเศษของผู้ใช้.
   - ถ้าผู้ใช้ไม่มีสิทธิพิเศษทั้งหมดที่ต้องมี (*ALLOBJ, *AUDIT, *IOSYSCFG, *SECADM) ผู้ใช้ก็จะไม่เห็นอ็อพชัน **Configure** และไม่สามารถใช้งาน Security Wizard ได้.
3. สมมุติว่าผู้ใช้มีอำนาจที่ต้องการ:
   - ผลลัพธ์จากการใช้ Wizard ครั้งก่อนจะถูกเรียกขึ้นมา.
   - ค่าเกี่ยวกับความปลอดภัยในปัจจุบันจะถูกเรียกขึ้นมา.

Security Wizard จะแสดงหนึ่งในสามหน้าจอต้อนรับ. หน้าจอต้อนรับที่แสดงให้เห็นนั้น ขึ้นกับเงื่อนไขดังนี้:

- wizard ยังไม่เคยถูกรันสำหรับเซิร์ฟเวอร์ iSeries ที่เป็นเป้าหมาย.
- Wizard เคยถูกเรียกใช้มาก่อน และการเปลี่ยนแปลงด้านความปลอดภัยยังไม่ได้ เกิดขึ้น.
- Wizard เคยถูกเรียกใช้มาก่อน และการเปลี่ยนแปลงด้านความปลอดภัยได้ถูกทำให้ เกิดผลแล้ว.

ถ้าคุณไม่ได้ใช้เนวิเกเตอร์ iSeries, คุณยังสามารถที่จะขอความช่วยเหลือในการวางแผนเกี่ยวกับการรักษาความปลอดภัยที่คุณต้องการได้. The eServer Security Planner เป็นเวอร์ชันออนไลน์ของ Security Wizard, แต่มีข้อแตกต่างเพียงอย่างเดียว. advisor จะไม่เปลี่ยนแปลงระบบของคุณโดยอัตโนมัติ. แต่จะสร้างรายงานที่มีคำแนะนำเกี่ยวกับความปลอดภัย โดยอาศัยคำตอบของคุณ. ในการเข้าถึง eServer Security Planner, ให้ไปที่ eServer Information Center:

`http://publib.boulder.ibm.com/eserver/`

---

eServer Security Planner

eServer Security Planner เป็นเวอร์ชันออนไลน์ของ Security Wizard. โดยจะถามคำถามเช่นเดียวกับที่ Security Wizard ถาม, และอาศัยคำตอบของคุณ, ในการ สร้างคำแนะนำเดียวกัน. ข้อแตกต่างหลักระหว่างเครื่องมือทั้งสอง คือ:

- eServer Security Planner **ไม่**—
  - สร้างรายงาน.
  - เปรียบเทียบค่าติดตั้งในปัจจุบันกับค่าที่แนะนำ.
  - ตั้งค่ากำหนดของระบบให้โดยอัตโนมัติ.
- คุณไม่สามารถนำคำแนะนำจาก eServer Security Planner ไปใช้ได้.

eServer Security Planner สร้าง CL program เพื่อให้คุณทำการ cut-and-paste และแก้ไขสำหรับการใช้งานของคุณเพื่อที่จะทำการปรับแต่งค่าความปลอดภัยโดยอัตโนมัติ. คุณสามารถลิงก์โดยตรงไป

ยัง iSeries server documentation จาก eServer Security Planner. ซึ่งจะให้ข้อมูลเกี่ยวกับค่าของระบบ หรือรายงานที่ช่วยคุณตัดสินใจว่าค่าเหล่านี้ เหมาะสมกับสภาพแวดล้อมของคุณหรือไม่.

สำหรับการใช้งาน eServer Security Planner, ใช้อินเตอร์เน็ตบราวเซอร์ชี้ไปที่ URL ต่อไปนี้:

`http://publib.boulder.ibm.com/eserver/`

บทที่ 3. ควบคุมการ sign-on แบบโต้ตอบ

เมื่อคุณนึกถึงข้อจำกัดในการเข้าระบบของคุณ, ซึ่งพูดให้ชัดเจน ก็คือ จอภาพ Sign-On. ต่อไปนี้เป็นตัวเลือกที่คุณสามารถใช้เพื่อทำให้ผู้อื่น sign on เข้าไปในระบบของคุณยากขึ้นโดยการใช้หน้าจอ Sign On.

ตั้งกฎการใช้รหัสผ่าน

เพื่อรักษาความปลอดภัยให้กับการ sign-on ของระบบ, ให้ดำเนินการตัวต่อไปนี้:

- ตั้งนโยบายที่แสดงว่ารหัสผ่านไม่ใช่เรื่องเล็กน้อย และจะต้องไม่ใช้ร่วมกันกับผู้อื่น.
- ตั้งค่ากำหนดของระบบเพื่อช่วยคุณบังคับใช้กฎเกณฑ์. ตารางที่ 1แสดงค่าของระบบที่แนะนำให้ใช้.

การรวมกันของค่าใน ตารางที่ 1 จะทำให้มีความเข้มงวด มากขึ้น และมีวัตถุประสงค์เพื่อลดปัญหาของรหัสผ่านลงอย่างมาก. อย่างไรก็ตาม, ผู้ใช้อาจพบกับความยุ่งยากและความกังวลใจในการเลือกรหัสผ่าน เพื่อให้เข้ากับข้อจำกัดนั้น.

ควรพิจารณาให้ข้อมูลแก่ผู้ใช้ ดังรายการต่อไปนี้:

1. เกณฑ์ทั้งหมดของรหัสผ่าน.
2. ตัวอย่างของรหัสผ่านที่ใช้ได้และใช้ไม่ได้.
3. คำแนะนำสำหรับวิธีการตั้งรหัสผ่านที่ดี.

รันคำสั่ง Configure System Security (CFGSYSSEC) เพื่อตั้งค่าเหล่านี้. ใช้คำสั่ง Print System Security Attributes (PRTSYSSECA) เพื่อพิมพ์ ค่ากำหนดของระบบของคุณที่ใช้ในขณะนี้.

บทที่ 3 ของ *iSeries Security Reference* หนังสือ. หัวข้อ "ค่าที่เซ็ตโดยคำสั่ง Configure System Security" ในหน้า 40 จะให้ข้อมูลเพิ่มเติม เกี่ยวกับคำสั่ง CFGSYSSEC.

ตารางที่ 1. ค่ากำหนดของระบบสำหรับรหัสผ่าน

ชื่อของค่ากำหนดของระบบ	คำอธิบาย	ค่าที่แนะนำให้ใช้
QPWDEXPITV	ระยะเวลาที่ผู้ใช้ของระบบจะต้องเปลี่ยนแปลง รหัสผ่าน. คุณสามารถใช้ค่าที่แตกต่างกันสำหรับผู้ใช้แต่ละรายในโปรไฟล์ผู้ใช้.	60 (วัน)
QPWDLMTAJC	ระบบป้องกันไม่ให้ตัวอักษรที่ติดกันเป็นตัวเดียวกัน.	1 (ใช่)
QPWDLMTCHR	ตัวอักษรที่ไม่สามารถใช้ในรหัสผ่าน.[2]	AEIOU#$@
QPWDLMTREP	ระบบป้องกันไม่ให้มีตัวอักษรเดียวกันปรากฏมากกว่าหนึ่งครั้ง ในรหัสผ่าน.	2 (ไม่อนุญาตให้ต่อเนื่องกัน)
QPWDLVL	มีการจำกัดรหัสผ่านของโปรไฟล์ผู้ใช้ไว้ที่ 10 ตัวอักษร หรือมีค่าสูงสุดที่ 128 ตัวอักษร.	0[3]
QPWDMAXLEN	จำนวนอักขระสูงสุดในรหัสผ่าน.	8
QPWDMINLEN	จำนวนอักขระน้อยสุดในรหัสผ่าน.	6
QPWDPOSDIF	ตัวอักษรแต่ละตัวในรหัสผ่านจะต้องแตกต่างจากตัวอักษร ในตำแหน่งเดียวกันของรหัสผ่านก่อนหน้านั้น.	1 (ใช่)
QPWDRQDDGT	รหัสผ่านต้องมีอักขระแบบตัวเลขอย่างน้อยหนึ่งตัว.	1 (ใช่)

ตารางที่ 1. ค่ากำหนดของระบบสำหรับรหัสผ่าน (ต่อ)

ชื่อของค่ากำหนดของระบบ	คำอธิบาย	ค่าที่แนะนำให้ใช้
QPWDRQDDIF	ระยะเวลาที่ผู้ใช้จะต้องรอก่อนกลับมาใช้ รหัสผ่านเดิมอีกครั้ง.[2]	5 หรือน้อยกว่า (ช่วงเวลาหมดอายุ)[1]
QPWDVLDPGM	โปรแกรมทางออก (Exit Program) ที่จะเรียกใช้ใน การตรวจสอบรหัสผ่านที่ได้รับการกำหนดใหม่.	*NONE

หมายเหตุ:

1. ค่ากำหนดของระบบ QPWDEXPITV จะระบุระยะเวลาที่คุณต้องเปลี่ยนรหัสผ่านของคุณ, เช่น ทุกๆ 60 วัน. ซึ่งก็คือ **ช่วงเวลาหมดอายุ (expiration interval)**. ค่ากำหนดของระบบ QPWDRQDDIF ระบุถึงจำนวนของช่วงเวลาที่หมดอายุ ที่จะต้อง ผ่านไปก่อนที่คุณจะสามารถใช้รหัสผ่านเดิมได้อีกครั้ง. ในบทที่ 3 ของหนังสือ *iSeries Security Reference* จะให้ข้อมูลเพิ่มเติมเกี่ยวกับการทำงานร่วมกันของค่ากำหนดของระบบทั้งสองค่า.
2. QPWDLMTCHR ไม่มีการบังคับเมื่อระดับของรหัสผ่านอยู่ที่ 2 หรือ 3. ดูใน "ระดับต่างๆ ของรหัสผ่าน"สำหรับรายละเอียด.
3. ดูจาก "การวางแผนการเปลี่ยนแปลงระดับของรหัสผ่าน" ในหน้า 17 ในการพิจารณาระดับของรหัสผ่าน ที่ถูกต้องตามที่คุณต้องการ.

ระดับต่างๆ ของรหัสผ่าน

เริ่มต้นการใช้งานด้วย V5R1 ของระบบปฏิบัติการ, ค่ากำหนดของระบบที่เป็น QPWDLVL จะช่วยเพิ่มความปลอดภัยให้กับรหัสผ่านมากยิ่งขึ้น . ในรีลีสก่อนหน้านี้, ผู้ใช้ถูกจำกัดให้มีรหัสผ่านที่มีความยาวไม่เกิน 10 ตัวอักษร, จากขอบเขตของอักขระที่จำกัด. ปัจจุบัน, ผู้ใช้สามารถเลือกรหัสผ่าน (หรือประโยคผ่าน) ด้วยตัวอักษรมากถึง 128 ตัว, ขึ้นอยู่กับระดับของรหัสผ่านตามที่ระบบตั้งค่าเอาไว้. ระดับต่างๆ ของรหัสผ่านได้แก่:

- **ระดับ 0:** ระบบหลายๆ ระบบถูกส่งมาที่ระดับนี้. ที่ระดับ 0, รหัสผ่านมีความยาวไม่เกิน 10 ตัวอักษร, ประกอบด้วยอักขระ A–Z, 0–9, #, @, $, และ _ เท่านั้น. รหัสผ่านที่ระดับ 0 มีความปลอดภัยน้อยกว่ารหัสผ่านในระดับอื่นๆ ที่สูงกว่า.
- **ระดับ 1:**มีกฎทั่วๆ ไปเช่นเดียวกับระดับ 0, แต่รหัสผ่านสำหรับ iSeries ที่สนับสนุนสำหรับ Windows Network Neighborhood (หลังจากนี้จะถูกอ้างอิงถึงว่าเป็น iSeries NetServer) จะไม่ถูกบันทึกเอาไว้ .
- **ระดับ 2:** รหัสผ่านถือว่ามีความปลอดภัยมากในระดับนี้. ระดับนี้สามารถถูกนำไปใช้เพื่อจุดประสงค์ในการทดสอบต่างๆ . รหัสผ่านถูกบันทึกไว้สำหรับผู้ใช้ที่ระดับ 0 หรือ 1 ถ้ามีขนาด 10 ตัวอักขระ หรือน้อยกว่านั้น, และใช้ชุดอักขระสำหรับรหัสผ่านระดับ 0 หรือ 1. รหัสผ่าน (passwords หรือ passphrases) ที่ระดับนี้มีลักษณะดังต่อไปนี้:
  - มีความยาวได้ถึง 128 ตัวอักษร.
  - ประกอบด้วยอักขระของคีย์บอร์ดที่มีอยู่.
  - อาจไม่ประกอบด้วยช่องว่างทั้งหมด; ช่องว่างจะถูกลบออกจากส่วนท้ายของรหัสผ่าน.
  - คำนึงถึงตัวอักษรใหญ่เล็ก.
- **ระดับ 3:** รหัสผ่านที่ระดับนี้มีความปลอดภัยมากที่สุด, และมีการใช้ประโยชน์จาก algorithm การเข้ารหัสระดับที่สูงที่สุดที่มี. รหัสผ่านในระดับนี้มีลักษณะเหมือนกับในระดับ 2. ไม่มีการบันทึกรหัสผ่านสำหรับ iSeries NetServer ในระดับนี้.

คุณควรใช้เพียงรหัสผ่านระดับ 2 และ 3 เท่านั้น ถ้าทุกระบบในเครือข่ายมีคุณสมบัติตรงตามเกณฑ์ต่อไปนี้:

- มีระบบปฏิบัติการเป็น V5R1 หรือรุ่นเหลังจากนั้น
- ระดับของรหัสผ่านที่ตั้งค่าให้เป็น 2 หรือ 3

เช่นเดียวกัน, ผู้ใช้ทั้งหมดต้องล็อกอินโดยใช้ระดับของรหัสผ่านในระดับเดียวกัน. ระดับของรหัสผ่านเป็นแบบโกลบอล; ผู้ใช้ไม่สามารถเลือกใช้ระดับที่พวกเขาต้องการให้รหัสผ่านนั้นปลอดภัยได้.

การวางแผนการเปลี่ยนแปลงระดับของรหัสผ่าน

การเปลี่ยนระดับของรหัสผ่านต้องวางแผนอย่างระมัดระวัง. การทำงานกับระบบอื่นๆ อาจล้มเหลวหรือผู้ใช้อาจไม่สามารถ sign on ไปยังระบบได้ ถ้าคุณไม่ได้วางแผนในการเปลี่ยนระดับของรหัสผ่านอย่างเพียงพอ. ก่อนที่จะเปลี่ยนค่ากำหนดของระบบ QPWDLVL, ต้องแน่ใจว่าคุณได้บันทึกข้อมูลความปลอดภัยโดยใช้คำสั่ง SAVSECDTA หรือ SAVSYS ไว้แล้ว. ถ้าคุณมีข้อมูลปัจจุบันสำรองไว้, คุณจะสามารถตั้งรหัสผ่านใหม่ให้กับโปรไฟล์ผู้ใช้ทุกโปรไฟล์ หากคุณต้องการที่จะกลับไปยังระดับของรหัสผ่านที่ต่ำกว่า.

ผลิตภัณฑ์ที่คุณใช้บนระบบของคุณ, และบนไคลเอ็นต์ที่ระบบติดต่ออยู่, อาจมีปัญหาเกิดขึ้นเมื่อระดับของรหัสผ่านของค่ากำหนดของระบบที่เป็น (QPWDLVL) ถูกตั้งค่าให้เป็น 2 หรือ 3. ผลิตภัณฑ์ใดๆ หรือไคลเอ็นต์ที่ทำการส่งรหัสผ่านให้กับระบบในรูปแบบที่ถูกเข้ารหัสไว้, แทนที่จะเป็นแบบข้อความที่ชัดเจนตามที่ผู้ใช้ได้ใส่ลงบนจอภาพ sign-on, จะต้องถูกอัพเกรดให้ทำงานกับกฎของการเข้ารหัสให้กับรหัสผ่านใหม่ๆ สำหรับ QPWDLVL 2 หรือ 3 ได้. การส่งผ่านรหัสผ่านที่ได้รับการเข้ารหัสแล้วนั้นจะรู้จักกันว่าเป็น **การแทนค่ารหัสผ่าน**.

การแทนค่ารหัสผ่านถูกใช้เพื่อป้องกันรหัสผ่านไม่ให้ถูกดักจับในระหว่างการส่งข้อมูลภายในเครือข่าย. ค่าแทนของรหัสผ่านถูกสร้างขึ้นโดยไคลเอ็นต์ที่เก่ากว่าที่ไม่สนับสนุน algorithm ใหม่สำหรับ QPWDLVL 2 หรือ 3, ถึงแม้ว่าอักขระที่ระบุไว้จะถูกต้อง, แต่ก็จะไม่ถูกยอมรับโดยไคลเอ็นต์นั้นๆ . วิธีการนี้ยังใช้ได้กับการเข้าถึงในระดับเสมอกันแบบ iSeries ไป iSeries ที่ใช้ประโยชน์ของค่าที่ทำการเข้ารหัสแล้วมาแสดงตนจากระบบหนึ่งไปยังอีกระบบหนึ่ง.

ปัญหานี้จะประกอบไปด้วยความจริงที่ว่าผลิตภัณฑ์ที่ได้รับผลกระทบบางตัว (อาทิเช่น Java Toolbox) ถูกจัดทำมาในรูปของ middleware. ผลิตภัณฑ์ที่เป็น third party ที่ทำงานร่วมกันกับผลิตภัณฑ์เหล่านี้ในเวอร์ชันก่อน จะทำงานได้ไม่ถูกต้องจนกว่าจะมีการสร้างขึ้นใหม่โดยใช้ middleware ในเวอร์ชันที่อัพเดตแล้ว.

จากสถานการณ์ที่กล่าวมา และสถานการณ์อื่นๆ , เป็นการง่ายที่จะเห็นว่าทำไมการวางแผนอย่างระมัดระวัง จึงมีความจำเป็นก่อนที่จะเปลี่ยนค่ากำหนดของระบบ QPWDLVL.

ข้อควรพิจารณาในการเปลี่ยนค่า QPWDLVL จาก 0 เป็น 1

รหัสผ่านระดับที่ 1 อนุญาตให้ระบบ, ที่ไม่จำเป็นต้องติดต่อสื่อสารกับผลิตภัณฑ์ที่เป็น Windows 95/98/ME AS/400® ไคลเอนต์สนับสนุนสำหรับ Windows Network Neighborhood (iSeries NetServer), เพื่อให้รหัสผ่านของ iSeries NetServer ถูกกำจัดไปจากระบบ. การกำจัดรหัสผ่านที่เข้ารหัสที่ไม่จำเป็นจากระบบ จะช่วยเพิ่มความปลอดภัยโดยรวมของระบบ.

ที่ QPWDLVL 1, กลไกของการแทนค่ารหัสผ่านของรุ่น pre-V5R1 และการพิสูจน์รหัสผ่าน, ที่มีอยู่ในปัจจุบัน, ยังคงทำงานต่อไป. มีค่าความเสียหายที่เป็นไปได้น้อยมากยกเว้นสำหรับฟังก์ชันและเซอร์วิสที่ต้องใช้รหัสผ่านของ iSeries NetServer.

ข้อควรพิจารณาในการเปลี่ยนค่า QPWDLVL จาก 0 หรือ 1 เป็น 2

ระดับของรหัสผ่าน 2 มีการใช้รหัสผ่านที่คำนึงถึงตัวอักษรใหญ่เล็ก ที่มีความยาวได้ถึง 128 ตัวอักษร (และอาจเรียกว่า passphrase) และให้ความสามารถสูงสุดในการกลับค่า QPWDLVL ไปเป็น 0 หรือ 1.

โดยไม่คำนึงถึงระดับของรหัสผ่านของระบบ, รหัสผ่านที่ระดับ 2 และ 3 ถูกสร้างขึ้นเมื่อมีการเปลี่ยนรหัสผ่านหรือเมื่อผู้ใช้ sign on ไปยังระบบ. การมีรหัสผ่านที่ระดับ 2 และ 3 ที่สร้างขึ้นในขณะที่ระบบยังคงอยู่ที่ระดับของรหัสผ่าน 0 หรือ 1 ช่วยให้เตรียมพร้อมสำหรับการเปลี่ยนไปยังระดับของรหัสผ่าน 2 หรือ 3.

ก่อนที่จะทำการเปลี่ยนค่าของ QPWDLVL ให้เป็น 2, คุณควรที่จะใช้คำสั่ง DSPAUTUSR หรือ PRTUSRPRF TYPE(*PWDINFO) ในการระบุตำแหน่งของโปรไฟล์ผู้ใช้ที่ไม่มีรหัสผ่านที่ใช้ได้กับที่รหัสผ่านระดับ 2. ขึ้นอยู่กับว่าโปรไฟล์ใดที่คำสั่งเหล่านี้ระบุตำแหน่งไว้ให้, คุณอาจต้องการที่จะใช้วิธีใดวิธีหนึ่งจากกลวิธีต่อไปนี้ในการที่จะทำให้รหัสผ่านระดับ 2 และ 3 ถูกเพิ่มเข้าไปในโปรไฟล์ .

- เปลี่ยนรหัสผ่านของโปรไฟล์ผู้ใช้โดยใช้คำสั่ง CHGUSRPRF หรือ คำสั่ง CL CHGPWD หรือ API QSYCHGPW. ซึ่งจะทำให้ระบบเปลี่ยนรหัสผ่านที่ใช้ได้กับระดับ 0 และ 1; และระบบยังสร้างรหัสผ่านที่คำนึงถึงตัวอักษรใหญ่เล็ก ที่ เทียบเท่ากันสองแบบ ซึ่งใช้ได้กับระดับ 2 และ 3. รหัสผ่านที่เป็นตัวอักษรพิมพ์ใหญ่ทั้งหมดและที่เป็นตัวพิมพ์เล็กทั้งหมดถูกสร้างขึ้นเพื่อใช้กับระดับของรหัสผ่าน 2 หรือ 3.

  ตัวอย่างเช่น, การเปลี่ยนรหัสผ่านเป็น C4D2RB4Y เป็นผลให้ระบบสร้างรหัสผ่าน C4D2RB4Y และ c4d2rb4y ที่อยู่ในระดับ 2.
- การ sign on ไปยังระบบผ่านกลไกที่แสดงรหัสผ่านโดยไม่มีการปิดบัง (ไม่ใช้ password substitution). ถ้ารหัสผ่านถูกต้องและโปรไฟล์ผู้ใช้ไม่มีรหัสผ่านที่ใช้ได้กับระดับ 2 และ 3, ระบบจะสร้างรหัสผ่านที่คำนึงถึงตัวอักษรใหญ่เล็ก และ equivalent กันสองแบบที่ใช้ได้กับระดับ 2 และ 3. รหัสผ่านที่เป็นตัวอักษรพิมพ์ใหญ่ทั้งหมดและที่เป็นตัวพิมพ์เล็กทั้งหมด ถูกสร้างขึ้นเพื่อใช้กับระดับของรหัสผ่าน 2 หรือ 3.

การหายไปของรหัสผ่านที่ใช้ได้กับระดับ 2 หรือ 3 อาจเป็นปัญหาได้ เมื่อโปรไฟล์ผู้ใช้ไม่มีรหัสผ่านที่สามารถใช้ได้ในระดับ 0 และ 1 เช่นกัน หรือเมื่อผู้ใช้พยายามที่จะ sign on ผ่านผลิตภัณฑ์ที่ใช้ password substitution. ในกรณีเช่นนี้, ผู้ใช้จะไม่สามารถ sign on ได้เมื่อระดับของรหัสผ่านถูกเปลี่ยนเป็น 2.

ถ้าโปรไฟล์ผู้ใช้ไม่มีรหัสผ่านที่ใช้ได้ในระดับ 2 และ 3, โปรไฟล์ผู้ใช้ไม่มีรหัสผ่านที่ใช้ได้ในระดับ 0 และ 1, และผู้ใช้ sign on ผ่านผลิตภัณฑ์ที่ส่งรหัสผ่านโดยไม่ปิดบัง, จากนั้นระบบจะตรวจสอบผู้ใช้ด้วยรหัสผ่านระดับ 0 และสร้างรหัสผ่านในระดับ 2 ขึ้นมาสองค่า (ดังคำอธิบายข้างต้น) ให้กับโปรไฟล์ผู้ใช้. การ sign on ครั้งต่อไปจะถูกตรวจสอบด้วยรหัสผ่านที่ระดับ 2.

ไคลเอ็นต์/เซอร์วิสใดๆ ที่ใช้ password substitution จะทำงานได้ไม่ถูกต้องที่ QPWDLVL 2 ถ้าไม่มีการอัพเดตไคลเอ็นต์/เซอร์วิสให้ใช้โครงร่างของ password (passphrase) substitution ใหม่. ผู้บริหารระบบควรตรวจสอบว่า จำเป็นจะต้องมีการอัพเดตไคลเอ็นต์/เซอร์วิส ให้โครงร่างของ password substitution ใหม่หรือไม่.

ไคลเอ็นต์/เซอร์วิส ที่ใช้ password substitution ประกอบด้วย:

- TELNET
- iSeries Access
- iSeries Host Servers
- QFileSrv.400
- การสนับสนุนการพิมพ์ของ iSeries NetServer
- DDM
- DRDA®
- SNA LU6.2

เป็นเรื่องสมควรอย่างยิ่งที่จะมีการบันทึกข้อมูลความปลอดภัยไว้ก่อนที่จะมีการเปลี่ยน ค่า QPWDLVL เป็น 2. วิธีนี้จะช่วยให้การเปลี่ยนกลับไปยังระดับ QPWDLVL 0 หรือ 1 ทำได้ง่ายขึ้น หากจำเป็นต้องมีการทำเช่นนั้น.

และขอแนะนำว่า ค่ากำหนดของระบบของรหัสผ่านค่าอื่นๆ , เช่น QPWDMINLEN และ QPWDMAXLEN ควรไม่มีการเปลี่ยนแปลงจนกว่าจะมีการทดสอบที่ระดับ QPWDLVL 2 บางส่วนแล้ว. วิธีนี้จะทำให้การเปลี่ยนกลับไปยังระดับ QPWDLVL 1 หรือ 0 ทำได้ง่ายขึ้น หากจำเป็น. อย่างไรก็ตาม, ค่ากำหนดของระบบ QPWDVLDPGM ต้องระบุเป็น *REGFAC หรือ *NONE ก่อนที่ระบบจะอนุญาตให้ค่า QPWDLVL เปลี่ยนเป็น 2. ดังนั้น, ถ้าคุณใช้โปรแกรมตรวจสอบความถูกต้อง, คุณอาจเขียนโปรแกรมขึ้นใหม่ โดยให้โปรแกรมนั้นสามารถที่จะเรจิสเตอร์ QIBM_QSY_VLD_PASSWRD exit point โดยใช้คำสั่ง ADDEXITPGM.

รหัสผ่าน iSeries NetServer จะยังคงใช้ได้ที่ QPWDLVL 2, ดังนั้นฟังก์ชัน/เซอร์วิสใดๆ ที่จำเป็นต้องใช้รหัสผ่านของ iSeries NetServer ควรที่จะทำงานได้อย่างถูกต้อง.

เมื่อผู้บริหารระบบสะดวกที่จะให้ระบบทำงานที่ระดับ QPWDLVL 2, พวกเขาสามารถเริ่มที่จะเปลี่ยนค่ากำหนดของระบบของรหัสผ่านให้สามารถมีรหัสผ่านที่ยาวขึ้น. อย่างไรก็ตาม, ผู้บริหารระบบจำเป็นต้องทราบว่า รหัสผ่านที่ยาวขึ้นจะส่งผลกระทบดังต่อไปนี้:

- ถ้ามีการระบุรหัสผ่านยาวกว่า 10 ตัวอักษร, รหัสผ่านที่ระดับ 0 และ 1 จะถูกลบออก. โปรไฟล์ผู้ใช้นี้จะไม่สามารถ sign on ได้ หากระบบกลับไปสู่ระดับของรหัสผ่าน 0 หรือ 1.
- ถ้ารหัสผ่านมีอักขระพิเศษหรือไม่เป็นไปตามกฎของการสร้างชื่ออ็อบเจ็กต์ธรรมดา (ยกเว้นการคำนึงถึงตัวอักษรขนาดใหญ่-เล็ก), รหัสผ่านที่ระดับ 0 และ 1 จะถูกลบออก.
- ถ้ารหัสผ่านที่มีขนาดมากกว่า 14 อักขระถูกระบุไว้, รหัสผ่านของ iSeries NetServer สำหรับโปรไฟล์ผู้ใช้จะถูกลบทิ้งไป.

- ค่ากำหนดของระบบจะสามารถใช้ได้กับค่ารหัสผ่านระดับ 2 และไม่สามารถใช้ได้กับรหัสผ่านระดับ 0 และ 1 ที่ถูกกำหนดขึ้นโดยระบบ หรือค่าของรหัสผ่านของ iSeries NetServer (ถ้าได้กำหนดไว้).

ข้อควรพิจารณาในการเปลี่ยนค่า QPWDLVL จาก 2 เป็น 3

หลังจากการทำงานของระบบที่ระดับ QPWDLVL 2 ได้ระยะหนึ่ง, ผู้บริหารระบบสามารถพิจารณาที่จะย้ายไปยัง QPWDLVL ระดับ 3 เพื่อป้องกันความปลอดภัยของรหัสผ่านให้มากที่สุด.

ที่ระดับ QPWDLVL 3, รหัสผ่านทั้งหมดของ iSeries NetServer จะถูกลบทิ้ง ดังนั้นระบบสมควรที่จะไม่ถูกเลื่อนไปเป็น QPWDLVL 3 จนกระทั่งไม่มีความจำเป็นที่จะใช้รหัสผ่านของ iSeries NetServer.

ที่ QPWDLVL 3, รหัสผ่านที่ระดับ 0 และ 1 ถูกลบออก. ผู้บริหารระบบสามารถใช้คำสั่ง DSPAUTUSR หรือ PRTUSRPRF เพื่อหาตำแหน่งของโปรไฟล์ผู้ใช้ ที่ไม่มีรหัสผ่านที่สัมพันธ์กับโปรไฟล์เหล่านี้นในระดับ 2 หรือ 3.

การเปลี่ยนแปลงระดับของรหัสผ่านไปยังระดับที่ต่ำกว่า

การกลับไปยังค่า QPWDLVL ที่ต่ำกว่า, ในขณะที่เป็นไปได้, เป็นสิ่งไม่ได้คาดหวังว่าจะเป็นการดำเนินการที่ไม่มีความเสียหายใดๆ เลย. โดยทั่วไป, มีความตั้งใจที่จะเปลี่ยนค่า QPWDLVL จากระดับน้อยกว่าไปสู่ระดับสูงกว่าเท่านั้น. อย่างไรก็ตาม, อาจมีกรณีที่ต้องมีการใช้ค่า QPWDLVL ที่ต่ำกว่าอีกครั้ง.

ส่วนต่อไปนี้จะกล่าวถึงงานที่จำเป็นต้องกลับไปยังระดับของรหัสผ่านที่ต่ำกว่า.

ข้อควรพิจารณาในการเปลี่ยนค่า QPWDLVL จาก 2 เป็น 3: การเปลี่ยนแปลงนี้ค่อนข้างง่าย. เมื่อ QPWDLVL ถูกตั้งค่าให้เป็น 2, administrator จำเป็นที่จะต้องตรวจดูว่ามีโปรไฟล์ผู้ใช้ใดบ้างที่จำเป็นจะต้องมีรหัสผ่านของ iSeries NetServer หรือรหัสผ่านระดับ 0 หรือ 1 และ, ถ้าเป็นเช่นนั้น, ให้เปลี่ยนรหัสผ่านของโปรไฟล์ผู้ใช้ให้เป็นค่าที่อนุญาตให้ใช้ได้.

นอกจากนี้, ค่ากำหนดของระบบที่เป็นรหัสผ่านอาจจะต้องถูกเปลี่ยนกลับไปเป็นค่าที่ใช้ร่วมกันได้กับiSeries NetServer และรหัสผ่าน ระดับ 0 หรือ 1, ถ้ารหัสผ่านเหล่านั้นเป็นสิ่งที่จำเป็น.

ข้อควรพิจารณาในการเปลี่ยนค่า QPWDLVL จาก 3 เป็น 1 หรือ 0: เนื่องจากมีโอกาสอย่างมากที่จะเกิดปัญหากับระบบ (เช่น ไม่มีผู้ใดสามารถ sign on ได้ เนื่องจากรหัสผ่านที่ระดับ 0 และ 1 ทั้งหมดถูกลบออก), จึงไม่มีการสนับสนุนการเปลี่ยนค่านี้โดยตรง. เพื่อที่จะเปลี่ยนค่าจาก QPWDLVL 3 ไปเป็น QPWDLVL 1 หรือ 0, ระบบจะต้องเปลี่ยนค่าเป็น QPWDLVL 2 เสียก่อน.

ข้อควรพิจารณาในการเปลี่ยนค่า QPWDLVL จาก 2 เป็น 1: ก่อนหน้าที่จะเปลี่ยนค่า QPWDLVL เป็น 1, ผู้บริหารระบบควรใช้คำสั่ง DSPAUTUSR หรือ PRTUSRPRF TYPE (*PWDINFO) เพื่อหาตำแหน่งของโปรไฟล์ผู้ใช้ใดๆ ที่ไม่มีรหัสผ่านในระดับ 0 หรือ 1. ถ้าโปรไฟล์ผู้ใช้ต้องการรหัสผ่านหลังจากมีการเปลี่ยนค่า QPWDLVL, ผู้บริหารระบบต้องแน่ใจว่า รหัสผ่านในระดับ 0 และ 1 ถูกสร้างให้กับโปรไฟล์โดยใช้กลไกอย่างใดอย่างหนึ่งต่อไปนี้:

- เปลี่ยนรหัสผ่านของโปรไฟล์ผู้ใช้โดยใช้คำสั่ง CHGUSRPRF หรือ คำสั่ง CL CHGPWD หรือ API QSYCHGPW. ซึ่งจะทำให้ระบบเปลี่ยนรหัสผ่านที่ใช้ได้กับระดับ 2 และ 3; และระบบยัง

สร้างรหัสผ่านเป็นตัวอักษรพิมพ์ใหญ่ทั้งหมดที่ equivalent กัน ซึ่งใช้ได้กับระดับ 0 และ 1. ระบบจะสามารถสร้างรหัสผ่านในระดับ 0 และ 1 ได้ หากเป็นไปตามเงื่อนไข ดังนี้:

- รหัสผ่านมีความยาวเท่ากับ 10 ตัวอักษรหรือน้อยกว่า.
- รหัสผ่านสามารถถูกแปลงเป็นตัวอักษรพิมพ์ใหญ่ EBCDIC (A-Z), 0-9, @, #, $, และเครื่องหมายเส้นใต้ (_).
- รหัสผ่านไม่สามารถขึ้นต้นด้วยตัวเลขหรือเครื่องหมายเส้นใต้.

ตัวอย่างเช่น, การเปลี่ยนรหัสผ่านเป็น RainyDay เป็นผลให้ระบบสร้างรหัสผ่านในระดับ 0 และ 1 เป็น RAINYDAY. แต่การเปลี่ยนรหัสผ่านเป็น Rainy Days In April จะทำให้ระบบไม่มีรหัสผ่านในระดับ 0 และ 1 (เนื่องจากรหัสผ่านมีความยาวมากเกินไป และมีช่องว่างในรหัสผ่านนั้น).

ไม่มีการแสดงข้อความหรือสิ่งชี้บอกใดๆ ถ้าไม่มีการสร้างรหัสผ่านที่ระดับ 0 หรือ 1.

- การ sign on ไปยังระบบผ่านกลไกที่แสดงรหัสผ่านโดยไม่มีการปิดบัง (ไม่ใช้ password substitution). ถ้ารหัสผ่านถูกต้องและโปรไฟล์ผู้ใช้ไม่มีรหัสผ่านที่ใช้ได้กับระดับ 0 และ 1, ระบบจะสร้างรหัสผ่านที่เป็นตัวอักษรพิมพ์ใหญ่ทั้งหมดที่ equivalent กัน ซึ่งใช้ได้กับระดับ 0 และ 1. ระบบจะสามารถสร้างรหัสผ่านในระดับ 0 และ 1 ได้ หากเป็นไปตามเงื่อนไขที่แสดงไว้ข้างต้น.

ผู้บริหารระบบสามารถเปลี่ยน QPWDLVL ไป 1. ทุก iSeries รหัสผ่าน NetServer และลบทิ้งเมื่อการเปลี่ยน QPWDLVL 1 เกิดผล (ต่อจาก IPL).

ข้อควรพิจารณาในการเปลี่ยนค่า QPWDLVL จาก 2 เป็น 0: ข้อควรพิจารณาจะเป็นอันเดียวกันกับการเปลี่ยนจาก QPWDLVL 2 ไปเป็น 1 ยกเว้นว่ารหัสผ่านทั้งหมดของiSeries NetServer จะยังคงไว้เมื่อการเปลี่ยนแปลงนั้นบังเกิดผล.

ข้อควรพิจารณาในการเปลี่ยนค่า QPWDLVL จาก 1 เป็น 0: หลังการเปลี่ยนแปลง QPWDLVL ให้เป็น 0, administrator สมควรที่จะใช้คำสั่ง DSPAUTUSR หรือ PRTUSRPRF ในการระบุตำแหน่งของโปรไฟล์ผู้ใช้ใดๆ ที่ไม่มีรหัสผ่านของ iSeries NetServer . ถ้าโปรไฟล์ผู้ใช้นั้นจำเป็นต้องใช้รหัสผ่านของ iSeries NetServer, มันสามารถถูกสร้างขึ้นโดยการเปลี่ยนแปลงรหัสผ่านของผู้ใช้หรือการ sign - on ผ่านกลวิธีที่จะแสดงรหัสผ่านในรูปของข้อความที่ชัดเจน.

จากนั้น ผู้บริหารระบบสามารถเปลี่ยน QPWDLVL ไปเป็น 0.

การเปลี่ยนแปลงรหัสผ่านที่รู้จักแล้ว

ดำเนินการดังต่อไปนี้เพื่อทำการปิดทางเข้าเซิร์ฟเวอร์ iSeries ที่รู้จักดี ที่อาจมีปรากฏอยู่บนระบบของคุณ.

__ ขั้นตอนที่ 1. เพื่อให้มั่นใจว่าไม่มีโปรไฟล์ผู้ใช้ใดใช้รหัสผ่านดีฟอลต์ (ซึ่งมีค่าเท่ากับ ชื่อของโปรไฟล์ผู้ใช้). คุณสามารถใช้คำสั่ง Analyze Default Passwords (ANZDFTPWD). (ดูใน “หลีกเลี่ยงการใช้รหัสผ่านดีฟอลต์” ในหน้า 27.)

__ ขั้นตอนที่ 2. พยายามเข้าสู่ระบบของคุณ โดยใช้โปรไฟล์ผู้ใช้ร่วมกับรหัสผ่านที่แสดงในตารางที่ 2 ในหน้า 22. จะมีการ พับลิชรหัสผ่าน, ที่อาจเป็นทางเลือกและของบุคคลที่

พยายามเข้าสู่ระบบ ของคุณ. หากคุณสามารถ sign on ได้, ให้ใช้คำสั่ง Change User Profile (CHGUSRPRF) เพื่อเปลี่ยนรหัสผ่านไปเป็นค่าที่แนะนำ.

__ ขั้นตอนที่ 3. Start the Dedicated Service Tools (DST) และพยายามที่จะ sign on ด้วยรหัสผ่านที่แสดงอยู่ใน ตารางที่ 2. อ้างอิงถึง iSeries Information Center—>Security—>Service Tools. โปรดดูที่ "สิ่งที่ต้องรู้ก่อนและข้อมูลที่เกี่ยวข้อง" ในหน้า xiii สำหรับข้อมูลในการเข้าไปใช้งาน iSeries Information Center.

__ ขั้นตอนที่ 4. ถ้าคุณสามารถ sign on เข้าไปยัง DST ด้วยรหัสผ่านใดๆ เหล่านี้, คุณสมควรที่จะเปลี่ยนรหัสผ่านเสียด้วย. iSeries Information Center—>Security—>Service Tools มีวิธีการโดยละเอียดในการเปลี่ยนแปลง ID ของผู้ใช้ and passwords. โปรดดูที่ "สิ่งที่ต้องรู้ก่อนและข้อมูลที่เกี่ยวข้อง" ในหน้า xiii สำหรับข้อมูลเกี่ยวกับการเข้าถึง iSeries Information Center.

__ ขั้นตอนที่ 5. ท้ายที่สุด, ตรวจสอบให้แน่ใจว่าคุณไม่สามารถ sign on ได้โดยการกดปุ่ม Enter ที่หน้าจอ Sign On เพียงอย่างเดียว ยังต้องใส่ ID ของผู้ใช้และรหัสผ่านเข้าไปด้วย. ให้ลองกับหน้าจอต่างๆ กัน. หากคุณสามารถ sign on โดยไม่ต้องข้อมูลใดบนหน้าจอ Sign On, ให้ทำตามข้อใดข้อหนึ่งต่อไปนี้:

- เปลี่ยนระดับความปลอดภัยเป็น 40 หรือ 50 (ค่ากำหนดของระบบ QSECURITY).

  หมายเหตุ: แอ็พพลิเคชันของคุณอาจรันแตกต่างกันออกไปเมื่อคุณได้เพิ่มค่าของระดับการรักษาความปลอดภัยขึ้นเป็น 40 หรือ 50.
- เปลี่ยนจากทางเข้าของเวิร์กสเตชันทั้งหมด จากระบบย่อยแบบโต้ตอบเป็นการชี้ไปยัง job description ที่มีการระบุค่า USER(*RDQ).

ตารางที่ 2. Passwords for IBM-supplied profiles

User ID	รหัสผ่าน	ค่าที่แนะนำให้ใช้
QSECOFR	QSECOFR[1]	ค่าสำคัญที่รู้จักกันในเฉพาะหมู่นักบริหาร ความปลอดภัย. **บันทึกรหัสผ่านที่คุณเลือก และเก็บไว้ในที่ที่ปลอดภัย.**
QSYSOPR	QSYSOPR	*NONE[2]
QPGMR	QPGMR	*NONE[2]
QUSER	QUSER	*NONE[2, 3]
QSRV	QSRV	*NONE[2]
QSRVBAS	QSRVBAS	*NONE[2]

หมายเหตุ:

1. ระบบจะมาพร้อมกับค่า *Set password to expired*สำหรับ QSECOFR ตั้งค่าให้เป็น *YES. ครั้งแรก ที่คุณทำการ sign on เข้าสู่ระบบใหม่, คุณต้องเปลี่ยนรหัสผ่านของ QSECOFR.
2. ระบบต้องการโปรไฟล์ผู้ใช้เหล่านี้ในฟังก์ชันระบบ, แต่คุณไม่ควรให้ผู้ใช้ สามารถ sign on โดยใช้ค่าโปรไฟล์เหล่านี้. สำหรับระบบใหม่ที่ติดตั้ง V3R1 หรือรีลีสที่สูงกว่า, รหัสผ่านที่มาพร้อมเครื่องจะเป็น *NONE.

   เมื่อคุณ รันคำสั่ง CFGSYSSEC, ระบบจะตั้งรหัสผ่านเหล่านี้เป็น *NONE.
3. การรัน iSeries Access for Windows โดยใช้ TCP/IP, ต้องมีการทำให้ค่าของโปรไฟล์ผู้ใช้ QUSER สามารถใช้งานได้เสียก่อน.

ตารางที่ 3. รหัสผ่านสำหรับ Dedicated Service Tools

ระดับ DST	User ID[1]	รหัสผ่าน	ค่าที่แนะนำให้ใช้
ความสามารถพื้นฐาน	11111111	11111111	ค่าสำคัญที่รู้จักกันในเฉพาะหมู่นักบริหารความปลอดภัย.[2]
ความสามารถเต็ม	22222222	22222222[3]	ค่าสำคัญที่รู้จักกันในเฉพาะหมู่นักบริหารความปลอดภัย.[2]
ความสามารถด้านความปลอดภัย	QSECOFR	QSECOFR[3]	ค่าสำคัญที่รู้จักกันในเฉพาะหมู่นักบริหารความปลอดภัย.[2]
ความสามารถด้านบริการ	QSRV	QSRV[3]	ค่าสำคัญที่รู้จักกันในเฉพาะหมู่นักบริหารความปลอดภัย.[2]

หมายเหตุ:

1. ID ของผู้ใช้จะจำเป็นสำหรับรีลีสของระบบปฏิบัติการที่เป็น PowerPC® AS (RISC) เท่านั้น .
2. ถ้าผู้ให้บริการฮาร์ดแวร์ต้องการ sign on โดยใช้ user ID และรหัสผ่านเหล่านี้, ให้เปลี่ยนรหัสผ่านเป็นค่าใหม่ หลังจากที่ผู้ให้บริการฮาร์ดแวร์จากไป.
3. โปรไฟล์ผู้ใช้ของเครื่องมือบริการจะหมดอายุลง หลังการใช้งานในครั้งแรก.

หมายเหตุ: รหัสผ่าน DST จะสามารถเปลี่ยนได้โดย authenticated device เท่านั้น. ซึ่งจะเป็นเช่นนี้กับทุกรหัสผ่านและ user ID ที่สัมพันธ์กัน. สำหรับข้อมูลเพิ่มเติมเกี่ยวกับอุปกรณ์ที่ใช้ในการแสดงตนของผู้ใช้, โปรดดูที่ข้อมูลเกี่ยวกับการติดตั้ง Operations Console ใน iSeries Information Center.

การตั้งค่า sign-on

ตารางที่ 4แสดงค่าหลายๆ ค่าที่คุณสามารถกำหนดเพื่อทำให้ผู้บุกรุก เข้ามายังระบบของคุณได้ยากขึ้น. หากคุณรัน CFGSYSSEC command, จะมีการเปลี่ยนแปลงค่ากำหนดของระบบ ไปเป็นค่าที่แนะนำ. คุณสามารถอ่านเพิ่มเติมเกี่ยวกับค่าของระบบได้ ในบทที่ 3 ของหนังสือ *iSeries Security Reference* .

ตารางที่ 4. Sign-on system values

ชื่อของค่ากำหนดของระบบ	คำอธิบาย	ค่าติดตั้งที่แนะนำให้ใช้
QAUTOCFG	ระบบทำตามติดตั้งค่าให้กับอุปกรณ์ใหม่โดยอัตโนมัติ.	0 (ไม่)
QAUTOVRT	จำนวนของคำอธิบายอุปกรณ์เสมือนที่ระบบทำการสร้างให้โดยอัตโนมัติ เมื่อไม่มีอุปกรณ์เหลือไว้ให้ใช้งาน.	0
QDEVRCYACN	สิ่งที่ระบบกระทำเมื่ออุปกรณ์ติดต่ออีกครั้ง (reconnect) หลังจากเกิดข้อผิดพลาด.[1]	*DSCMSG
QDSCJOBITV	ระยะเวลาที่ระบบรอก่อนที่จะจบงานที่ขาดการติดต่อแล้ว (disconnected job).	120
QDSPSGNINF	ระบบแสดงข้อมูลเกี่ยวกับการ sign-on ครั้งก่อน เมื่อผู้ใช้ sign on เข้ามา.	1 (ใช่)
QINACTITV	ระยะเวลาที่ระบบรอก่อนที่จะจัดการ เมื่องานงานโต้ตอบไม่ทำงาน.	60

ตารางที่ 4. Sign-on system values (ต่อ)

ชื่อของค่ากำหนดของระบบ	คำอธิบาย	ค่าติดตั้งที่แนะนำให้ใช้
QINACTMSGQ	สิ่งที่ระบบทำเมื่อระยะเวลา QINACTITV ครบกำหนด.	*ENDJOB
QLMTDEVSSN	ระบบป้องกันผู้ใช้จากการ sign on มากกว่า หนึ่งเวิร์กสเตชันในเวลาเดียวกัน.	1 (ใช่)
QLMTSECOFR	ผู้ใช้ที่มีสิทธิพิเศษ *ALLOBJ หรือ *SERVICE จะสามารถ Sign-On เฉพาะเวิร์กสเตชันที่กำหนดไว้เท่านั้น.	1 (ใช่)[2]
QMAXSIGN	จำนวนครั้งสูงสุดของการ sign on ที่ผิดพลาดต่อเนื่องกัน (โปรไฟล์ผู้ใช้หรือรหัสผ่านไม่ถูกต้อง).	3
QMAXSGNACN	สิ่งที่ระบบทำเมื่อจำนวนครั้ง QMAXSIGN ครบจำนวน.	3 (ให้ทั้งโปรไฟล์ผู้ใช้และอุปกรณ์ทำงานไม่ได้)

หมายเหตุ:

1. ระบบสามารถตัดการเชื่อมต่อและทำการเชื่อมต่อใหม่เซสชัน TELNET อีกครั้งเมื่อdevice description สำหรับเซสชันนั้นถูกกำหนดค่าไว้อย่างชัดเจน.
2. หากคุณตั้งค่ากำหนดของระบบเป็น 1 (ใช่), คุณต้องให้สิทธิอย่างชัดแจ้งแก่ผู้ใช้ในอุปกรณ์ ด้วยสิทธิพิเศษ *ALLOBJ หรือ *SERVICE. วิธีที่ง่ายที่สุด คือ การให้สิทธิ *CHANGE แก่โปรไฟล์ผู้ใช้ QSECOFR ในอุปกรณ์ที่กำหนด.

การเปลี่ยนข้อความแสดงความผิดพลาดในการ sign-on

นักเจาะระบบต้องการทราบเมื่อเขากำลังเจาะเข้าสู่ระบบว่ามีความผิดพลาดใดเกิดขึ้น. เมื่อข้อความแสดงความผิดพลาดบนหน้าจอ Sign On แสดงข้อความ `Password not correct`, นักเจาะระบบจะสามารถคาดเดาได้ว่า user ID นั้น ถูกต้อง แล้ว. คุณสามารถทำความสับสนให้แก่นักเจาะระบบโดยการใช้คำสั่ง Change Message Description (CHGMSGD) เพื่อเปลี่ยนแปลงข้อความแสดงข้อผิดพลาด สำหรับการ sign-on สองข้อความ. ตารางที่ 5แสดงถึงข้อความที่ควรใช้.

ตารางที่ 5. Sign-on error messages

Message ID	ข้อความที่ถูกส่งมาด้วย	ข้อความที่แนะนำให้ใช้
CPF1107	CPF1107 – Password not correct for user profile.	Sign-on information is not correct **หมายเหตุ:** ไม่ต้องมี message ID อยู่ในข้อความแสดงความผิดพลาด.
CPF1120	CPF1120 – User `XXXXX` does not exist.	Sign-on information is not correct. **หมายเหตุ:** ไม่ต้องมี message ID อยู่ในข้อความแสดงความผิดพลาด.

ตารางการใช้งานของโปรไฟล์ผู้ใช้

คุณอาจต้องการให้บางโปรไฟล์ผู้ใช้สามารถ sign-on ได้เฉพาะในบางเวลาของวัน หรือในบางวันของสัปดาห์. ตัวอย่างเช่น, ถ้าคนมีโปรไฟล์ที่ทำไว้ให้กับผู้ตรวจสอบ ระบบความปลอดภัย, คุณอาจต้องการให้โปรไฟล์ผู้ใช้นี้สามารถทำงานได้ในช่วงเวลาที่ ผู้ตรวจสอบเข้ามาทำงาน. คุณอาจต้องการให้โปรไฟล์ผู้ใช้ทุกคนที่มีสิทธิพิเศษ *ALLOBJ (ซึ่งรวมถึงโปรไฟล์ผู้ใช้ QSECOFR) ไม่สามารถทำงานได้ระหว่างช่วงเวลาที่ ไม่ได้เปิดทำการ.

คุณสามารถใช้คำสั่ง Change Activation Schedule Entry (CHGACTSCDE) เพื่อทำให้โปรไฟล์ผู้ใช้สามารถทำงานหรือ ไม่ทำงานโดยอัตโนมัติ. สำหรับผู้ใช้แต่ละคนที่คุณต้องการจัดตารางเวลา, คุณสามารถสร้างรายการที่กำหนด ตารางเวลาของโปรไฟล์ผู้ใช้ได้.

ตัวอย่างเช่น, ถ้าคุณต้องการให้โปรไฟล์ผู้ใช้ QSECOFR สามารถทำงานได้ในช่วง 7 นาฬิกาจนถึง 22 นาฬิกา, คุณอาจป้อนตัวอย่างข้างล่างนี้ในหน้าจอของ CHGACTSCDE:

```
              Change Activation Scd Entry (CHGACTSCDE)

Type choices, press Enter.

User profile . . . . . . . . . . > QSECOFR       Name
Enable time  . . . . . . . . . . > '7:00'        Time, *NONE
Disable time . . . . . . . . . . > '22:00'       Time, *NONE
Days . . . . . . . . . . . . . . > *MON          *ALL, *MON, *TUE, *WED...
                                 > *TUE
                                 > *WED
                                 > *THU
               + for more values > *FRI
```

รูปที่ 2. Schedule Profile Activation Display–ตัวอย่าง

ในความเป็นจริง, คุณอาจต้องการให้โปรไฟล์ QSECOFR สามารถใช้งานได้ในจำนวน ที่จำกัดในแต่ละวัน. คุณสามารถใช้โปรไฟล์ผู้ใช้อื่นๆ ที่มีคลาส *SECOFR ในการทำงาน ส่วนใหญ่ของระบบ. ดังนั้น, คุณสามารถหลีกเลี่ยงการเปิดเผยโปรไฟล์ผู้ใช้ที่เป็นที่ รู้จักต่อผู้ที่บุกรุกเข้าระบบ.

คุณสามารถใช้คำสั่ง Display Audit Journal Entries (DSPAUDJRNE) เป็นระยะๆ เพื่อพิมพ์รายงานรายการตรวจสอบ CP (Change Profile) audit journal entries. ใช้รายการเหล่านี้ในการตรวจสอบระบบ เพื่อกำหนดให้โปรไฟล์ผู้ใช้ทำงาน หรือไม่ทำงานตามตารางเวลาที่วางไว้.

อีกวิธีที่ใช้ในการตรวจสอบให้แน่ใจว่าโปรไฟล์ผู้ใช้อยู่ในสภาพที่ถูกระงับการใช้งานในตารางเวลาที่ได้กำหนดไว้ก็คือการใช้คำสั่ง Print User Profile (PRTUSRPRF) . เมื่อคุณระบุค่า *PWDINFO สำหรับ ชนิดของรายงาน, ในรายงานจะมีสถานะของแต่ละ โปรไฟล์ผู้ใช้ที่ถูกเลือก. ตัวอย่างเช่น, ถ้าคุณทำให้ทุกโปรไฟล์ผู้ใช้ที่มีสิทธิพิเศษ *ALLOBJ ไม่สามารถใช้งานได้, คุณสามารถใช้คำสั่งต่อไปนี้ได้ทันที หลังจากที่โปรไฟล์เหล่านี้ไม่ทำงาน:

```
PRTUSRPRF TYPE(*PWDINFO) SELECT(*SPCAUT) SPCAUT(*ALLOBJ)
```

ทำการลบโปรไฟล์ผู้ใช้ที่เป็น inactive ออกไป

ระบบของคุณควรมีเฉพาะโปรไฟล์ผู้ใช้ที่จำเป็นเท่านั้น. ถ้าคุณไม่ต้องการ โปรไฟล์ผู้ใช้หนึ่ง เนื่องจากผู้ใช้ได้ลาออกไป หรือย้ายไปอยู่ส่วนอื่นภายในองค์กร, ให้ทำการลบโปรไฟล์ผู้ใช้นั้นออก. ถ้ามีบุคคลที่จากองค์กรไปเป็นระยะเวลานาน, ให้ตั้งโปรไฟล์ของผู้ใช้นั้นให้ไม่ทำงาน (disable หรือ deactivate). โปรไฟล์ผู้ใช้ที่ไม่จำเป็นอาจเป็นช่องทางที่ไม่ได้รับอนุญาตในการเข้าสู่ระบบของคุณ.

การระงับใช้โปรไฟล์ผู้ใช้โดยอัตโนมัติ

โดยปกติ คุณสามารถใช้คำสั่ง Analyze Profile Activity (ANZPRFACT) ในการทำให้โปรไฟล์ผู้ใช้ที่ไม่ได้ใช้งาน มาเป็นระยะเวลาที่กำหนดให้ไม่สามารถทำงานได้. เมื่อคุณใช้คำสั่ง ANZPRFACT, คุณต้องระบบจำนวนวันที่ไม่ได้ใช้งานที่ระบบมองหา. ระบบจะมองหาวันสุดท้ายที่ใช้งาน, วันที่เอากลับมา, และวันที่สร้างโปรไฟล์ผู้ใช้นั้น.

หลังจากที่คุณได้กำหนดค่าสำหรับคำสั่ง ANZPRFACT แล้ว, ระบบจะตั้งเวลาสำหรับงาน โดยจะทำทุกสัปดาห์ที่เวลา 1 นาฬิกา (เริ่มต้นหนึ่งวันหลังจากที่คุณได้กำหนดค่า). โดยงานจะทำการตรวจสอบทุกโปรไฟล์ และทำให้โปรไฟล์ที่ไม่ได้ใช้งานไม่สามารถทำงานได้. คุณไม่จำเป็นต้องเรียกใช้คำสั่ง ANZPRFACT อีกจนกว่าคุณจะต้องการเปลี่ยนแปลง จำนวนวันที่ไม่ได้ใช้งาน.

คุณสามารถใช้คำสั่ง Change Active Profile List (CHGACTPRFL) เพื่อสร้างรายการ ของโปรไฟล์ยกเว้นจากการประมวลผลของ ANZPRFACT. คำสั่ง CHGACTPRAL จะสร้างรายการ ของโปรไฟล์ผู้ใช้ที่คำสั่ง ANZPRFACT จะไม่ทำให้ไม่ทำงาน, โดยไม่สนใจระยะเวลา ที่โปรไฟล์เหล่านี้ไม่ได้ถูกใช้งาน.

เมื่อระบบมีการใช้คำสั่ง ANZPRFACT, จะมีการเขียนรายการ CP ลงใน เจอร์นัลตรวจสอบของแต่ละโปรไฟล์ผู้ใช้ที่ไม่ทำงาน. คุณสามารถใช้คำสั่ง DSPAUDJRNE เพื่อดูรายการโปรไฟล์ผู้ใช้ที่เพิ่งจะถูกทำให้ไม่ทำงาน.

หมายเหตุ: ระบบจะเขียนรายการตรวจสอบถ้าค่า QAUDCTL ถูกกำหนดเป็น *AUDLVL และค่ากำหนด ของระบบ QAUDLVL ถูกกำหนดเป็น *SECURITY.

อีกวิธีหนึ่งสำหรับการตรวจสอบให้แน่ใจว่าโปรไฟล์ผู้ใช้ถูกระงับการใช้งานอยู่ในตารางเวลาที่กำหนดก็คือการใช้คำสั่ง Print User Profile (PRTUSRPRF) . เมื่อคุณระบุค่า *PWDINFO สำหรับชนิดของรายงาน, รายงานจะมีการแสดงสถานะของ แต่ละโปรไฟล์ผู้ใช้ที่ถูกเลือก.

การลบโปรไฟล์ผู้ใช้ออกโดยอัตโนมัติ

คุณสามารถใช้คำสั่ง Change Expiration Schedule Entry (CHGEXPSCDE) ในการจัดการการลบหรือ ทำให้โปรไฟล์ผู้ใช้ไม่ทำงาน. ถ้าคุณทราบว่าผู้ใช้จากไปเป็นระยะเวลานาน, คุณสามารถตั้งเวลาที่โปรไฟล์ผู้ใช้จะถูกลบหรือทำให้ไม่ทำงานได้.

ในครั้งแรกที่คุณใช้คำสั่ง CHGEXPSCDE, จะมีการสร้าง job schedule entry ที่จะทำงานเมื่อ 1 นาทีหลังจากเที่ยงคืนในทุกๆ วัน. โดยงานนี้จะมองหา ไฟล์ QASECEXP เพื่อตัดสินใจว่าโปรไฟล์ผู้ใช้ใดถูกตั้งเวลาในการถูกลบภายในวันนั้น.

ด้วยคำสั่ง CHGEXPSCDE, คุณสามารถลบโปรไฟล์ผู้ใช้ หรือไม่ให้โปรไฟล์ผู้ใช้ทำงาน. หากคุณเลือกที่จะลบโปรไฟล์ผู้ใช้, คุณต้องระบุระบบที่จะทำงานกับอ็อบเจ็กต์ ที่ผู้ใช้นั้นเป็นเจ้าของ. ก่อนที่คุณจะตั้งเวลาให้ลบโปรไฟล์ผู้ใช้, คุณจะต้องค้นหาว่ามีอ็อบเจ็กต์ใดบ้างที่ผู้ใช้นั้นเป็นเจ้าของ. ตัวอย่างเช่น, ถ้าผู้ใช้นั้นเป็นเจ้าของโปรแกรมที่รับสิทธิมา, คุณต้องการให้โปรแกรมเหล่านั้น รับความเป็นเจ้าของของเจ้าของใหม่หรือไม่? หรือต้องการให้เจ้าของใหม่มีสิทธิ มากกว่าที่จำเป็น (เช่น สิทธิพิเศษ)? ในบางครั้ง, คุณจำเป็นต้องสร้างโปรไฟล์ ผู้ใช้ใหม่ที่มีสิทธิเฉพาะที่จะเป็นเจ้าของโปรแกรมที่ต้องมีการรับเอาสิทธิมา.

คุณยังต้องการต่อไปว่า จะมีปัญหากับแอ็พพลิเคชันใดบ้าง เมื่อคุณลบโปรไฟล์ผู้ใช้. ตัวอย่างเช่น, มีคำอธิบายงาน (job description) ใดที่ระบุให้โปรไฟล์ผู้ใช้นั้น เป็นผู้ใช้ดีฟอลต์?

คุณสามารถใช้คำสั่ง Display Expiration Schedule (DSPEXPSCD) เพื่อแสดงรายการของ โปรไฟล์ที่ถูกตั้งเวลาให้ทำให้ไม่สามารถใช้งานหรือลบทิ้ง.

คุณสามารถใช้คำสั่ง Display Authorized Users (DSPAUTUSR) เพื่อแสดงรายการ ของโปรไฟล์ผู้ใช้ทั้งหมดบนระบบของคุณ. และใช้คำสั่ง Delete User Profile (DLTUSRPRF) เพื่อลบโปรไฟล์ผู้ใช้ที่ไม่ใช้งานแล้ว.

Security note:: คุณทำให้โปรไฟล์ผู้ใช้ไม่สามารถทำงานได้โดยการตั้งค่าสถานะของ โปรไฟล์ผู้ใช้เป็น *DISABLED. เมื่อคุณทำให้โปรไฟล์ผู้ใช้ไม่ทำงาน,, นั่นคือ การทำให้ไม่สามารถใช้โปรไฟล์ผู้ใช้ให้ ทำงานแบบโต้ตอบได้. คุณจะไม่สามารถ sign on หรือเปลี่ยนงานของคุณไปยัง โปรไฟล์ผู้ใช้ที่ไม่สามารถใช้งานได้. งานประเภทแบ็ตช์ยังสามารถทำงานได้ภายใต้โปรไฟล์ผู้ใช้ที่ถูกทำให้ใช้งานไม่ได้.

หลีกเลี่ยงการใช้รหัสผ่านดีฟอลต์

เมื่อคุณสร้างโปรไฟล์ผู้ใช้ใหม่, ค่าดีฟอลต์ของรหัสผ่านคือ ชื่อของโปรไฟล์ ผู้ใช้. ซึ่งจะเป็นช่องทางให้บุคคลอื่นเข้ามาในระบบคุณได้, ถ้าคนนั้นทราบนโยบาย ในการกำหนดชื่อโปรไฟล์ของคุณ และทราบว่ามีผู้ร่วมงานใหม่ในองค์กรของคุณ.

เมื่อคุณสร้างโปรไฟล์ผู้ใช้ใหม่, ให้พิจารณาการใช้รหัสผ่านที่เป็นชื่อเฉพาะ ที่ไม่เป็นที่สังเกต, แทนที่จะใช้รหัสผ่านดีฟอลต์. บอกรหัสผ่านนี้แก่ผู้ใช้ใหม่ อย่างเป็นความลับ, เช่นในจดหมาย “Welcome to the System” ที่แสดงถึงกรอบ ของนโยบายด้านความปลอดภัย. และผู้ใช้ต้องเปลี่ยนรหัสผ่านในครั้งแรกที่ผู้ใช้ sign on โดยกำหนดโปรไฟล์ผู้ใช้นั้นเป็น PWDEXP (*YES).

คุณสามารถใช้คำสั่ง Analyze Default Passwords (ANZDFTPWD) เพื่อตรวจสอบ รหัสผ่านดีฟอลต์ของโปรไฟล์ผู้ใช้ทั้งหมดในระบบของคุณ. เมื่อคุณพิมพ์รายงาน, คุณมีทางเลือกที่จะกำหนดให้ระบบทำการเมื่อรหัสผ่านเป็นชื่อเดียวกับชื่อ โปรไฟล์ผู้ใช้ (เช่น การทำให้โปรไฟล์นั้นใช้งานไม่ได้). คำสั่ง ANZDFTPWD จะพิมพ์รายชื่อของโปรไฟล์และงานที่คำสั่งนี้ทำ เมื่อพบโปรไฟล์ที่มีปัญหา.

หมายเหตุ: จะมีการเก็บรหัสผ่านไว้ในระบบด้วยรูปแบบการเข้ารหัสทางเดียว. ซึ่งจะไม่ สามารถถอดรหัสได้. ระบบทำการเข้ารหัสให้กับรหัสผ่านที่ระบุ และเปรียบเทียบกับ รหัสผ่านที่เก็บไว้ เช่นเดียวกับที่ระบบทำการตรวจสอบรหัสผ่านของคุณเมื่อ sign on เข้าระบบ.

ถ้าคุณทำการตรวจสอบความล้มเหลวของสิทธิ (*AUTFAIL), ระบบจะบันทึกรายการ เจอร์นัลตรวจสอบ PW ของแต่ละโปรไฟล์ผู้ใช้ที่ *ไม่มี* รหัสผ่านดีฟอลต์ (สำหรับระบบที่รัน V4R1 หรือรีลีสก่อนหน้านี้). ตั้งแต่ V4R2, ระบบจะไม่บันทึกรายการเจอร์นัลตรวจสอบ PW เมื่อคุณรันคำสั่ง ANZDFTPWD.

การมอนิเตอร์ activity ในการ sign-on และใส่รหัสผ่าน

ถ้าคุณเป็นกังวลเกี่ยวกับการบุกรุกเข้าสูระบบของคุณ, คุณสามารถใช้คำสั่ง PRTUSRPRF เพื่อช่วยเหลือคุณ ในการเฝ้าสังเกตกิจกรรมการ sign-on และรหัสผ่าน.

คำแนะนำในการใช้รายงานนี้ มีดังนี้:

- ตรวจสอบดูว่าช่วงเวลาที่รหัสผ่านหมดอายุของโปรไฟล์ผู้ใช้บางคนยาวนานกว่า ค่าที่กำหนดโดยระบบหรือไม่ หรือดูว่าช่วงเวลาที่หมดอายุนั้นสมเหตุสมผลหรือไม่. ตัวอย่างเช่น, ในรายงาน USERY มีช่วงเวลาที่รหัสผ่านหมดอายุ คือ 120 วัน.
- รันรายงานนี้อย่างสม่ำเสมอ เพื่อสังเกตการ sign-on ที่ไม่เป็นผลสำเร็จ. บางคนที่พยายามเข้าสู่ระบบของคุณอาจรู้ว่าระบบของคุณอาจมีการทำบางอย่าง หลังจากที่ความพยายามในการเข้าสู่ระบบของคุณไม่สำเร็จหลายครั้ง. ในแต่ละคืน, ผู้ที่อาจจะเป็นผู้บุกรุกเหล่านี้อาจพยายามเจาะเข้าสู่ระบบด้วยจำนวนครั้งที่น้อย กว่าค่า QMAXSIGN เพื่อหลีกเลี่ยงการเตือนคุณในเรื่องการบุกรุก. อย่างไรก็ตาม, ให้เรียกใช้รายงานในทุกเช้าและให้สังเกตบางโปรไฟล์ที่มักจะมีการ sign-on ที่ไม่สำเร็จ, คุณอาจสงสัยได้ว่ากำลังจะมีปัญหาเกิดขึ้น.
- แยกแยะโปรไฟล์ผู้ใช้ที่ไม่ได้ถูกใช้งานมาเป็นเวลานาน หรือรหัสผ่านของ โปรไฟล์ผู้ใช้ที่ไม่ได้ถูกเปลี่ยนมาเป็นเวลานาน.

การบันทึกข้อมูลของรหัสผ่าน

ในการสนับสนุนฟังก์ชันเน็ตเวิร์กและความต้องการในด้านการสื่อสารบางประการ, เซิร์ฟเวอร์ iSeries มีวิธีการรักษาความปลอดภัยในการบันทึกรหัสผ่านที่สามารถถูกถอดรหัสได้. ระบบของคุณมีการใช้งานรหัสผ่านเหล่านี้, เช่น, สร้างการเชื่อมต่อกับระบบอื่นๆ โดยใช้ SLIP. (“ความปลอดภัยและเซสชันการ dial-out” ในหน้า 139 อธิบายถึงการใช้งานของรหัสผ่านที่เก็บไว้.)

เซิร์ฟเวอร์ iSeries ทำการบันทึกรหัสผ่านพิเศษเหล่านี้ลงในพื้นที่ที่ปลอดภัยที่ไม่สามารถเข้าถึงได้โปรแกรมของผู้ใช้หรืออินเตอร์เฟสใดๆ . มีเพียงฟังก์ชันของระบบที่มีสิทธิเท่านั้น ที่จะ สามารถตั้งและเรียกรหัสผ่านเหล่านี้ออกมาได้.

ตัวอย่างเช่น, เมื่อคุณใช้รหัสผ่านที่เก็บไว้กับการเชื่อมต่อภายนอกแบบ SLIP, คุณตั้งรหัสผ่านนี้โดยคำสั่งของระบบที่สามารถสร้างคอนฟิกูเรชันโปรไฟล์ (WRKTCPPTP). คุณจะต้องมี *IOSYSCFG เพื่อใช้คำสั่งนี้. สคริปต์ในการเชื่อมต่อที่มีโค้ดพิเศษ จะเรียกใช้รหัสผ่านและถอดรหัสระหว่างขั้นตอนการเชื่อมต่อไปภายนอก. รหัสผ่านที่ ถูกถอดรหัสจะไม่สามารถเห็นได้โดยผู้ใช้ หรือในบันทึกการใช้งาน (job log) ใดๆ .

ในฐานะผู้บริหารความปลอดภัย, คุณต้องตัดสินใจว่าคุณจะอนุญาตให้รหัสผ่านที่ สามารถถอดรหัสได้นั้นเก็บอยู่ในระบบของคุณหรือไม่. โดยใช้ค่ากำหนดของระบบ Retain Server Security Data

(QRETSVRSEC) ในการระบุค่า. ค่าดีฟอลต์คือ 0 (ไม่). ดังนั้น, ระบบของคุณจะไม่เก็บค่ารหัสผ่านที่สามารถถอดรหัสได้ จนกว่าคุณจะเป็นผู้ กำหนดค่ากำหนดของระบบนี้เอง.

ถ้าคุณต้องใช้รหัสผ่านที่เก็บไว้เหล่านี้ในการเชื่อมต่อกับระบบเครือข่าย, คุณจะต้องกำหนดนโยบายที่เหมาะสม และเข้าใจนโยบายและวิธีปฏิบัติของผู้ที่คุณ จะทำการติดต่อสื่อสารด้วย. ตัวอย่างเช่น, เมื่อคุณใช้ SLIP ในการสื่อสารกับเซิร์ฟเวอร์ iSeries อีกเซิร์ฟเวอร์หนึ่ง, ระบบทั้งสองควรจะพิจารณาในส่วนของการตั้งค่าโปรไฟล์ผู้ใช้พิเศษสำหรับการสร้างเซสชันนี้ขึ้น. โปรไฟล์พิเศษควรจะมีสิทธิในระบบที่จำกัด. ซึ่งจะจำกัดผลกระทบต่อระบบของคุณในกรณีที่รหัสผ่านที่เก็บไว้นี้ถูกละเมิดโดย ผู้ที่คุณเชื่อมต่อด้วย.

บทที่ 4. การปรับแต่งค่าของ iSeries เพื่อใช้งาน Security Tools

ข้อมูลนี้อธิบายวิธีการติดตั้งระบบของคุณเพื่อที่จะใช้ security tools ที่เป็นส่วนหนึ่งของ OS/400. เมื่อคุณติดตั้ง OS/400, ทูลของ security tools ก็พร้อมที่จะใช้งานได้. หัวข้อต่อไปนี้ จะให้คำแนะนำเกี่ยวกับขั้นตอนการปฏิบัติกับ security tools.

ทำการติดตั้ง Security Tools อย่างระมัดระวัง

เมื่อคุณติดตั้ง OS/400, อ็อบเจ็กต์ที่สัมพันธ์กับ security tools จะปลอดภัย. เพื่อทำให้ security tools ปลอดภัย, ควรหลีกเลี่ยงการเปลี่ยนแปลงสิทธิใดๆ ในอ็อบเจ็กต์ ของ security tool.

ต่อไปนี้คือ การตั้งความปลอดภัยและสิ่งจำเป็นสำหรับอ็อบเจ็กต์ของ security tool :

- โปรแกรมและคำสั่งของ security tool จะอยู่ในไลบรารีผลิตภัณฑ์ QSYS. คำสั่งและโปรแกรมที่มาพร้อมกับเครื่องจะมีสิทธิพับลิกเป็น *EXCLUDE. คำสั่งของ security tool หลายคำสั่ง จะสร้างไฟล์ในไลบรารี QUSRSYS. เมื่อระบบสร้างไฟล์เหล่านี้, สิทธิพับลิกของไฟล์ ก็จะเป็น *EXCLUDE.

  ไฟล์ที่มีข้อมูลสำหรับการสร้างรายงานการเปลี่ยนแปลง จะมีชื่อเริ่มต้นด้วย QSEC. ไฟล์ที่มีข้อมูลเกี่ยวกับการจัดการ โปรไฟล์ผู้ใช้จะมีชื่อเริ่มต้นด้วย QASEC. ไฟล์เหล่านี้จะมีข้อมูล ของระบบคุณที่เป็นความลับ. ดังนั้น, คุณจะต้องไม่เปลี่ยนสิทธิพับลิกในไฟล์ เหล่านี้.
- security tools จะใช้ค่าปกติของระบบที่จัดเตรียมสำหรับการพิมพ์ออกโดยตรง . รายงานเหล่านี้จะมีข้อมูล เกี่ยวกับระบบของคุณที่เป็นความลับ. เพื่อให้งานที่พิมพ์ออกไปยังเอาต์พุตคิว ที่มีการป้องกัน, ให้เปลี่ยนแปลงโปรไฟล์ผู้ใช้หรือคำอธิบายงาน (job description) ของผู้ใช้ที่จะรัน security tools ให้เหมาะสม.
- เนื่องจากฟังก์ชันความปลอดภัย และมีการเข้าถึงหลายอ็อบเจ็กต์ในระบบ, คำสั่งของ security tool จึงต้องการสิทธิพิเศษ *ALLOBJ. และในบางคำสั่งยังต้องการสิทธิพิเศษ *SECADM, *AUDIT, หรือ *IOSYSCFG. เพื่อให้มั่นใจว่าคำสั่งสามารถทำงานได้สำเร็จ, คุณต้อง sign on เป็นเจ้าหน้าที่รักษาความปลอดภัยระบบ เมื่อคุณใช้ security tools. เพราะฉะนั้น, คุณไม่จำเป็นต้องให้สิทธิไพรเวตกับคำสั่งใดๆ ของ security tool .

หลีกเลี่ยงไฟล์ที่ขัดแย้งกัน

คำสั่งเกี่ยวกับรายงานของ security tool หลายๆ คำสั่ง จะสร้างไฟล์ฐานข้อมูลที่คุณ สามารถใช้พิมพ์เวอร์ชันที่เปลี่ยนแปลงของรายงานได้. “คำสั่งและเมนูสำหรับคำสั่งที่เกี่ยวกับความปลอดภัย” ในหน้า 32 แสดงชื่อไฟล์ของแต่ละคำสั่ง.คุณสามารถรันได้เพียงหนึ่งคำสั่งต่อหนึ่งงานในเวลา เดียวกัน. คำสั่งส่วนใหญ่ปัจจุบันมีการตรวจสอบให้ทำตามในลักษณะนี้. หากคุณรันคำสั่ง ในขณะที่มีงานอื่นยังกำลังรันคำสั่งนั้นอยู่, คุณจะได้รับข้อความแสดงความผิดพลาด.

งานที่เกี่ยวกับการพิมพ์ส่วนใหญ่ เป็นงานที่ใช้ระยะเวลานาน. คุณจึงจำเป็น ที่จะต้องหลีกเลี่ยงความขัดแย้งของไฟล์ เมื่อคุณส่งรายงานไปยังแบตช์ หรือเพิ่ม เข้าไปในตารางเวลางาน (job scheduler).

ตัวอย่างเช่น, คุณอาจต้องการพิมพ์รายงานของ PRTUSRPRF สองเวอร์ชันที่มีความแตกต่างในกฎเกณฑ์การเลือก. ถ้าคุณส่งรายงาน เข้าไปในแบตช์, คุณจะต้องใช้คิวงานที่ทำงานเพียงหนึ่งงานในเวลาเดียวกัน เพื่อให้ มั่นใจว่างานพิมพ์รายงานจะทำงานตามลำดับกัน.

ถ้าคุณใช้ตารางเวลางาน, คุณจำเป็นต้องตั้งเวลาของสองงานห่างกันเพียงพอที่ จะทำให้ เวอร์ชันแรกพิมพ์เสร็จก่อนที่งานที่สองจะเริ่ม.

การบันทึก Security Tools

คุณได้บันทึกโปรแกรมของ security tool เมื่อคุณรันคำสั่ง Save System (SAVSYS) หรือเลือกอ็อพชันจากเมนู Save ซึ่งรันคำสั่ง SAVSYS.

ไฟล์ของ security tool จะอยู่ในไลบรารี QUSRSYS. การจัดเก็บไลบรารีนี้ ควรเป็นส่วนหนึ่งของขั้นตอนปฏิบัติการปกติของคุณ. ไลบรารี QUSRSYS จะบรรจุข้อมูล สำหรับโปรแกรมไลเซนส์ในระบบของคุณ. ดูใน Information Center สำหรับข้อมูล เพิ่มเติมเกี่ยวกับคำสั่งและอ็อพชัน สำหรับการบันทึกไลบรารี QUSRSYS.

คำสั่งและเมนูสำหรับคำสั่งที่เกี่ยวกับความปลอดภัย

ในส่วนนี้ จะอธิบายเกี่ยวกับคำสั่งและเมนูของเครื่องมือด้านความปลอดภัย. ตัวอย่างการใช้งานคำสั่งถูกรวบรวมอยู่ในข้อมูลนี้โดยตลอด.

เมนูสำหรับเครื่องมือด้านความปลอดภัยมี 2 เมนู:

- เมนู SECTOOLS (Security Tools) เพื่อรันคำสั่งแบบโต้ตอบ.
- เมนู SECBATCH (Submit or Schedule Security Reports to Batch) เพื่อรันคำสั่ง รายงานในแบ็ตช์. เมนู SECBATCH มีสองส่วน. ส่วนแรกของเมนู ใช้คำสั่ง Submit Job (SBMJOB) ในการส่งรายงานเข้าไปประมวลผลในแบตช์ทันที.

  ส่วนที่สองของเมนู ใช้ คำสั่ง Add Job Schedule Entry (ADDJOBSCDE). คุณสามารถใช้ในการตั้งเวลา ให้ทำ รายงานด้านความปลอดภัยเป็นระยะๆ ณ วันและเวลาที่กำหนด.

ตัวเลือกเมนูของทูลที่เกี่ยวกับความปลอดภัย

ตารางที่ 6อธิบายถึงอ็อพชันของเมนูและคำสั่งที่สัมพันธ์กัน:

ตารางที่ 6. คำสั่งที่ใช้เป็นทูลที่ใช้กับโปรไฟล์ผู้ใช้

เมนูตัวเลือกที่[1]	ชื่อคำสั่ง	คำอธิบาย	ไฟล์ฐานข้อมูลที่ใช้
1	ANZDFTPWD	ใช้คำสั่ง Analyze Default Passwords เพื่อทำรายงานและจัดการกับโปรไฟล์ผู้ใช้ที่มีรหัสผ่านตรงกับชื่อโปรไฟล์ผู้ใช้.	QASECPWD[2]
2	DSPACTPRFL	ใช้คำสั่ง Display Active Profile List เพื่อแสดงผลหรือพิมพ์รายชื่อของโปรไฟล์ผู้ใช้ที่ยกเว้นจากการถูกประมวลผลของ คำสั่ง ANZPRFACT.	QASECIDL[2]

ตารางที่ 6. คำสั่งที่ใช้เป็นทูลที่ใช้กับโปรไฟล์ผู้ใช้ (ต่อ)

เมนูตัวเลือกที่[1]	ชื่อคำสั่ง	คำอธิบาย	ไฟล์ฐานข้อมูลที่ใช้
3	CHGACTPRFL	ใช้คำสั่ง Change Active Profile List เพื่อเพิ่มหรือลบโปรไฟล์ผู้ใช้ที่อยู่ในรายชื่อที่ยกเว้นจากคำสั่ง ANZPRFACT. โปรไฟล์ผู้ใช้ที่อยู่ในรายชื่อโปรไฟล์ที่แอ็คทีฟจะยังคงแอ็คทีฟไปตลอด (จนกว่าคุณลบโปรไฟล์นั้นออกจากรายการ). คำสั่ง ANZPRFACT ไม่ทำให้โปรไฟล์ ที่อยู่ในรายชื่อโปรไฟล์ที่ใช้งานไม่สามารถใช้งานได้โดยไม่สนใจว่าโปรไฟล์นั้น ไม่ได้ใช้งานมานานเพียงใด.	QASECIDL[2]
4	ANZPRFACT	ใช้คำสั่ง Analyze Profile Activity เพื่อทำให้โปรไฟล์ผู้ใช้ที่ไม่ได้ถูกใช้งานตามจำนวนวันที่กำหนดไม่สามารถใช้งานได้. หลังจากที่คุณใช้คำสั่ง ANZPRFACT ในการกำหนดจำนวนวัน, ระบบจะรันคำสั่ง ANZPRFACT ในทุกคืน. คุณสามารถใช้คำสั่ง CHGACTPRFL ยกเว้นโปรไฟล์ผู้ใช้จากการถูกทำให้ไม่สามารถใช้งานได้.	QASECIDL[2]
5	DSPACTSCD	ใช้คำสั่ง Display Profile Activation Schedule เพื่อแสดงผลหรือพิมพ์ข้อมูลเกี่ยวกับตารางเวลาใช้งานได้หรือใช้งานไม่ได้ของ โปรไฟล์ผู้ใช้ที่ระบุ. คุณสร้างตารางเวลานั้นได้ ด้วยคำสั่ง CHGACTSCDE.	QASECACT[2]
6	CHGACTSCDE	ใช้คำสั่ง Change Activation Schedule Entry เพื่อทำให้โปรไฟล์ผู้ใช้ sign on ได้เฉพาะในเวลาที่กำหนดของวันหรือสัปดาห์. สำหรับแต่ละโปรไฟล์ที่คุณสร้างตารางเวลา, ระบบจะสร้างรายการในตารางเวลางาน เพื่อทำให้มีเวลาที่ใช้งานได้และใช้งานไม่ได้.	QASECACT[2]
7	DSPEXPSCD	ใช้คำสั่ง Display Expiration Schedule เพื่อแสดงผลหรือพิมพ์รายชื่อของโปรไฟล์ผู้ใช้ที่ถูกตั้งตารางเวลาให้ใช้งานไม่ได้ หรือถูกลบออกจากระบบในอนาคต. โดยใช้คำสั่ง CHGEXPSCDE ในการตั้งค่าโปรไฟล์ผู้ใช้ที่หมดอายุ.	QASECEXP[2]
8	CHGEXPSCDE	ใช้คำสั่ง Change Expiration Schedule Entry ตั้งตารางเวลาของโปรไฟล์ผู้ใช้เพื่อทำการลบ. คุณสามารถลบแบบชั่วคราว (โดยทำให้ใช้งานไม่ได้) หรือลบออกจากระบบ. คำสั่งนี้ใช้ตารางเวลางานที่เรียกใช้ทุกวัน ที่เวลา 00:01 (1 นาทีหลังเที่ยงคืน). โดยงานจะดูที่ไฟล์ QASECEXP เพื่อหาว่ามีโปรไฟล์ผู้ใช้ใดที่ถูกตั้งให้หมดอายุ ในวันนั้น. ใช้คำสั่ง DSPEXPSCD เพื่อแสดงโปรไฟล์ผู้ใช้ที่ถูกกำหนดให้หมดอายุ.	QASECEXP[2]

ตารางที่ 6. คำสั่งที่ใช้เป็นทูลที่ใช้กับโปรไฟล์ผู้ใช้ (ต่อ)

เมนูตัวเลือกที่[1]	ชื่อคำสั่ง	คำอธิบาย	ไฟล์ฐานข้อมูลที่ใช้
9	PRTPRFINT	ใช้คำสั่ง Print Profile Internals เพื่อพิมพ์ รายงานที่มีข้อมูลของจำนวนรายการที่อยู่ในโปรไฟล์ผู้ใช้. จำนวนของรายการเป็น ตัวบอกขนาดของโปรไฟล์ผู้ใช้.	

หมายเหตุ:

1. อ็อพชันมาจากเมนู SECTOOLS.
2. ไฟล์นี้อยู่ในไลบรารี QUSRSYS.

คุณสามารถ page down บนเมนูเพื่อดูอ็อพชันเพิ่มเติม. ตารางที่ 7อธิบายถึงอ็อพชันและคำสั่งที่เกี่ยวข้องกับการตรวจสอบความปลอดภัย:

ตารางที่ 7. คำสั่งที่เป็นทูลที่ใช้กับการตรวจสอบความปลอดภัย

เมนูตัวเลือกที่[1]	ชื่อคำสั่ง	คำอธิบาย	ไฟล์ฐานข้อมูลที่ใช้
10	CHGSECAUD	ใช้คำสั่ง Change Security Auditing เพื่อจัด เตรียมการตรวจสอบความปลอดภัยและเปลี่ยนค่ากำหนดของระบบที่ควบคุมการตรวจสอบความปลอดภัย. เมื่อคุณรันคำสั่ง CHGSECAUD, ระบบจะสร้างเจอร์นัลการตรวจสอบความปลอดภัย (QAUDJRN) หากยังไม่มีอยู่ในระบบ. คำสั่ง CHGSECAUD มีอ็อพชันที่ทำให้การตั้งค่ากำหนดของระบบ QAUDLVL (audit level) ง่ายขึ้น. คุณสามารถกำหนดค่า *ALL เพื่อทำให้ระดับ การตรวจสอบทั้งหมดทำงาน. หรือ, คุณอาจระบุค่า *DFTSET เพื่อให้ค่าที่ใช้อยู่ปกติ (*AUTFAIL, *CREATE, *DELETE, *SECURITY, และ *SAVRST) ทำงานได้. **หมายเหตุ:** หากคุณใช้เครื่องมือความปลอดภัยเพื่อจัดเตรียมการตรวจสอบ, ต้องแน่ใจว่า ได้มีการ วางแผนเพื่อบริหารตัวรับบันทึกการตรวจสอบ (audit journal receiver) ของคุณแล้ว. มิฉะนั้น, ในไม่ช้า คุณอาจได้พบกับปัญหา การใช้พื้นที่ในดิสก์ของคุณ .	
11	DSPSECAUD	ใช้คำสั่ง Display Security Auditing เพื่อแสดง ข้อมูลเกี่ยวกับเจอร์นัลการตรวจสอบความปลอดภัย และค่ากำหนดของระบบที่ควบคุม การตรวจสอบความปลอดภัย.	

หมายเหตุ:

1. อ็อพชันมาจากเมนู SECTOOLS.

ใช้เมนูแบ็ตช์ที่เกี่ยวกับการรักษาความปลอดภัย

ภาพต่อไปนี้ คือส่วนแรกของเมนู SECBATCH:

```
SECBATCH          ทำการส่งค่าหรือกำหนดตารางเวลาของการรักษาความปลอดภัยให้กับระบบแบ็ตช์   :
 เลือกข้อใดข้อหนึ่งจากตัวเลือกต่อไปนี้:

 การส่งรายงานให้กับแบ็ตช์
     3. Authorization list authorities
     4. Command authority
     5. Command private authorities
     6. Communications security
     7. Directory authority
     8. Directory private authority
     9. Document authority
    10. Document private authority
    11. File authority
    12. File private authority
    13. Folder authority
```

เมื่อคุณเลือกตัวเลือกจากเมนูนี้, คุณจะมองเห็นหน้าจอ Submit Job (SBMJOB) . หากคุณต้องการเปลี่ยนดีฟอลต์อ็อพชันของคำสั่ง, คุณสามารถกด F4 (Prompt) บนบรรทัด *Command to run*.

เพื่อดู Schedule Batch Reports, ให้กด page down บนเมนู SECBATCH. โดยการใช้ อ็อพชันในส่วนนี้ของเมนู, คุณสามารถจัดเตรียมให้ระบบของคุณรันเวอร์ชันที่ เปลี่ยนแปลงของรายงานได้เป็นประจำ เป็นต้น . คุณสามารถใช้ page down สำหรับอ็อพชันเพิ่มเติม. เมื่อคุณเลือกตัวเลือกจากส่วนนี้ของเมนู, คุณจะมองเห็นหน้าจอ Add Job Schedule Entry (ADDJOBSCDE) .

คุณสามารถวางเคอร์เซอร์บนบรรทัด *Command to run* และกด F4 (Prompt) เพื่อเลือกค่าติดตั้งอื่นๆ สำหรับรายงาน. คุณต้องกำหนดชื่องาน ที่มีความหมาย เพื่อที่คุณจะได้จำชื่อรายการได้เมื่อคุณแสดงรายการตารางเวลางาน (job schedule entry).

เมนูอ็อพชันของงานแบ็ตช์ที่เกี่ยวกับความปลอดภัย

ตารางที่ 8 ในหน้า 36 แสดงอ็อพชันของเมนู และคำสั่งที่เกี่ยวข้องกับรายงาน ด้านความปลอดภัย.

เมื่อคุณรันรายงานด้านความปลอดภัย, ระบบจะพิมพ์เฉพาะข้อมูลที่ตรงตามเกณฑ์ การเลือกที่คุณกำหนด และเกณฑ์การเลือก (selection criteria) สำหรับเครื่องมือ. ตัวอย่างเช่น, คำอธิบายงาน (job description) ที่กำหนดชื่อโปรไฟล์ผู้ใช้ และความปลอดภัยที่เกี่ยวข้อง. ดังนั้น, รายงาน job description (PRTJOBDAUT) จะพิมพ์คำอธิบายงาน (job description) เฉพาะที่อยู่ในไลบรารีที่กำหนด ถ้า สิทธิพับลิกของคำอธิบายงานไม่ใช่ *EXCLUDE *และ* คำอธิบายงานระบุชื่อโปรไฟล์ผู้ใช้ในพารามิเตอร์ USER.

เช่นเดียวกัน, เมื่อคุณพิมพ์ข้อมูลของระบบย่อย (คำสั่ง PRTSBSDAUT), ระบบจะพิมพ์ ข้อมูลเกี่ยวกับระบบย่อยเฉพาะเมื่อคำอธิบายระบบย่อย (subsystem description) มีรายการการสื่อสารที่ระบุโปรไฟล์ผู้ใช้.

หากรายงานพิมพ์ข้อมูลน้อยกว่าที่คุณคาดไว้, ให้ดูในคำอธิบายออนไลน์ เพื่อค้นหา เกณฑ์การเลือกของรายงานนั้น.

ตารางที่ 8. คำสั่งสำหรับรายงานเกี่ยวกับความปลอดภัย

เมนูตัวเลือกที่[1]	ชื่อคำสั่ง	คำอธิบาย	ไฟล์ฐานข้อมูลที่ใช้
1, 40	PRTADPOBJ	ใช้คำสั่ง Print Adopting Objects พิมพ์รายการ ของอ็อบเจ็กต์ที่ได้รับสิทธิของโปรไฟล์ผู้ใช้ที่ระบุไว้. คุณสามารถระบุเป็น หนึ่งโปรไฟล์เดี่ยว หรือชื่อโปรไฟล์ทั่วไป (เช่น โปรไฟล์ที่ขึ้นต้นด้วย Q) หรือทุกโปรไฟล์ผู้ใช้ในระบบ. รายงานฉบับนี้มีสองเวอร์ชัน. รายงานฉบับเต็ม (full report) แสดงรายชื่อของอ็อบเจ็กต์ที่เปลี่ยนแปลงทั้งหมดที่ตรงกับเกณฑ์ การเลือก. รายงานส่วนที่เปลี่ยนแปลง จะแสดงความแตกต่างระหว่างอ็อบเจ็กต์ที่ เปลี่ยนแปลงที่ใช้ในระบบ ณ ขณะนี้กับอ็อบเจ็กต์ที่เปลี่ยนแปลงที่อยู่ในระบบ เมื่อคุณรันรายงานนี้ในครั้งที่แล้ว.	QSECADPOLD[2]
2, 41	DSPAUDJRNE	ใช้คำสั่ง Display Audit Journal Entries เพื่อแสดงหรือพิมพ์ข้อมูลเกี่ยวกับรายการในเจอร์นัลการตรวจสอบความปลอดภัย. คุณสามารถเลือกกำหนดชนิดของรายการ, ผู้ใช้ หรือช่วงเวลา.	QASYxxJ4[3]
3, 42	PRTPVTAUT *AUTL	เมื่อคุณใช้คำสั่ง Print Private Authorities สำหรับอ็อบเจ็กต์ *AUTL, คุณจะได้รายการของ authorization list ทั้งหมดในระบบ. รายงานจะแสดงถึงผู้ใช้ผู้มีสิทธิในแต่ละรายการ และสิทธิที่ผู้ใช้มีต่อรายการนั้น. ให้ใช้ข้อมูลนี้เพื่อช่วยคุณวิเคราะห์ต้นทางของสิทธิอ็อบเจ็กต์ในระบบของคุณ. รายงานฉบับนี้มีสามเวอร์ชัน. รายงานฉบับเต็มแสดง authorization list ทั้งหมดในระบบ. รายงานส่วนที่เปลี่ยนแปลงแสดงส่วนที่เพิ่มขึ้นหรือเปลี่ยนแปลงของการให้สิทธิตั้งแต่ที่คุณรันรายงานนี้ครั้งก่อน. รายงานการลบ (deleted report) แสดงรายชื่อ ของผู้ใช้ที่มีสิทธิใน authorization list ที่ถูกลบ หลังจากที่คุณรันรายงานนี้ ครั้งที่แล้ว. เมื่อคุณพิมพ์รายงานฉบับเต็ม คุณมีอ็อพชันที่เลือกพิมพ์รายชื่อของอ็อบเจ็กต์ ที่แต่ละ authorization list ปลอดภัย. ระบบจะสร้างรายงานที่แยกกันของแต่ละ authorization list.	QSECATLOLD[2]
6, 45	PRTCMNSEC	ใช้คำสั่ง Print Communications Security เพื่อพิมพ์ค่าติดตั้งที่เกี่ยวข้องกับความปลอดภัยสำหรับอ็อบเจ็กต์ ที่ส่งผลต่อ การสื่อสารในระบบของคุณ. ค่าเหล่านี้จะส่งผลต่อวิธีการที่ผู้ใช้และงานเข้าสู่ระบบ ของคุณ. คำสั่งนี้จะสร้างสองรายงาน: รายงานที่แสดงค่าติดตั้งของรายการคอนฟิกูเรชันของระบบ และรายงานที่แสดงพารามิเตอร์ที่เกี่ยวข้องกับความปลอดภัยของ line descriptions, controllers และ device descriptions. ในแต่ละรายงาน จะมีทั้งเวอร์ชันเต็ม และเวอร์ชันที่แสดงส่วนที่เปลี่ยนแปลง.	QSECCMNOLD[2]

ตารางที่ 8. คำสั่งสำหรับรายงานเกี่ยวกับความปลอดภัย (ต่อ)

เมนูตัวเลือกที่[1]	ชื่อคำสั่ง	คำอธิบาย	ไฟล์ฐานข้อมูลที่ใช้
15, 54	PRTJOBDAUT	ใช้คำสั่ง Print Job Description Authority เพื่อพิมพ์รายชื่อของคำอธิบายงาน ที่ระบุโปรไฟล์ผู้ใช้ และมีสิทธิพับลิกที่ไม่ใช่ *EXCLUDE. รายงานจะแสดงสิทธิพิเศษสำหรับโปรไฟล์ผู้ใช้ที่ระบุไว้ใน คำอธิบายงาน. ราบงานฉบับนี้มีสองเวอร์ชัน. รายงานฉบับเต็ม แสดงรายชื่อของ อ็อบเจ็กต์คำอธิบายงานทั้งหมดที่ตรงกับเกณฑ์การเลือก. รายงานส่วนที่เปลี่ยนแปลง จะแสดงความแตกต่างระหว่างอ็อบเจ็กต์คำอธิบายงานที่ใช้ในระบบ ณ ขณะนี้กับอ็อบเจ็กต์ คำอธิบายงานที่อยู่ในระบบ เมื่อคุณรันรายงานนี้ในครั้งที่แล้ว.	QSECJBDOLD[2]
ดูหมายเหตุ 4.	PRTPUBAUT	ใช้คำสั่ง Print Publicly Authorized Objects เพื่อพิมพ์รายชื่อของอ็อบเจ็กต์ที่มีสิทธิพับลิกที่ไม่ใช่ *EXCLUDE. เมื่อคุณเรียกใช้คำสั่ง คุณต้องกำหนดชนิดของอ็อบเจ็กต์และไลบรารีหนึ่ง หรือหลายไลบรารีสำหรับรายงาน. ใช้คำสั่ง PRTPUBAUT เพื่อพิมพ์ข้อมูลเกี่ยวกับ อ็อบเจ็กต์ที่ผู้ใช้ทุกคนในระบบสามารถเข้าถึงได้. ราบงานฉบับนี้มีสองเวอร์ชัน. รายงานฉบับเต็ม แสดงรายชื่อของอ็อบเจ็กต์ทั้งหมดที่ตรงกับเกณฑ์การเลือก. รายงานส่วนที่เปลี่ยนแปลง จะแสดงความแตกต่างระหว่างอ็อบเจ็กต์ที่ใช้ในระบบ ณ ขณะนี้ กับอ็อบเจ็กต์ (ที่เป็นประเภทเดียวกัน อยู่ในไลบรารีเดียวกัน) ที่อยู่ในระบบเมื่อคุณรันรายงานนี้ในครั้งที่แล้ว.	QPBxxxxxx[5]
ดูหมายเหตุ 5.	PRTPVTAUT	ใช้คำสั่ง Print Private Authorities เพื่อพิมพ์ รายชื่อของสิทธิไพรเวตไปยังอ็อบเจ็กต์ประเภทที่กำหนด และอยู่ในไลบรารีที่กำหนด. ใช้รายงานนี้ช่วยคุณในการหาต้นทางของสิทธิในอ็อบเจ็กต์. รายงานฉบับนี้มีสามเวอร์ชัน. รายงานฉบับเต็ม แสดงรายชื่อของอ็อบเจ็กต์ทั้งหมดที่ตรงกับเกณฑ์การเลือก. รายงานส่วนที่เปลี่ยนแปลง จะแสดงความแตกต่างระหว่างอ็อบเจ็กต์ที่ใช้ในระบบ ณ ขณะนี้ กับอ็อบเจ็กต์ (ที่เป็นประเภทเดียวกัน อยู่ในไลบรารีเดียวกัน) ที่อยู่ในระบบเมื่อคุณรันรายงานนี้ในครั้งที่แล้ว. รายงานการลบ (deleted report) แสดงรายชื่อ ของผู้ใช้ที่มีสิทธิในอ็อบเจ็กต์ ที่ถูกลบหลังจากที่คุณพิมพ์รายงานนี้ครั้งที่แล้ว.	QPVxxxxxx[5]

ตารางที่ 8. คำสั่งสำหรับรายงานเกี่ยวกับความปลอดภัย (ต่อ)

เมนูตัวเลือกที่[1]	ชื่อคำสั่ง	คำอธิบาย	ไฟล์ฐานข้อมูลที่ใช้
24, 63	PRTQAUT	ใช้คำสั่ง Print Queue Report พิมพ์ค่าติดตั้ง ความปลอดภัยของเอาต์พุตคิวและคิวงานในระบบของคุณ. ค่าติดตั้งเหล่านี้ควบคุมว่า ผู้ใดสามารถดูหรือเปลี่ยนแปลงรายการในเอาต์พุตคิวหรือคิวงาน. รายงานฉบับนี้มีสองเวอร์ชัน. รายงานฉบับเต็ม แสดงรายชื่อของอ็อบเจ็กต์เอาต์พุตคิว และคิวงานทั้งหมดที่ตรงกับเกณฑ์การเลือก. รายงานส่วนที่เปลี่ยนแปลง จะแสดง ความแตกต่างระหว่างอ็อบเจ็กต์เอาต์พุตคิวและคิวงานที่เปลี่ยนแปลงที่ใช้ในระบบ ณ ขณะนี้กับอ็อบเจ็กต์เอาต์พุตคิวและคิวงานที่เปลี่ยนแปลงที่อยู่ในระบบ เมื่อคุณ รันรายงานนี้ในครั้งที่แล้ว.	QSECQOLD[2]
25, 64	PRTSBSDAUT	ใช้คำสั่ง Print Subsystem Description เพื่อพิมพ์ รายการสื่อสารที่เกี่ยวข้องกับความปลอดภัยของคำอธิบายระบบย่อย (subsystem description) ในระบบของคุณ. ค่าติดตั้งนี้ควบคุมวิธีการที่งานสามารถเข้าสู่ระบบของคุณ และวิธีที่งานรัน. รายงานนี้จะพิมพ์คำอธิบายระบบย่อย (subsystem description) เมื่อมีรายการสื่อสารที่ระบุชื่อโปรไฟล์ผู้ใช้. รายงานฉบับนี้มีสองเวอร์ชัน. รายงานฉบับเต็ม แสดงรายชื่อของ อ็อบเจ็กต์ subsystem descriptions ทั้งหมดที่ตรงกับเกณฑ์การเลือก. รายงานส่วนที่เปลี่ยนแปลง จะแสดงความแตกต่างระหว่างอ็อบเจ็กต์ subsystem descriptions ที่ใช้ในระบบ ณ ขณะนี้กับอ็อบเจ็กต์ subsystem descriptions ที่อยู่ในระบบ เมื่อคุณรันรายงานนี้ในครั้งที่แล้ว.	QSECSBDOLD[2]
26, 65	PRTSYSSECA	ใช้คำสั่ง Print System Security Attributes เพื่อพิมพ์รายการค่ากำหนดของระบบ และแอ็ตทริบิวต์ของเครือข่ายที่เกี่ยวข้องกับ ความปลอดภัย. รายงานจะแสดงถึงค่าที่ใช้ในปัจจุบันและค่าที่แนะนำ.	
27, 66	PRTTRGPGM	ใช้คำสั่ง Print Trigger Programs พิมพ์รายชื่อ ของทริกเกอร์โปรแกรมที่สัมพันธ์กับไฟล์ฐานข้อมูลในระบบของคุณ. รายงานฉบับนี้มีสองเวอร์ชัน. รายงานฉบับเต็ม แสดงรายการของทริกเกอร์โปรแกรมทุกโปรแกรมที่ถูก กำหนด และตรงกับเกณฑ์การเลือกของคุณ. รายงานส่วนที่เปลี่ยนแปลงจะแสดงรายการของ ทริกเกอร์โปรแกรมที่ถูกกำหนด กำหนด ตั้งแต่คุณรันรายงานนี้ในครั้งที่แล้ว.	QSECTRGOLD[2]

ตารางที่ 8. คำสั่งสำหรับรายงานเกี่ยวกับความปลอดภัย (ต่อ)

เมนูตัวเลือกที่[1]	ชื่อคำสั่ง	คำอธิบาย	ไฟล์ฐานข้อมูลที่ใช้
28, 67	PRTUSROBJ	ใช้คำสั่ง Print User Objects ในการพิมพ์รายการอ็อบเจ็กต์ของผู้ใช้ (อ็อบเจ็กต์ที่ไม่ได้กำหนดโดย IBM) ที่อยู่ในไลบรารี. คุณอาจใช้รายงานนี้พิมพ์รายชื่อของอ็อบเจ็กต์ผู้ใช้ที่อยู่ในไลบรารีหนึ่ง (เช่น QSYS) ที่อยู่ใน system portion ของรายชื่อไลบรารี. รายงานฉบับนี้มีสองเวอร์ชัน. รายงานฉบับเต็ม แสดงรายชื่อของอ็อบเจ็กต์ผู้ใช้ทั้งหมดที่ตรงกับ เกณฑ์การเลือก. รายงานส่วนที่เปลี่ยนแปลง จะแสดงความแตกต่างระหว่างอ็อบเจ็กต์ ผู้ใช้ที่อยู่ในระบบ ณ ขณะนี้กับอ็อบเจ็กต์ผู้ใช้ที่อยู่ในระบบ เมื่อคุณรัน รายงานนี้ในครั้งที่แล้ว.	QSECPUOLD[2]
29, 68	PRTUSRPRF	ใช้คำสั่ง Print User Profile เพื่อวิเคราะห์โปรไฟล์ที่ตรงกับเกณฑ์ที่กำหนด. คุณสามารถเลือกโปรไฟล์ผู้ใช้จากสิทธิพิเศษ, คลาสผู้ใช้, หรือความไม่ตรงกันระหว่างสิทธิพิเศษกับคลาสผู้ใช้. คุณสามารถพิมพ์ ข้อมูลเกี่ยวกับสิทธิ, ข้อมูลของสภาพแวดล้อม (environment information), ข้อมูลของรหัสผ่าน, หรือข้อมูลของระดับรหัสผ่าน.	
30, 69	PRTPRFINT	ใช้คำสั่ง Print Profile Internals เพื่อพิมพ์ รายงานของข้อมูลภายในตามจำนวนของรายการที่ป้อน.	
31, 70	CHKOBJITG	ใช้คำสั่ง Check Object Integrity เพื่อพิจาราณา ว่าอ็อบเจ็กต์ที่ทำงานได้ (เช่น โปรแกรม) ถูกเปลี่ยนแปลงโดยไม่ได้ใช้คอมไพเลอร์. คำสั่งนี้สามารถช่วยคุณตรวจจับการนำโปรแกรมไวรัสเข้ามาในระบบคุณ หรือเพื่อเปลี่ยนโปรแกรมที่ใช้คำสั่งที่ไม่มีสิทธิ. หนังสือ *iSeries Security Reference* มีข้อมูลเพิ่มเติมของคำสั่ง CHKOBJITG.	

หมายเหตุ:

1. อ็อพชันมาจากเมนู SECBATCH.
2. ไฟล์นี้อยู่ในไลบรารี QUSRSYS.
3. xx เป็น journal entry type ยาว 2 ตัวอักษร. ตัวอย่างเช่น, แบบ (model) เอาต์พุตไฟล์ของ AE journal entry คือ QSYS/QASYAEJ4. คำอธิบายเรื่อง แบบเอาต์พุตไฟล์อยู่ในภาคผนวก F ของหนังสือ *iSeries Security Reference* .
4. เมนู SECBATCH มีอ็อพชันสำหรับประเภทของอ็อบเจ็กต์ที่มักจะเกี่ยวข้องกับ ผู้บริหารระบบความปลอดภัย. ตัวอย่างเช่น, ใช้อ็อพชัน 11 หรือ 50 เพื่อรันคำสั่ง PRTPUBAUT กับอ็อบเจ็กต์ *FILE. ใช้อ็อพชันทั่วไป (18 และ 57) เพื่อระบุประเภท ของอ็อบเจ็กต์.
5. เมนู SECBATCH มีอ็อพชันสำหรับประเภทของอ็อบเจ็กต์ที่มักจะเกี่ยวข้องกับ ผู้บริหารระบบความปลอดภัย. ตัวอย่างเช่น, ใช้อ็อพชัน 12 หรือ 51 เพื่อรันคำสั่ง PRTPVTAUT กับอ็อบเจ็กต์ *FILE. ใช้อ็อพชันทั่วไป (19 และ 58) เพื่อระบุประเภท ของอ็อบเจ็กต์.
6. xxxxxx ในชื่อของไฟล์คือประเภทของอ็อบเจ็กต์. ตัวอย่างเช่น, ไฟล์สำหรับอ็อบเจ็กต์โปรแกรมเรียกว่า QPBPGM สำหรับสิทธิพับลิก และเรียกว่า QPVPGM สำหรับสิทธิไพรเวต. ไฟล์นี้อยู่ในไลบรารี QUSRSYS.

   ในไฟล์จะมีสมาชิกของแต่ละไลบรารีที่คุณได้พิมพ์รายงานไปแล้ว. ชื่อของสมาชิกจะ เหมือนกับชื่อไลบรารี.

คำสั่งสำหรับการปรับแต่งค่าความปลอดภัยตามความต้องการ

ตารางที่ 9แสดงคำสั่งที่คุณสามารถใช้เพื่อปรับแต่งค่าความปลอดภัยของระบบ. คำสั่งเหล่านี้อยู่ในเมนู SECTOOLS.

ตารางที่ 9. คำสั่งสำหรับการปรับแต่งระบบตามความต้องการของคุณ

เมนูตัวเลือกที่[1]	ชื่อคำสั่ง	คำอธิบาย	ไฟล์ฐานข้อมูลที่ใช้
60	CFGSYSSEC	ใช้คำสั่ง Configure System Security เพื่อตั้ง ค่ากำหนดของระบบที่เกี่ยวข้องกับความปลอดภัยเป็นค่าที่แนะนำ. คำสั่งนี้ยังทำการจัดเตรียมการตรวจสอบความปลอดภัยในระบบของคุณ. "ค่าที่เซ็ตโดยคำสั่ง Configure System Security"อธิบายถึงสิ่งที่คำสั่งกระทำ. **หมายเหตุ:** เพื่อให้ได้ค่าของความปลอดภัยที่แนะนำให้ใช้ซึ่งจะถูกปรับตามความต้องการให้ใช้กับสถานการณ์ของคุณได้, ให้รัน iSeries Security Wizard หรือ iSeries Security Advisor แทนที่จะรันคำสั่งนี้. โปรดดูที่ บทที่ 2, "iSeries Security Wizard และ eServer Security Planner", ในหน้า 11 สำหรับข้อมูลของเครื่องมือเหล่านี้.	
61	RVKPUBAUT	ใช้คำสั่ง Revoke Public Authority เพื่อตั้ง ค่าสิทธิพับลิกเป็น *EXCLUDE ให้กับชุดคำสั่งที่อ่อนไหวต่อความปลอดภัย (security-sensitive command) ในระบบของคุณ. "ฟังก์ชันของคำสั่ง Revoke Public Authority" ในหน้า 43 แสดงรายการ ของสิ่งที่คำสั่ง RVKPUBAUT กระทำ.	

หมายเหตุ:

1. อ็อพชันมาจากเมนู SECTOOLS.

ค่าที่เซ็ตโดยคำสั่ง Configure System Security

ตารางที่ 10แสดงค่าของระบบที่ถูกกำหนดเมื่อคุณรันคำสั่ง CFGSYSSEC. คำสั่ง CFGSYSSEC รันโปรแกรมที่ชื่อ QSYS/QSECCFGS.

ตารางที่ 10. ค่าที่ถูกเซ็ตโดยคำสั่ง CFGSYSSEC

ชื่อของค่ากำหนดของระบบ	ค่าที่กำหนด	รายละเอียดของค่ากำหนดของระบบ
QALWOBJRST	*NONE	สามารถเรียกsystem state programsและโปรแกรมที่ รับสิทธิมา คืนมาดังเดิมได้
QAUTOCFG	0 (ไม่)	กำหนดค่าของอุปกรณ์ใหม่โดยอัตโนมัติ
QAUTOVRT	0	จำนวนของคำอธิบายอุปกรณ์เสมือนที่ระบบทำการสร้างให้โดยอัตโนมัติ เมื่อไม่มีอุปกรณ์เหลือไว้ให้ใช้งาน.
QDEVRCYACN	*DSCMSG (ตัดการติดต่อด้วยข้อความ)	การกระทำของระบบเมื่อการสื่อสารเริ่มต้นใหม่อีกครั้ง
QDSCJOBITV	120	ระยะเวลาก่อนที่ระบบจะกระทำกับงานที่ไม่สามารถ ติดต่อได้

ตารางที่ 10. ค่าที่ถูกเซ็ตโดยคำสั่ง CFGSYSSEC (ต่อ)

ชื่อของค่ากำหนดของระบบ	ค่าที่กำหนด	รายละเอียดของค่ากำหนดของระบบ
QDSPSGNINF	1 (ใช่)	ผู้ใช้เห็นหน้าจอของการ sign-on
QINACTITV	60	ระยะเวลาก่อนที่ระบบจะกระทำกับงานโต้ตอบที่ไม่ทำงาน
QINACTMSGQ	*ENDJOB	การกระทำที่ระบบกระทำกับงานที่ไม่ทำงาน (inactive)
QLMTDEVSSN	1 (ใช่)	ผู้ใช้ถูกจำกัดให้ sing-on ได้บนหนึ่งอุปกรณ์ในเวลาเดียวกัน
QLMTSECOFR	1 (ใช่)	ผู้ใช้ *ALLOBJ และ *SERVICE ถูกจำกัดให้ใช้ เฉพาะอุปกรณ์ที่กำหนด
QMAXSIGN	3	จำนวนครั้งที่อนุญาตให้กับการ sign-on ที่ ไม่สำเร็จต่อเนื่องกัน
QMAXSGNACN	3 (ทั้งคู่)	ระบบจะทำให้เวิร์กสเตชันหรือโปรไฟล์ผู้ใช้ใช้งานไม่ได้ เมื่อถึงค่าจำกัด QMAXSIGN.
QRMTSIGN	*FRCSIGNON	วิธีการที่ระบบจัดการกับ remote sign-on (pass-through หรือ TELNET).
QRMTSVRATR	0 (ปิด)	อนุญาตให้ระบบถูกวิเคราะห์จากระยะไกล.
QSECURITY [1 ในหน้า 42]	50	ระดับของความปลอดภัยที่บังคับใช้
QVFYOBJRST	3 (ตรวจสอบ signatures ในขณะเรียกคืน)	ตรวจสอบอ็อบเจ็กต์ในขณะเรียกคืน
QPWDEXPITV	60	ระยะเวลาที่ผู้ใช้ของระบบจะต้องเปลี่ยนรหัสผ่าน.
QPWDMINLEN	6	ความยาวที่สั้นที่สุดสำหรับรหัสผ่าน
QPWDMAXLEN	8	ความยาวที่ยาวที่สุดสำหรับรหัสผ่าน
QPWDPOSDIF	1 (ใช่)	ทุกตำแหน่งในรหัสผ่านใหม่ต้องแตกต่างจากตำแหน่ง เดียวกันในรหัสผ่านครั้งก่อน
QPWDLMTCHR	ดูหมายเหตุ 2 ในหน้า 42	อักขระที่ไม่อนุญาตให้ใช้ในรหัสผ่าน
QPWDLMTAJC	1 (ใช่)	ตัวเลขที่อยู่ติดกันถูกห้ามใช้ในรหัสผ่าน
QPWDLMTREP	2 (ไม่สามารถใช้ซ้ำต่อเนื่องกัน)	อักขระซ้ำกันที่ถูกห้ามใช้ในรหัสผ่าน
QPWDRQDDGT	1 (ใช่)	รหัสผ่านต้องมีตัวเลขอย่างน้อยหนึ่งตัว
QPWDRQDDIF	1 (32 รหัสผ่านที่ไม่ซ้ำกัน)	จำนวนของรหัสผ่านที่ไม่ซ้ำกันก่อนที่รหัสผ่านจะกลับมาซ้ำกันได้
QPWDVLDPGM	*NONE	โปรแกรมทางออกของผู้ใช้ที่ระบบเรียกเพื่อใช้ตรวจสอบรหัสผ่าน

ตารางที่ 10. ค่าที่ถูกเซ็ตโดยคำสั่ง CFGSYSSEC (ต่อ)

ชื่อของค่ากำหนดของระบบ	ค่าที่กำหนด	รายละเอียดของค่ากำหนดของระบบ
หมายเหตุ: 1. ถ้าคุณกำลังทำงานด้วยค่า QSECURITY ที่ 40 หรือน้อยกว่า, ให้แน่ใจว่าได้อ่านทบทวนข้อมูลในบทที่ 2 ของหนังสือ *iSeries Security Reference* ก่อนที่คุณจะเปลี่ยนไปยังระดับความปลอดภัยที่สูงขึ้น. 2. อักขระที่ห้ามใช้ถูกเก็บในข้อความ ID CPXB302 ในไฟล์ข้อความ QSYS/QCPFMSG. ซึ่งมีค่าเป็น AEIOU@$#. คุณสามารถใช้คำสั่ง Change Message Description (CHGMSGD) เพื่อเปลี่ยนอักขระที่ห้ามใช้. ค่ากำหนดของระบบ QPWDLMTCHR ไม่มีการบังคับเมื่อระดับของรหัสผ่านอยู่ที่ 2 หรือ 3.		

คำสั่ง CFGSYSSEC ยังตั้งค่ารหัสผ่านเป็น *NONE สำหรับโปรไฟล์ผู้ใช้ที่ IBM จัดหาให้:

QSYSOPR

QPGMR

QUSER

QSRV

QSRVBAS

ในท้ายที่สุด, คำสั่ง CFGSYSSEC จะจัดเตรียมการตรวจสอบความปลอดภัยโดยใช้คำสั่ง Change Security Auditing (CHGSECAUD). คำสั่ง CFGSYSSEC จะเปิดการตรวจสอบการกระทำ และการตรวจสอบอ็อบเจ็กต์, และระบุชุดของการกระทำเพื่อตรวจสอบบนคำสั่ง CHGSECAUD.

การปรับค่าโปรแกรมตามความต้องการ

ถ้าค่าติดตั้งเหล่านี้ บางค่าไม่เหมาะสมกับการติดตั้งของคุณ, คุณสามารถสร้างโปรแกรมในเวอร์ชันของคุณที่จะประมวลคำสั่ง. โดยทำดังนี้:

__ ขั้นตอนที่ 1. ใช้คำสั่ง Retrieve CL Source (RTVCLSRC) เพื่อก็อปปี้ต้นฉบับของโปรแกรมที่ทำงานเมื่อคุณใช้คำสั่ง CFGSYSSEC. โปรแกรมที่เรียกออกมาคือ QSYS/QSECCFGS. เมื่อคุณเรียกโปรแกรมนั้นออกมาแล้ว, ให้เปลี่ยนชื่อเป็น *ชื่ออื่น*.

__ ขั้นตอนที่ 2. แก้ไขโปรแกรมตามที่คุณต้องการ. คอมไพล์โปรแกรมนั้น. เมื่อคุณคอมไพล์, ต้องแน่ใจว่าคุณ *ไม่ได้* แทนที่โปรแกรม QSYS/QSECCFGS ที่ IBM จัดหาให้. โปรแกรมของคุณต้องมีชื่อเป็นชื่ออื่น.

__ ขั้นตอนที่ 3. ใช้คำสั่ง Change Command (CHGCMD) เพื่อเปลี่ยนโปรแกรมที่ประมวลพารามิเตอร์ คำสั่ง (PGM) สำหรับคำสั่ง CFGSYSSEC. ตั้งค่า PGM เป็นชื่อโปรแกรมของคุณ. ตัวอย่างเช่น, , ถ้าคุณสร้างโปรแกรมไว้ในไลบรารี QGPL ที่เรียกว่า MYSECCFG, คุณจะต้องพิมพ์ดังนี้:

```
CHGCMD CMD(QSYS/CFGSYSSEC) PGM(QGPL/MYSECCFG)
```

หมายเหตุ: ถ้าคุณเปลี่ยนแปลงโปรแกรม QSYS/QSECCFGS, IBM ไม่สามารถรับรอง หรือให้ความเชื่อถือได้, ความสามารถด้านบริการ,

ประสิทธิภาพหรือการทำงานของโปรแกรม. การรับประกันโดยนัยต่อสินค้าและความเหมาะสมสำหรับวัตถุประสงค์เฉพาะ จะไม่สามารถ นำมากล่าวอ้างได้.

ฟังก์ชันของคำสั่ง Revoke Public Authority

คุณสามารถใช้คำสั่ง Revoke Public Authority (RVKPUBAUT) เพื่อกำหนดสิทธิพับลิก สำหรับกลุ่มของคำสั่งและโปรแกรมเป็น *EXCLUDE. คำสั่ง RVKPUBAUT รันโปรแกรมที่ชื่อ QSYS/QSECRVKP. ตามที่มาพร้อมกับเครื่อง, คำสั่ง QSECRVKP เพิกถอนสิทธิพับลิก (โดยการกำหนดสิทธิพับลิกเป็น *EXCLUDE) ของคำสั่งที่แสดงใน ตารางที่ 11และ application programming interfaces (APIs) ที่แสดงใน ตารางที่ 12. ตอนที่ระบบของคุณมาถึง, คำสั่งและ APIs เหล่านี้มีสิทธิพับลิกที่กำหนดเป็น *USE.

คำสั่งที่แสดงใน ตารางที่ 11และ APIs ที่แสดงใน ตารางที่ 12ทั้งหมดทำงานในระบบของคุณ ซึ่งอาจทำให้เกิดความเสียหาย. ในฐานะผู้บริหารความปลอดภัย, คุณจะต้องกำหนดสิทธิให้เป็นการเฉพาะสำหรับผู้ใช้ เพื่อใช้งานคำสั่งและโปรแกรม เหล่านี้มากกว่าที่จะให้ผู้ใช้ทุกคนในระบบสามารถใช้งานได้.

เมื่อคุณรันคำสั่ง RVKPUBAUT, ให้คุณระบุไลบรารีที่มีคำสั่งนี้. ซึ่งมีค่า ดีฟอลต์คือไลบรารี QSYS. ถ้าคุณมีมากกว่าหนึ่งภาษาในระบบของคุณ, คุณจะต้องรัน คำสั่งสำหรับแต่ละไลบรารี QSYSxxx.

ตารางที่ 11. คำสั่งที่สิทธิพับลิกของมันถูกเซ็ตโดยคำสั่ง RVKPUBAUT

ADDAJE	CHGJOBQE	RMVCMNE
ADDCFGLE	CHGPJE	RMVJOBQE
ADDCMNE	CHGRTGE	RMVPJE
ADDJOBQE	CHGSBSD	RMVRTGE
ADDPJE	CHGWSE	RMVWSE
ADDRTGE	CPYCFGL	RSTLIB
ADDWSE	CRTCFGL	RSTOBJ
CHGAJE	CRTCTLAPPC	RSTS36F
CHGCFGL	CRTDEVAPPC	RSTS36FLR
CHGCFGLE	CRTSBSD	RSTS36LIBM
CHGCMNE	ENDRMTSPT	STRRMTSPT
CHGCTLAPPC	RMVAJE	STRSBS
CHGDEVAPPC	RMVCFGLE	WRKCFGL

APIs ทั้งหมดใน ตารางที่ 12อยู่ในไลบรารี QSYS:

ตารางที่ 12. โปรแกรมที่มีสิทธิพับลิกของมันที่ถูกเซ็ตโดยคำสั่ง RVKPUBAUT

QTIENDSUP
QTISTRSUP
QWTCTLTR
QWTSETTR
QY2FTML

เมื่อคุณรันคำสั่ง RVKPUBAUT , ระบบทำการเซ็ตค่าสิทธิพับลิกสำหรับไดเร็กทอรีรากให้เป็น *USE (ยกเว้นถ้าว่ามันเป็น *USE อยู่แล้วหรือน้อยกว่านั้น).

การปรับโปรแกรมตามความต้องการ

ถ้าค่าติดตั้งเหล่านี้ บางค่าไม่เหมาะสมกับการติดตั้งของคุณ, คุณสามารถสร้างโปรแกรมในเวอร์ชันของคุณที่จะประมวลคำสั่ง. โดยทำดังนี้:

__ ขั้นตอนที่ 1. ใช้คำสั่ง Retrieve CL Source (RTVCLSRC) เพื่อก็อปปีต้นฉบับของโปรแกรมที่ทำงานเมื่อคุณใช้คำสั่ง RVKPUBAUT. โปรแกรมที่เรียกออกมาคือ QSYS/QSECRVKP. เมื่อคุณเรียกโปรแกรมนั้นออกมาแล้ว, ให้เปลี่ยนชื่อเป็น *ชื่ออื่น*.

__ ขั้นตอนที่ 2. แก้ไขโปรแกรมตามที่คุณต้องการ. คอมไพล์โปรแกรมนั้น. เมื่อคุณคอมไพล์, ต้องแน่ใจว่าคุณ *ไม่ได้* แทนที่โปรแกรม QSYS/QSECRVKP ที่ IBM จัดหาให้. โปรแกรมของคุณต้องมีชื่อเป็นชื่ออื่น.

__ ขั้นตอนที่ 3. ใช้คำสั่ง Change Command (CHGCMD) เพื่อเปลี่ยนโปรแกรมที่ประมวลพารามิเตอร์ คำสั่ง (PGM) สำหรับคำสั่ง RVKPUBAUT. ตั้งค่า PGM เป็นชื่อโปรแกรมของคุณ. ตัวอย่างเช่น, , ถ้าคุณสร้างโปรแกรมไว้ในไลบรารี QGPL ที่เรียกว่า MYRVKPGM, คุณจะต้องพิมพ์ดังนี้:

```
CHGCMD CMD(QSYS/RVKPUBAUT) PGM(QGPL/MYRVKPGM)
```

หมายเหตุ: ถ้าคุณเปลี่ยนแปลงโปรแกรม QSYS/QSECRVKP, IBM ไม่สามารถรับรอง หรือให้ความเชื่อถือได้, ความสามารถด้านบริการ, ประสิทธิภาพหรือการทำงานของโปรแกรม. การรับประกันโดยนัยต่อสินค้าและความเหมาะสมสำหรับวัตถุประสงค์เฉพาะ จะไม่สามารถ นำมากล่าวอ้างได้.

ส่วนที่ 2. ความปลอดภัยระดับสูงของ iSeries

บทที่ 5. ปกป้องข้อมูลทรัพย์สินด้วยสิทธิอ็อบเจ็กต์

ความท้าทายของคุณในฐานะของผู้บริหารความปลอดภัย คือ การปกป้องสินทรัพย์ข้อมูลในองค์กรของคุณโดยไม่ทำความรบกวนต่อผู้ใช้ในระบบของคุณ. คุณต้องทำให้มั่นใจว่า ผู้ใช้มีสิทธิ เพียงพอที่จะทำงานของเขาโดยไม่ต้องให้สิทธิในการเลือกดู (browse) ตลอดทั้งระบบ และทำการเปลี่ยนแปลงที่ไม่ได้อนุญาต.

ข้อแนะนำด้านความปลอดภัย

การให้สิทธิที่เข้มงวดเกินไปสามารถส่งผลย้อนกลับได้. บางครั้งผู้ใช้อาจมี ปฏิกิริยาต่อการให้สิทธิที่เข้มงวดเกินไป โดยการแบ่งใช้รหัสผ่านร่วมกัน.

ระบบปฏิบัติการ OS/400 มีความปลอดภัยของอ็อบเจ็กต์แบบรวมกัน. ผู้ใช้ ต้องใช้อินเตอร์เฟสที่ระบบมีให้ในการเข้าถึงอ็อบเจ็กต์. ตัวอย่างเช่น, ถ้าคุณต้องการเข้าถึงไฟล์ฐานข้อมูล, คุณต้องใช้คำสั่งหรือโปรแกรมที่ออกแบบให้ เข้าถึงไฟล์ฐานข้อมูล. คุณไม่สามารถใช้คำสั่งที่ออกแบบให้ใช้สำหรับเข้าถึง message queue หรือบันทึกการใช้งานได้.

เมื่อใดที่คุณใช้อินเตอร์เฟสของระบบเข้าถึงอ็อบเจ็กต์, ระบบจะตรวจสอบว่าคุณ มีสิทธิในอ็อบเจ็กต์ที่ต้องการโดย อินเตอร์เฟสนั้น. สิทธิอ็อบเจ็กต์เป็นเครื่องมือ ที่มีประสิทธิภาพและยืดหยุ่นต่อการป้องกันสินทรัพย์ในระบบของคุณ. ความท้าทายใน ฐานะผู้บริหารความปลอดภัยคือการจัดเตรียมโครงร่างความปลอดภัยของอ็อบเจ็กต์ที่มีประสิทธิภาพที่คุณสามารถจัดการและดูแลได้.

การบังคับใช้สิทธิอ็อบเจ็กต์

เมื่อใดก็ตามที่คุณพยายามที่จะเข้าไปใช้อ็อบเจ็กต์, ระบบปฏิบัติการจะตรวจสอบสิทธิของคุณที่มีต่ออ็อบเจ็กต์นั้น. อย่างไรก็ตาม, หากระดับความปลอดภัยในระบบ ของคุณ (ค่ากำหนดของระบบ QSECURITY) ถูกกำหนดเป็น 10 หรือ 20, ผู้ใช้ทุกคนจะมี สิทธิในการเข้าถึงทุกอ็อบเจ็กต์โดยอัตโนมัติ เนื่องจากทุกโปรไฟล์ผู้ใช้มีสิทธิพิเศษเป็น *ALLOBJ.

ข้อแนะนำเกี่ยวกับสิทธิอ็อบเจ็กต์: ถ้าคุณไม่แน่ใจว่าคุณกำลังใช้ความปลอดภัยของอ็อบเจ็กต์หรือไม่, ให้ตรวจสอบค่ากำหนดของระบบที่เป็น QSECURITY (ระดับความปลอดภัย). หาก QSECURITY เป็น 10 หรือ 20, คุณกำลัง ไม่ ใช้ความปลอดภัยของอ็อบเจ็กต์.

คุณต้องวางแผนและเตรียมตัวก่อนที่คุณจะเปลี่ยนระดับความปลอดภัยเป็น 30 หรือสูงกว่า. มิฉะนั้น, ผู้ใช้ของคุณอาจไม่สามารถเข้าถึงข้อมูลที่พวกเขาต้องการได้.

หัวข้อของ **การรักษาความปลอดภัยให้กับและการวางแผนระดับต้น** ใน Information Center ได้รวบรวมวิธีการสำหรับการวิเคราะห์แอ็พพลิเคชันของคุณและตัดสินใจว่าจะทำการตั้งค่าความ

ปลอดภัยของอ็อบเจ็กต์อย่างไร. ถ้าคุณยังไม่ได้ใช้ความปลอดภัย ของอ็อบเจ็กต์ หรือโครงสร้างความปลอดภัยของอ็อบเจ็กต์ของคุณนั้นล้าสมัยและซ้อนทับกัน, ให้อ่านหัวข้อนี้ เพื่อช่วยให้คุณเริ่มต้น.

เมนูเกี่ยวกับความปลอดภัย

เซิร์ฟเวอร์ iSeries ในตอนแรกได้ถูกออกแบบมาให้เป็นผลิตภัณฑ์ที่ต่อเนื่องมาจาก S/36 และ S/38. การติดตั้งเซิร์ฟเวอร์ iSeries จำนวนมาก, ที่ครั้งหนึ่งเคยเป็น , การติดตั้ง S/36 หรือ S/38 . เพื่อควบคุมสิ่งที่ผู้ใช้สามารถทำได้, ผู้บริหารความปลอดภัยของระบบรุ่นก่อนหน้านี้มักจะใช้เทคนิคที่ถูกอ้างถึงในชื่อของ **เมนูความปลอดภัย** หรือ **เมนูแอ็คเซสคอนโทรล**.

เมนูแอ็คเซสคอนโทรลหมายถึง เมื่อผู้ใช้ทำการ sign on, ผู้ใช้จะมองเห็นเมนูนี้ . ผู้ใช้สามารถทำงานได้เฉพาะฟังก์ชันที่อยู่บนเมนู. ผู้ใช้ไม่สามารถไปยังบรรทัด คำสั่งของระบบเพื่อเรียกใช้ฟังก์ชันใดๆ ที่ไม่ได้อยู่บนเมนู. ในทางทฤษฎี, ผู้บริหารความปลอดภัยไม่ต้องกังวลเกี่ยวกับสิทธิในอ็อบเจ็กต์ เพราะเมนูและโปรแกรม ควบคุมสิ่งที่ผู้ใช้สามารถทำได้.

เซิร์ฟเวอร์ iSeries มีตัวเลือกเกี่ยวกับโปรไฟล์ผู้ใช้มากมายให้เลือกใช้กับเมนูแอ็คเซสคอนโทรล, คุณสามารถใช้:

- พารามิเตอร์ **Initial menu** (INLMNU) เพื่อควบคุมว่า เมนูใดที่ผู้ใช้จะพบหลังจากที่ผู้ใช้ sign on.
- พารามิเตอร์ **Initial program** (INLPGM) เพื่อรัน setup program ก่อนที่ผู้ใช้จะเห็นเมนู. หรือ, คุณสามารถใช้พารามิเตอร์ INLPGM เพื่อควบคุมให้ผู้ใช้รันโปรแกรมได้เพียงโปรแกรมเดียว.
- พารามิเตอร์ **Limit capabilities** (LMTCPB) เพื่อควบคุม ผู้ใช้ไปยังชุดคำสั่งที่จำกัดไว้. และยังป้องกันไม่ให้ผู้ใช้ระบุ initial program อื่นหรือเมนูอื่นบนหน้าจอ Sign On. (พารามิเตอร์ LMTCPB จำกัดเพียงคำสั่งที่ ถูกป้อนจากบรรทัดรับคำสั่งเท่านั้น.)

ข้อจำกัดของเมนูแอ็คเซสคอนโทรล

คอมพิวเตอร์และผู้ใช้คอมพิวเตอร์มีการเปลี่ยนแปลงอย่างมากในเวลาไม่กี่ปีที่ผ่านมา. เครื่องมือหลายอย่าง, เช่น โปรแกรมสอบถาม (query) และสเปรดชีต, ทำให้ผู้ใช้สามารถ ทำโปรแกรมมิงด้วยตัวเอง เพื่อลดภาระของฝ่ายระบบสารสนเทศ. เครื่องมือบางอย่าง, เช่น SQL หรือ ODBC มีความสามารถในการดูข้อมูลและ เปลี่ยนแปลงข้อมูล. การทำให้เครื่องมือเหล่านี้สามารถทำงานภายใต้โครงสร้างของเมนู เป็นเรื่องที่ยากมาก.

เวิร์กสเตชันที่ทำหน้าที่เฉพาะ ("จอภาพสีเขียว") ถูกแทนที่อย่างรวดเร็ว ด้วยเครื่องคอมพิวเตอร์ส่วนบุคคล และเครือข่ายระหว่างคอมพิวเตอร์ไปยังคอมพิวเตอร์. ถ้าระบบของคุณเข้าร่วมอยู่ในเครือข่าย, ผู้ใช้อาจเข้าสู่ระบบของคุณ โดยไม่จำเป็น ต้องมองเห็นจอภาพ sign-on หรือเมนู.

ในฐานะผู้บริหารความปลอดภัยผู้ซึ่งพยายามควบคุมการเข้าถึงเมนู, คุณมีปัญหา พื้นฐานสองข้อ:

- ถ้าคุณประสบความสำเร็จในการจำกัดผู้ใช้ไปยังเมนู, ผู้ใช้ของคุณอาจจะไม่พอใจ เนื่องจากขีดความสามารถของเขาในการใช้เครื่องมือสมัยใหม่ถูกจำกัด.
- ถ้าคุณไม่ประสบความสำเร็จ, คุณอาจทำให้ข้อมูล (ที่สำคัญมาก, และเป็นความลับ) ที่การควบคุมการเข้าถึงเมนูทำหน้าที่ป้องกันอยู่เป็นอันตรายได้. เมื่อระบบของคุณ มีส่วนร่วมอยู่ในเครือ

ข่าย, ความสามารถของคุณในการบังคับใช้การควบคุมการเข้าถึงเมนูจะลดลง. ตัวอย่างเช่น, พารามิเตอร์ LMTCPB จะควบคุมเฉพาะคำสั่งที่ถูกป้อนจากบรรทัด รับคำสั่งในเซสชันแบบโต้ตอบเท่านั้น. พารามิเตอร์ LMTCPB ไม่มีผลต่อการร้องขอจาก เซสชันการสื่อสาร เช่น การถ่ายโอนไฟล์จาก PC, FTP หรือคำสั่งรีโมต เป็นต้น.

การเพิ่มประสิทธิภาพให้กับเมนูแอ็คเซสคอนโทรลด้วยความปลอดภัยของอ็อบเจ็กต์

ด้วยตัวเลือกใหม่ๆ มากมายที่เพิ่มขึ้นเพื่อช่วยในการเชื่อมต่อเข้ากับระบบ, รูปแบบของการรักษาความปลอดภัยให้กับเซิร์ฟเวอร์ iSeries ที่จะคงอยู่ต่อไปได้สำหรับในอนาคตนั้นไม่สามารถขึ้นอยู่กับเมนูแอ็คเซสคอนโทรลเพียงอย่างเดียว. หัวข้อนี้จะให้คำแนะนำสำหรับการเปลี่ยนแปลงไปยังสภาพ แวดล้อมความปลอดภัยของอ็อบเจ็กต์ ซึ่งทำให้การควบคุมการเข้าถึงเมนูของคุณสมบูรณ์ขึ้น.

หัวข้อ *การรักษาความปลอดภัยให้กับระบบและการวางแผนเบื้องต้น* ใน Information Center อธิบายถึงเทคนิคในการวิเคราะห์สิทธิที่ผู้ใช้จะต้องมีในอ็อบเจ็กต์เพื่อ รันแอ็พพลิเคชันของคุณในปัจจุบัน. จากนั้นคุณกำหนดผู้ใช้ไปยังกลุ่ม และให้ สิทธิที่เหมาะสมกับกลุ่ม. วิธีการนี้มีเหตุมีผลและเหมาะสม. อย่างไรก็ตาม, ถ้าระบบของคุณใช้งานมานานหลายปีและมีแอ็พพลิเคชันหลายตัว, ภาระในการวิเคราะห์ แอ็พพลิเคชันและจัดเตรียมสิทธิในอ็อบเจ็กต์ ดูเหมือนจะมากจนเกินไป.

ข้อแนะนำเกี่ยวกับสิทธิอ็อบเจ็กต์: เมนูปัจจุบันของคุณที่รวมเข้ากับโปรแกรมที่มีการรับสิทธิของเจ้าของโปรแกรมมาใช้อาจจะมีการอนุญาตให้มีการส่งผ่านที่นอกเหนือไปจากเมนูแอ็คเซสคอนโทรล. ต้องมั่นใจว่าได้ป้องกันทั้งโปรแกรมที่รับสิทธิมา และโปรไฟล์ผู้ใช้ที่เป็นเจ้าของโปรแกรม.

คุณอาจสามารถใช้เมนูปัจจุบันของคุณช่วยคุณเตรียมสภาพแวดล้อมที่เปลี่ยนไป ระหว่างที่คุณค่อยๆ วิเคราะห์แอ็พพลิเคชันและอ็อบเจ็กต์ของคุณ. ต่อไปนี้เป็นตัวอย่างที่ใช้เมนู Order Entry (OEMENU) และไฟล์และโปรแกรมที่เชื่อมโยงกัน.

ตัวอย่าง: การตั้งค่าสภาวะแวดล้อมของการส่งผ่าน

ตัวอย่างนี้เริ่มต้นด้วยข้อสมมติฐานและความต้องการดังต่อไปนี้:

- ไฟล์ทั้งหมดอยู่ในไลบรารี ORDERLIB.
- คุณไม่ทราบชื่อของทุกไฟล์. คุณยังไม่ทราบถึงสิทธิที่เมนูอ็อพชันต้องการในไฟล์ต่างๆ .
- เมนูและทุกโปรแกรมที่เมนูเรียกใช้อยู่ในไลบรารี ORDERPGM.
- คุณต้องการให้ทุกคนที่สามารถ sign on เข้ามาในระบบของคุณ สามารถดูข้อมูล ทุกอย่างในทุกๆ ไฟล์รายการสั่งซื้อ (order file), ไฟล์ลูกค้า, และไฟล์รายการสินค้า (ด้วยโปรแกรมดูข้อมูลหรือสเปรดชีต เป็นต้น).
- เฉพาะผู้ใช้ที่เมนู sign-on ในปัจจุบันเป็น OEMENU เท่านั้นที่สามารถ เปลี่ยนแปลงไฟล์. และ, จะต้องใช้โปรแกรมบนเมนูเพื่อทำการเปลี่ยนแปลง.
- ผู้ใช้ระบบที่ไม่ใช่ผู้บริหารความปลอดภัยไม่มีสิทธิพิเศษ *ALLOBJ หรือ *SECADM .

ดำเนินการตามขั้นตอนต่อไปนี้เพื่อเปลี่ยนแปลงสภาวะแวดล้อมของเมนูแอ็คเซสคอนโทรลเพื่อให้เหมาะสมกับความต้องการของเคียวรี่:

__ ขั้นตอนที่ 1. สร้างรายการของผู้ใช้ที่มีเมนูเริ่มต้นเป็น OEMENU.

คุณสามารถใช้คำสั่ง Print User Profile (PRTUSRPRF *ENVINFO) เพื่อแสดงรายการ สภาพแวดล้อมของโปรไฟล์ผู้ใช้ในระบบของคุณ. ในรายงานจะมีเมนูเริ่มต้น, โปรแกรม เริ่มต้น และไลบรารีปัจจุบัน. รูปที่ 7 ในหน้า 67 แสดงตัวอย่างของรายงาน.

__ ขั้นตอนที่ 2. ต้องแน่ใจว่าอ็อบเจ็กต์ OEMENU (ซึ่งอาจเป็นอ็อบเจ็กต์ *PGM หรืออ็อบเจ็กต์ *MENU) เป็นของโปรไฟล์ผู้ใช้ที่ไม่ใช้ในการ sign on. โปรไฟล์ผู้ใช้ต้องไม่สามารถ ใช้ได้หรือมีรหัสผ่านเป็น *NONE. ตัวอย่างเช่น, สมมติว่า OEOWNER เป็นเจ้าของ อ็อบเจ็กต์ของโปรแกรม OEMENU.

__ ขั้นตอนที่ 3. ต้องแน่ใจว่าโปรไฟล์ผู้ใช้ที่เป็นเจ้าของอ็อบเจ็กต์ของโปรแกรม OEMENU ไม่ใช่โปรไฟล์กลุ่ม. คุณสามารถใช้คำสั่งต่อไปนี้:

```
DSPUSRPRF USRPRF(OEOWNER) TYPE(*GRPMBR)
```

__ ขั้นตอนที่ 4. เปลี่ยนแปลงโปรแกรม OEMENU ให้รับสิทธิของโปรไฟล์ผู้ใช้ OEOWNER. (ใช้คำสั่ง CHGPGM เพื่อเปลี่ยนพารามิเตอร์ USRPRF เป็น *OWNER.)

หมายเหตุ: อ็อบเจ็กต์ *MENU ไม่สามารถรับสิทธิได้. ถ้า OEMENU เป็นอ็อบเจ็กต์ *MENU, คุณสามารถปรับตัวอย่างนี้โดยทำตามวิธีใดวิธีหนึ่งต่อไปนี้:

- สร้างโปรแกรมเพื่อแสดงเมนู.
- ใช้สิทธิที่รับมากับโปรแกรมที่ทำงานเมื่อผู้ใช้เลือกอ็อพชันจากเมนู OEMENU.

__ ขั้นตอนที่ 5. ตั้งค่าสิทธิพับลิกให้กับทุกไฟล์ใน ORDERLIB เป็น *USE โดยการพิมพ์คำสั่งสองคำสั่งต่อไปนี้:

```
RVKOBJAUT OBJ(ORDERLIB/*ALL) OBJTYPE(*FILE) USER(*PUBLIC)
     AUT(*ALL)
GRTOBJAUT OBJ(ORDERLIB/*ALL) OBJTYPE(*FILE) USER(*PUBLIC)
     AUT(*USE)
```

โปรดจำไว้ว่าถ้าคุณเลือกสิทธิ *USE, ผู้ใช้สามารถก็อปปี้ไฟล์โดยใช้การโอนถ่ายไฟล์จาก PC หรือ FTP.

__ ขั้นตอนที่ 6. ให้โปรไฟล์ที่เป็นเจ้าของเมนูโปรแกรมมีสิทธิ *ALL ไปยังไฟล์โดยการพิมพ์ดังนี้:

```
GRTOBJAUT OBJ(ORDERLIB/*ALL) OBJTYPE(*FILE) USER(OEOWNER)
     AUT(*ALL)
```

สำหรับแอ็พพลิเคชันส่วนใหญ่, สิทธิ *CHANGE ในไฟล์นั้น เพียงพอแล้ว. อย่างไรก็ตาม, แอ็พพลิเคชันของคุณอาจทำฟังก์ชัน เช่น การลบ สมาชิกฟิสิคัลไฟล์, ที่ต้องการอำนาจมากกว่า *CHANGE. ในที่สุด, คุณควรจะวิเคราะห์ แอ็พพลิเคชันของคุณ และให้เฉพาะสิทธิที่จำเป็นสำหรับแอ็พพลิเคชันเท่านั้น. อย่างไรก็ตาม, ในช่วงระหว่างการเปลี่ยนแปลง, โดยการรับสิทธิ *ALL, คุณควรหลีกเลี่ยงความล้มเหลวของแอ็พพลิเคชันที่อาจมีสาเหตุจากสิทธิที่ไม่พอเพียง.

__ ขั้นตอนที่ 7. จำกัดสิทธิในโปรแกรมที่อยู่ในไลบรารี order โดยพิมพ์ดังนี้:

```
GRTOBJAUT OBJ(ORDERPGM/*ALL) OBJTYPE(*PGM) USER(*PUBLIC)
     AUT(*EXCLUDE)
```

__ ขั้นตอนที่ 8. ให้สิทธิโปรไฟล์ OEOWNER กับโปรแกรมในไลบรารีนั้น โดยพิมพ์ดังนี้:

```
GRTOBJAUT OBJ(ORDERPGM/*ALL) OBJTYPE(*PGM) USER(OEOWNER)
     AUT(*USE)
```

__ ขั้นตอนที่ 9. ให้สิทธิแก่ผู้ใช้ที่ระบุในขั้นตอนที่ 1 ในโปรแกรมเมนู โดยพิมพ์ดังนี้สำหรับผู้ใช้แต่ละคน:

```
GRTOBJAUT OBJ(ORDERPGM/OEMENU) OBJTYPE(*PGM)
     USER(user-profile-name) AUT(*USE)
```

เมื่อคุณได้ทำตามขั้นตอนเหล่านี้แล้ว, ผู้ใช้ในระบบทุกคนที่ไม่ได้แยกออก อย่างชัดเจนจะสามารถเข้าถึง (แต่ไม่สามารถเปลี่ยนแปลง) ไฟล์ในไลบรารี ORDERLIB ได้. ผู้ใช้ที่มีสิทธิในโปรแกรม OEMENU จะสามารถใช้โปรแกรมที่อยู่ในเมนูเพื่ออัพเดต ไฟล์ในไลบรารี ORDERLIB ได้. มีแต่ผู้ใช้ที่มีสิทธิในโปรแกรม OEMENU เท่านั้น ที่จะสามารถเปลี่ยนแปลงไฟล์ ในไลบรารีได้. การผสมผสานความปลอดภัยของอ็อบเจ็กต์ และการควบคุมการเข้าถึงเมนู ป้องกันไฟล์เหล่านั้นไว้.

เมื่อคุณทำขั้นตอนอย่างเดียวกันกับทุกๆ ไลบรารีที่มีข้อมูลของผู้ใช้, คุณได้สร้างโครงร่างอย่างง่ายในการควบคุมการอัพเดตฐานข้อมูล. วิธีนี้ป้องกัน ผู้ใช้ระบบไม่ให้อัพเดตไฟล์ฐานข้อมูล ยกเว้นเมื่อเขาใช้เมนูและโปรแกรมที่ได้รับอนุญาต. ในเวลาเดียวกัน, คุณได้ทำให้ไฟล์ฐานข้อมูลพร้อมสำหรับการดู, การวิเคราะห์ และการก็อปปี โดยผู้ใช้ด้วยเครื่องมือช่วยการตัดสินใจ (decision-support tools) หรือด้วยการ เชื่อมโยงจากระบบอื่น หรือจากเครื่องพีซี.

ข้อแนะนำเกี่ยวกับสิทธิอ็อบเจ็กต์: เมื่อระบบของคุณเข้าไปมีส่วนร่วมในเน็ตเวิร์ก, สิทธิที่เป็น *USE อาจจะให้สิทธิในการใช้งานมากกว่าที่คุณคาดคิดไว้. ตัวอย่างเช่น, ด้วย FTP, คุณสามารถก็อปปีไฟล์ไปยังระบบอื่น (รวมทั้งพีซี) หากคุณ มีสิทธิ *USE ในไฟล์นั้น.

การใช้การรักษาความปลอดภัยของไลบรารีในการเติมเต็มเมนูความปลอดภัย

เมื่อเข้าถึงอ็อบเจ็กต์ในไลบรารี, คุณต้องมีสิทธิในอ็อบเจ็กต์และในไลบรารี. ปฏิบัติการส่วนใหญ่ต้องการทั้งสิทธิ *EXECUTE หรือ *USE ในไลบรารี.

ขึ้นกับสถานะการณ์ของคุณ, คุณอาจสามารถใช้สิทธิในไลบรารีเป็นเครื่องมืออย่างง่าย เพื่อทำให้อ็อบเจ็กต์ปลอดภัย. ตัวอย่าง, สมมุติให้ใช้ตัวอย่างเป็นเมนู Order-Entry, ทุกคนที่มีสิทธิในเมนู Order Entry จะสามารถใช้ทุกโปรแกรมในไลบรารี. คุณสามารถ กำหนดสิทธิในไลบรารี ORDERPGM เป็น *EXCLUDE, แทนที่จะทำให้แต่ละโปรแกรมปลอดภัย. จากนั้นคุณสามารถให้สิทธิ *USE ในไลบรารีแก่โปรไฟล์ผู้ใช้เฉพาะ, ซึ่งจะอนุญาต ให้ใช้โปรแกรมในไลบรารีได้. (สมมุติว่าสิทธิพับลิกในโปรแกรมเป็น *USE หรือมากกว่า.)

สิทธิไลบรารีเป็นวิธีที่ง่ายและมีประสิทธิภาพสำหรับการบริหารสิทธิอ็อบเจ็กต์. อย่างไรก็ตาม, คุณต้องมั่นใจว่าคุณคุ้นเคยกับสิ่งที่อยู่ในไลบรารีที่คุณจะทำให้ปลอดภัย เพื่อคุณจะได้ไม่ทำให้เกิดการเข้าถึงยังอ็อบเจ็กต์โดยไม่ได้ตั้งใจ.

การปรับแต่งค่าของความเป็นเจ้าของอ็อบเจ็กต์

ความเป็นเจ้าของของอ็อบเจ็กต์ในระบบของคุณ เป็นส่วนที่สำคัญของโครงร่าง สิทธิอ็อบเจ็กต์ (object authority scheme) ของคุณ. โดยดีฟอลต์, เจ้าของของ อ็อบเจ็กต์จะมีสิทธิที่ในอ็อบเจ็กต์ เป็น *ALL. บทที่ 5 ในหนังสือ *iSeries Security Reference* มีข้อแนะนำและตัวอย่างสำหรับการวาง แผน ความเป็นเจ้าของอ็อบเจ็กต์. ต่อไปนี้เป็นคำแนะนำบางอย่าง:

- โดยทั่วไป, โปรไฟล์กลุ่มต้องไม่เป็นเจ้าของอ็อบเจ็กต์. ถ้าโปรไฟล์กลุ่มเป็น เจ้าของอ็อบเจ็กต์, สมาชิกทั้งหมดในกลุ่มจะมีสิทธิ *ALL ในอ็อบเจ็กต์ ถ้าสมาชิก นั้นไม่ได้ถูกแยกออกอย่าง ชัดเจน.
- ถ้าคุณใช้สิทธิที่รับมา, พิจารณาว่าโปรไฟล์ผู้ใช้ที่เป็นเจ้าของโปรแกรม ควรจะเป็นเจ้าของอ็ อบเจ็กต์แอ็พพลิเคชัน เช่นไฟล์ ด้วยหรือไม่. คุณอาจไม่ ต้องการให้ผู้ใช้ที่รันโปรแกรมที่รับสิทธิ มามีสิทธิ *ALL ในไฟล์.

ถ้าคุณกำลังใช้ iSeries Navigator, วิธีนี้สามารถทำให้สำเร็จได้โดยการทำการเปลี่ยนแปลงโดย สมบูรณ์โดยการใช้ฟังก์ชันเกี่ยวกับ **นโยบาย** ความปลอดภัย. สำหรับข้อมูลเพิ่มเติม, ดูได้ใน iSeries Information Center (อ่าน "สิ่งที่ต้องรู้ก่อนและข้อมูลที่เกี่ยวข้อง" ในหน้า xiii สำหรับรายละเอียด).

สิทธิอ็อบเจ็กต์ในการใช้คำสั่งและโปรแกรมของระบบ

ต่อไปนี้ เป็นคำแนะนำบางอย่างเมื่อคุณจำกัดการให้สิทธิในอ็อบเจ็กต์ที่ IBM จัดหาให้:

- เมื่อคุณมีภาษาประจำชาติในระบบมากกว่าหนึ่งภาษา, ระบบของคุณจะมีไลบรารีระบบ (QSYS) มากกว่าหนึ่งไลบรารี. ระบบของคุณจะมีไลบรารี QSYSxxxx สำหรับแต่ละภาษา ประจำชาติในระบบ. ถ้าคุณใช้สิทธิอ็อบเจ็กต์เพื่อควบคุมการเข้าถึงยังคำสั่งของระบบ, โปรดจำ ไว้ว่าคุณต้องทำให้คำสั่งในไลบรารี QSYS และในทุกๆ ไลบรารี QSYSxxx ในระบบ ของคุณ ปลอดภัย.
- ในบางครั้ง ไลบรารี System/38™ มีคำสั่งที่มีฟังก์ชันที่เทียบเท่ากับคำสั่งที่คุณต้องการ ควบคุม. ต้องมั่นใจว่าคุณได้ควบคุมคำสั่งที่เทียบเท่าใน ไลบรารี QSYS38.
- ถ้าคุณมีสภาพแวดล้อม System/36™, คุณอาจจำเป็นต้องมีการควบคุมโปรแกรมเพิ่มเติม. เช่น, โปรแกรม QY2FTML ที่มีการโอนถ่ายไฟล์ของ System/36 .

การตรวจสอบฟังก์ชันความปลอดภัย

ในบทนี้จะอธิบายถึงเทคนิคในการตรวจสอบประสิทธิผลของความปลอดภัยในระบบของคุณ. เหตุ ผลที่ต้องมีการตรวจสอบความปลอดภัยของระบบ ได้แก่:

- เพื่อประเมินว่าแผนความปลอดภัยสมบูรณ์หรือไม่.
- เพื่อให้แน่ใจว่าการควบคุมความปลอดภัยที่วางแผนไว้ยังทำงานได้ดี. การตรวจสอบประเภทนี้ มักจะกระทำโดยเจ้าหน้าที่รักษาความปลอดภัยระบบ โดยเป็น ส่วนหนึ่งของการจัดการความ ปลอดภัยประจำวัน. การตรวจสอบที่ทำ, โดยมีรายละเอียด มากขึ้นในบางครั้ง, เป็นส่วนหนึ่งของ การตรวจสอบด้านความปลอดภัยเป็นครั้งคราว ที่กระทำโดยผู้ตรวจสอบภายในหรือภายนอก องค์กร.

- เพื่อให้แน่ใจว่าระบบยังอยู่ในสภาพเดิมภายใต้การเปลี่ยนแปลงของสภาพแวดล้อม ของระบบ. ตัวอย่างของการเปลี่ยนแปลงที่มีผลกระทบต่อความปลอดภัย ได้แก่:
  - อ็อบเจ็กต์ที่สร้างโดยผู้ใช้ระบบ
  - ผู้ใช้ใหม่ที่เพิ่มขึ้นในระบบ
  - การเปลี่ยนความเป็นเจ้าของอ็อบเจ็กต์ (โดยไม่ปรับการให้สิทธิ)
  - การเปลี่ยนความรับผิดชอบ (เปลี่ยนกลุ่มผู้ใช้)
  - สิทธิชั่วคราว (เวลาที่ถอนสิทธิไม่เหมาะสม)
  - ผลิตภัณฑ์ใหม่ที่ติดตั้ง
- การเตรียมรับเหตุการณ์ในอนาคต, เช่น การติดตั้งแอ็พพลิเคชันใหม่, การย้าย ไปสู่ระดับความปลอดภัยที่สูงขึ้น, หรือการจัดเตรียมเครือข่ายการสื่อสาร.

เทคนิคที่อธิบายในบทนี้เหมาะสมกับสถานการณ์เหล่านี้. สิ่งที่คุณจะตรวจสอบ และความถี่ในการตรวจสอบนั้น จะขึ้นกับขนาดและความต้องการด้านความปลอดภัยขององค์กรของคุณ. จุดประสงค์ของบทนี้ก็คือ อธิบายว่า ข้อมูลใดที่มีอยู่, วิธีการได้ข้อมูลนั้นมา, และความสำคัญของข้อมูลนั้น, มากกว่าการให้แนวทางในเรื่องความถี่ของการตรวจสอบ.

ข้อมูลนี้มีอยู่สามส่วนด้วยกัน:

- รายการของความปลอดภัยที่สามารถวางแผนและตรวจสอบได้.
- ข้อมูลเกี่ยวกับการจัดเตรียมและใช้เจอร์นัลตรวจสอบที่ได้จากระบบ.
- เทคนิคอื่นๆ ที่มีไว้เพื่อรวบรวมข้อมูลด้านความปลอดภัยในระบบ.

การตรวจสอบความปลอดภัยเกี่ยวข้องกับการใช้คำสั่งในระบบ iSeries และการเข้าถึง ข้อมูลของบันทึกการทำงานและเจอร์นัลในระบบ. คุณอาจต้องการสร้างโปรไฟล์พิเศษ ให้กับผู้ที่ทำหน้าที่ตรวจสอบความปลอดภัยระบบของคุณ. โปรไฟล์ของผู้ตรวจสอบจะต้อง มีสิทธิพิเศษ *AUDIT เพื่อจะสามารถเปลี่ยนคุณลักษณะของการตรวจสอบระบบของคุณ. งานในการตรวจสอบงานส่วนที่ได้แนะนำไว้ในบทนี้ต้องการโปรไฟล์ผู้ใช้ที่มีสิทธิพิเศษ *ALLOBJ และ *SECADM. ต้องแน่ใจว่าคุณตั้งรหัสผ่านสำหรับโปรไฟล์ของผู้ตรวจสอบเป็น *NONE เมื่อช่วงเวลา ของการตรวจสอบสิ้นสุดลง.

สำหรับรายละเอียดเพิ่มเติมเกี่ยวกับการตรวจสอบความปลอดภัย ดูได้ในบทที่ 9, ในหนังสือ*Security Reference* .

การวิเคราะห์โปรไฟล์ผู้ใช้

คุณสามารถแสดงหรือพิมพ์รายชื่อทั้งหมดของผู้ใช้บนระบบโดยการใช้คำสั่ง Display Authorized Users (DSPAUTUSR). รายชื่อเหล่านี้สามารถถูกเรียงลำดับตามชื่อของโปรไฟล์หรือชื่อของโปรไฟล์กลุ่ม. ต่อไปนี้เป็นตัวอย่าง การเรียงลำดับตาม โปรไฟล์กลุ่ม:

```
                        Display Authorized Users

                      Password
Group       User      Last         No
Profile     Profile   Changed   Password  Text
DPTSM
            ANDERSOR  08/04/0x           Roger Anders
            VINCENTM  09/15/0x           Mark Vincent
DPTWH
            ANDERSOR  08/04/0x           Roger Anders
            WAGNERR   09/06/0x           Rose Wagner
QSECOFR
            JONESS    09/20/0x           Sharon Jones
            HARRISOK  08/29/0x           Ken Harrison
*NO GROUP
            DPTSM     09/05/0x    X      Sales and Marketing
            DPTWH     08/13/0x    X      Warehouse
            RICHARDS  09/05/0x           Janet Richards
            SMITHJ    09/18/0x           John Smith
```

การพิมพ์โปรไฟล์ผู้ใช้ที่ถูกเลือกไว้

คุณสามารถใช้คำสั่ง Display User Profile (DSPUSRPRF) ในการสร้างไฟล์เอาต์พุต, ซึ่งนำมาประมวลผลโดยใช้ทูลในการทำเคียวรี่ได้.

```
DSPUSRPRF USRPRF(*ALL) +
          TYPE(*BASIC) OUTPUT(*OUTFILE)
```

คุณสามารถใช้ทูลในการทำเคียวรี่ สร้างรายงานในการวิเคราะห์หลายๆ แบบจากเอาต์พุตไฟล์, เช่น:

- รายชื่อของผู้ใช้ทั้งหมดที่มีสิทธิพิเศษในการใช้งานทั้งแบบ *ALLOBJ และ *SPLCTL .
- รายชื่อของลำดับผู้ใช้ทั้งหมดฟิลด์โปรไหล์ผู้ใช้, เช่น initial program หรือคลาสผู้ใช้.

Yคุณสามารถสร้างโปรแกรมเคียวรี่ที่สร้างรายงานที่แตกต่างจากไฟล์เอาต์พุตของคุณ. ตัวอย่างเช่น:

- โปรไฟล์รายชื่อผู้ใช้ทั้งหมดจะมีสิทธิพิเศษในการใช้งานใดๆ โดยเลือกเร็กคอร์ดที่ฟิลด์ UPSPAU ไม่เท่ากับ *NONE.
- รายชื่อผู้ใช้ทั้งหมดที่ได้รับอนุญาตในใช้คำสั่งโดยการเลือกเร็กคอร์ดที่ฟิลด์ *Limit capabilities* (เรียก UPLTCP ในฐานข้อมูล outfile) ให้เท่ากับ *NO หรือ *PARTIAL.
- แสดงผู้ใช้ทั้งหมดที่มีเมนูเริ่มต้นหรือ initial program เฉพาะ.
- แสดงผู้ใช้ที่ inactive โดยดูจากฟิลด์ date last sign-on.

การตรวจสอบโปรไฟล์ผู้ใช้ขนาดใหญ่

โปรไฟล์ผู้ใช้ที่มีสิทธิในการใช้งานเป็นจำนวนมาก, ซึ่งดูเหมือนว่าจะปรากฏอยู่ทั่วทั้งระบบส่วนใหญ่, สามารถสะท้อนให้เห็นถึง การขาดการวางแผนในด้านการรักษาความปลอดภัย. ต่อไปนี้เป็นวิธีการหนึ่งในการกำหนดตำแหน่ง และประเมินผลโปรไฟล์ผู้ใช้ที่มีเป็นจำนวนมาก:

1. ใช้คำสั่ง Display Object Description (DSPOBJD) ในการสร้างเอาต์พุตไฟล์ ที่มีข้อมูลเกี่ยวกับโปรไฟล์ผู้ใช้ทั้งหมดในระบบ:

   ```
   DSPOBJD OBJ(*ALL) OBJTYPE(*USRPRF) +
           DETAIL(*BASIC) OUTPUT(*OUTFILE)
   ```

2. สร้างโปรแกรมเคียวรี่เพื่อแสดงรายการของชื่อและขนาดของแต่ละโปรไฟล์ผู้ใช้, โดยเรียงลำดับตามขนาดของโปรไฟล์ จากมากไปหาน้อย.
3. พิมพ์ข้อมูลโดยละเอียดของโปรไฟล์ผู้ใช้ที่มีขนาดใหญ่สุด และประเมินดูสิทธิและอ็อบเจ็กต์ที่โปรไฟล์เป็นเจ้าของ เพื่อดูว่าเหมาะสมหรือไม่:

   ```
   DSPUSRPRF USRPRF(user-profile-name) +
             TYPE(*OBJAUT) OUTPUT(*PRINT)
   DSPUSRPRF USRPRF(user-profile-name) +
             TYPE(*OBJOWN) OUTPUT(*PRINT)
   ```

   โปรไฟล์ผู้ใช้ที่ IBM กำหนดให้บางโปรไฟล์ มีขนาดใหญ่มากเนื่องจากจำนวนอ็อบเจ็กต์ที่ผู้ใช้นั้นเป็นเจ้าของมีจำนวนมาก. การแสดงและการวิเคราะห์โปรไฟล์ผู้ใช้เหล่านั้นมักจะไม่ค่อยเป็นสิ่งที่จำเป็นนัก. อย่างไรก็ตาม, คุณควรตรวจสอบโปรแกรมที่ปรับเอาสิทธิในการใช้งานตามโปรไฟล์ผู้ใช้ที่ IBM กำหนดให้ที่มีสิทธิพิเศษแบบ *ALLOBJ, เช่น มี QSECOFR และ QSYS.

สำหรับรายละเอียดเพิ่มเติมเกี่ยวกับการตรวจสอบความปลอดภัย ดูได้ในบทที่ 9, ในหนังสือ *Security Reference* .

การวิเคราะห์สิทธิอ็อบเจ็กต์

คุณสามารถใช้วิธีการต่อไปนี้ในการพิจารณาผู้มีสิทธิที่จะเข้าไปใช้ไลบรารีในระบบ:

1. ใช้คำสั่ง DSPOBJD เพื่อแสดงรายชื่อไลบรารีทั้งหมดในระบบ:

   ```
   DSPOBJD OBJ(QSYS/*ALL) OBJTYPE(*LIB) ASPDEV(*ALLAVL) OUTPUT(*PRINT)
   ```

   หมายเหตุ: ไลบรารีที่อยู่ในพูลของหน่วยความจำอิสระซึ่งเป็นหน่วยความจำรองที่ไม่อยู่ในสถานะ AVAILABLE จะไม่ถูกแสดงผลโดยคำสั่งนี้.
2. ใช้คำสั่ง Display Object Authority (DSPOBJAUT) ในการแสดงสิทธิในการใช้งานของไลบรารีที่ระบุไว้:

   ```
   DSPOBJAUT OBJ(QSYS/library-name) OBJTYPE(*LIB) +
             ASPDEV(asp-device-name) OUTPUT(*PRINT)
   ```

3. ใช้คำสั่ง Display Library (DSPLIB) ในการแสดงรายการของอ็อบเจ็กต์ในไลบรารี:

   ```
   DSPLIB LIB(QSYS/library-name) ASPDEV(asp-device-name) OUTPUT(*PRINT)
   ```

จากการใช้รายงานเหล่านี้, ทำให้คุณสามารถทราบถึงสิ่งที่อยู่ในไลบรารีและผู้มีสิทธิที่จะเข้าไปใช้ไลบรารีนั้น. หากจำเป็น, คุณยังสามารถใช้คำสั่ง DSPOBJAUT เพื่อดูสิทธิในการใช้งานของอ็อบเจ็กต์ที่ถูกเลือกไว้ในไลบรารีนั้นได้ด้วย.

การตรวจสอบอ็อบเจ็กต์ที่มีการเปลี่ยนแปลง

คุณสามารถใช้คำสั่ง Check Object Integrity (CHKOBJITG) ในการหาอ็อบเจ็กต์ที่มีการเปลี่ยนแปลง. อ็อบเจ็กต์ที่ถูกเปลี่ยนแปลงมักจะเป็นการบ่งชี้ให้ให้เห็นว่า มีบางคนพยายามที่จะเข้ามารบกวนระบบของคุณ. คุณอาจต้องการรันคำสั่งนี้ หลังจากมีบางคนกระทำการต่อไปนี้:

- เรียกคืนโปรแกรมไปยังระบบของคุณ
- ใช้ dedicated service tools (DST)

เมื่อคุณรันคำสั่งนี้, ระบบจะสร้างไฟล์ฐานข้อมูลที่บรรจุข้อมูลเกี่ยวกับปัญหาของความเป็นหนึ่งเดียว (integrity) ที่มีแนวโน้มจะเกิดขึ้น. คุณสามารถตรวจสอบอ็อบเจ็กต์ที่มีเจ้าของเป็นโปรไฟล์เดียว, หรือโปรไฟล์หลายโปรไฟล์ที่แตกต่างกัน, หรือทุกโปรไฟล์ได้. คุณสามารถหาอ็อบเจ็กต์ที่โดเมนมีการเปลี่ยนแปลง. และยังสามารถคำนวณค่าการตรวจสอบโปรแกรมใหม่ เพื่อหาอ็อบเจ็กต์ที่เป็น *PGM, *SRVPGM, *MODULE, และ *SQLPKG ที่มีการเปลี่ยนแปลง.

การรันโปรแกรม CHKOBJITG ต้องมีสิทธิพิเศษ *AUDIT. คำสั่งนี้อาจใช้เวลานานในการรันเนื่องจากต้องทำการสแกนและการคำนวณ. จึงควรรันคำสั่งนี้ในขณะที่ระบบว่าง.

หมายเหตุ: โปรไฟล์ที่เป็นเจ้าของอ็อบเจ็กต์หลายอ็อบเจ็กต์ที่มีสิทธิไพรเวตสามารถกลับกลายเป็นโปรไฟล์ที่มีขนาดใหญ่มาก. ขนาดของโปรไฟล์เจ้าของมีผลกระทบต่อประสิทธิภาพการทำงานเมื่อมีการแสดงผลและทำงานกับสิทธิของอ็อบเจ็กต์ที่มันเป็นเจ้าของอยู่, และเมื่อบันทึกหรือเรียกคืนโปรไฟล์. และอาจส่งผลกระทบต่อการดำเนินการของระบบ. เพื่อป้องกันผลกระทบที่อาจเกิดขึ้นกับประสิทธิภาพการทำงานหรือการดำเนินการของระบบอย่างใดอย่างหนึ่ง, ให้ทำการกระจายความเป็นเจ้าของอ็อบเจ็กต์ให้กับโปรไฟล์หลายๆ โปรไฟล์. **อย่ากำหนดอ็อบเจ็กต์ทั้งหมด (หรือเกือบจะทั้งหมด) ให้กับโปรไฟล์เพียงโปรไฟล์เดียว.**

วิเคราะห์โปรแกรมที่ได้รับสิทธิมา

โปรแกรมที่ได้รับสิทธิของผู้ใช้ที่มีสิทธิพิเศษ *ALLOBJ แสดงให้เห็นถึงช่องโหว่ในด้านการรักษาความปลอดภัย. วิธีการต่อไปนี้สามารถใช้ในการหาและตรวจสอบโปรแกรมเหล่านั้น:

1. สำหรับผู้ใช้แต่ละคนที่มีสิทธิพิเศษ *ALLOBJ, ให้ใช้คำสั่ง Display Programs That Adopt (DSPPGMADP) เพื่อแสดงรายการของโปรแกรมที่ได้รับสิทธิของผู้ใช้นั้นๆ:

   ```
   DSPPGMADP USRPRF(user-profile-name) +
             OUTPUT(*PRINT)
   ```

   หมายเหตุ: หัวข้อ "การพิมพ์โปรไฟล์ผู้ใช้ที่ถูกเลือกไว้" ในหน้า 54 แสดงวิธีแสดงรายชื่อผู้ใช้ที่มีสิทธิ *ALLOBJ.
2. ใช้คำสั่ง DSPOBJAUT เพื่อพิจารณาผู้ที่ได้รับอนุญาตให้ใช้โปรแกรมแต่ละโปรแกรม และสิทธิพับลิกใดที่มีต่อโปรแกรมนั้น:

```
DSPOBJAUT OBJ(library-name/program-name) +
          OBJTYPE(*PGM) ASPDEV(library-name/program-name) +
          OUTPUT(*PRINT)
```

3. ตรวจสอบซอร์สโค้ดและคำอธิบายโปรแกรม (program description) เพื่อประเมินว่า:
   - มีการป้องกันผู้ใช้ของโปรแกรมนั้นจากฟังก์ชันส่วนเกิน, เช่น การใช้บรรทัดรับคำสั่ง หรือไม่, ในขณะที่กำลังรันอยู่ภายใต้โปรไฟล์ที่ได้รับมา.
   - โปรแกรมได้รับสิทธิในระดับที่ต่ำที่สุด ที่จำเป็นต่อฟังก์ชันที่ต้องการหรือไม่. แอ็พพลิเคชันที่ใช้ความล้มเหลวของโปรแกรม สามารถถูกออกแบบโดยใช้โปรไฟล์ของเจ้าของเดียวกันสำหรับทั้งอ็อบเจ็กต์และโปรแกรม. เมื่อสิทธิของเจ้าของโปรแกรมถูกนำมาใช้, ผู้ใช้จะมีสิทธิ *ALL ในอ็อบเจ็กต์ของแอ็พพลิเคชันนั้นๆ. ในหลายๆ กรณี, โปรไฟล์ของเจ้าของไม่จำเป็นที่จะต้องใช้สิทธิพิเศษใดๆ .
4. ตรวจสอบเมื่อโปรแกรมมีการเปลี่ยนแปลงครั้งล่าสุด, โดยใช้คำสั่ง DSPOBJD:

```
DSPOBJD OBJ(library-name/program-name) +
        OBJTYPE(*PGM) ASPDEV(library-name/program-name) +
        DETAIL(*FULL)
```

การจัดการเจอร์นัลตรวจสอบและ journal receiver

เจอร์นัลตรวจสอบ, QSYS/QAUDJRN, มีขึ้นเพื่อจุดประสงค์ในการตรวจสอบความปลอดภัยเท่านั้น. อ็อบเจ็กต์ไม่ควรถูกบันทึกลงในเจอร์นัลตรวจสอบ. commitment control ไม่ควรใช้เจอร์นัลตรวจสอบ. user entry ไม่ควรจะถูกส่งไปยังเจอร์นัลนี้ โดยการใช้คำสั่ง Send Journal Entry (SNDJRNE) หรือ API Send Journal Entry (QJOSJRNE).

การป้องกันโดยการล็อกแบบพิเศษจะถูกนำมาใช้ เพื่อให้แน่ใจว่าระบบสามารถเขียนรายการการตรวจสอบ ลงในเจอร์นัลตรวจสอบได้. เมื่อการตรวจสอบแอ็คทีฟ (ค่ากำหนดของระบบ QAUDCTL ไม่เป็น *NONE), system arbitrator job (QSYSARB) จะทำการพักล็อกไว้บนเจอร์นัล QSYS/QAUDJRN. คุณจะไม่สามารถกระทำการปฏิบัติการบางอย่างบนเจอร์นัลตรวจสอบได้ เมื่อการตรวจสอบกำลังแอ็คทีฟ , เช่น:

- คำสั่ง DLTJRN
- คำสั่ง ENDJRNxxx
- คำสั่ง APYJRNCHG
- คำสั่ง RMVJRNCHG
- คำสั่ง DMPOBJ หรือ DMPSYSOBJ
- การย้ายเจอร์นัล
- การกู้คืนเจอร์นัล
- ปฏิบัติการที่ทำงานกับสิทธิ, เช่น คำสั่ง GRTOBJAUT
- คำสั่ง WRKJRN

ข้อมูลที่บันทึกไว้ใน security journal entry ได้ถูกอธิบายไว้ในหนังสือ *Security Reference*. security entry ทั้งหมดในเจอร์นัลตรวจสอบมีเจอร์นัลโค้ดเป็น T. นอกเหนือจาก security entry, ยังมี system

entry ปรากฏอยู่ในเจอร์นัล QAUDJRN อีกด้วย. entry เหล่านี้จะมีคีเจอร์นัลโค้ดเป็น J, ซึ่งเกี่ยวข้องกับ initial program load (IPL) และปฏิบัติการทั่วไปที่กระทำบน journal receiver (ตัวอย่างเช่น, การบันทึก receiver).

หากมีความเสียหายเกิดขึ้นกับเจอร์นัลหรือ receiver ปัจจุบันของเจอร์นัลนั้น จนทำให้ไม่สามารถบันทึก auditing entry ได้, ค่ากำหนดของระบบ QAUDENDACN เป็นตัวกำหนด action ที่ระบบจะจัดการเมื่อเกิดความเสียหายนั้น. การกู้คืนจากเจอร์นัลหรือ journal receiver ที่เสียหายมีวิธีเช่นเดียวกันกับที่ทำกับเจอร์นัลอื่นๆ .

คุณอาจต้องการมีระบบที่จัดการการเปลี่ยนแปลงของ journal receiver. ระบุค่า MNGRCV (*SYSTEM) เมื่อคุณสร้างเจอร์นัล QAUDJRN, หรือเปลี่ยนค่าของเจอร์นัลไปเป็นค่านั้น. ถ้าคุณระบุค่า MNGRCV(*SYSTEM), ระบบจะดึง receiver ออกมาโดยอัตโนมัติ เมื่อมันมีขนาดเท่ากับค่า threshold และจะทำการสร้างและติด journal receiver เข้าไปใหม่. เช่นนี้เรียกว่า **System change-journal management**. โปรดดูที่ iSeries Information Center->Systems management->Journal management->Local journal management->Manage journals สำหรับข้อมูลเพิ่มเติม. โปรดดูที่ “สิ่งที่ต้องรู้ก่อนและข้อมูลที่เกี่ยวข้อง” ในหน้า xiii สำหรับข้อมูลในการเข้าไปใช้งานใน iSeries Information Center.

บทที่ 6. การจัดการสิทธิในการใช้งาน

ชุดของรายงานความปลอดภัยมีไว้เพื่อช่วยเหลือคุณในการติดตามว่า มีการจัดเตรียม สิทธิในระบบของคุณอย่างไร. คุณรันรายงานเหล่านี้ในครั้งแรก, คุณสามารถ พิมพ์ทุกอย่าง (เช่น, สิทธิของทุกไฟล์ หรือทุกโปรแกรม).

หลังจากที่คุณได้เริ่มมีข้อมูลพื้นฐานของคุณแล้ว, คุณสามารถรันรายงานใน เวอร์ชันส่วนที่เปลี่ยนแปลง (changed version) ได้เป็นประจำ. รายงานเวอร์ชัน ส่วนที่เปลี่ยนแปลงจะช่วยคุณแยกแยะการเปลี่ยนแปลงที่เกี่ยวข้องกับความปลอดภัย ในระบบของคุณ ที่คุณต้องเอาใจใส่เป็นพิเศษ. ตัวอย่างเช่น, คุณสามารถรันรายงาน ที่แสดงสิทธิพับลิกสำหรับไฟล์ทุกสัปดาห์. โดยสามารถร้องขอเฉพาะเวอร์ชันส่วนที่ เปลี่ยนแปลงของรายงาน. ซึ่งจะแสดงให้คุณเห็นทั้งไฟล์ใหม่ในระบบที่มีสำหรับทุกคน และไฟล์เดิมที่สิทธิพับลิกถูกเปลี่ยนแปลงตั้งแต่รายงานฉบับที่แล้ว.

มีสองเมนูสำหรับการรันเครื่องมือด้านความปลอดภัย:

- ใช้เมนู SECTOOLS สำหรับการรันโปรแกรมแบบโต้ตอบ.
- ใช้เมนู SECBATCH สำหรับการรันโปรแกรมแบบแบ็ตช์. เมนู SECBATCH แบ่งเป็น สองส่วน: ส่วนหนึ่งสำหรับการส่งงานไปยังคิวงานโดยทันที, และอีกส่วนสำหรับการ ใส่งานไว้ในตารางเวลางาน.

ถ้าคุณกำลังใช้ iSeries Navigator, ให้ทำตามขั้นตอนต่อไปนี้เพื่อที่จะรันทูลในการรักษาความปลอดภัย:

1. ใน iSeries Navigator, ให้ทำการขยายเนื้อที่บนเซิร์ฟเวอร์—>**ความปลอดภัย**ของคุณ.
2. คลิ๊กเมาส์ปุ่มขวาบน **Policy** และเลือก**Explore** เพื่อทำการแสดงผลรายการของ policy ที่คุณสามารถสร้างและควบคุมจัดการได้.

การมอนิเตอร์สิทธิพับลิกที่มีต่ออ็อบเจ็กต์

เพื่อความเรียบง่ายและมีประสิทธิภาพ, ระบบส่วนใหญ่ถูกจัดเตรียมให้อ็อบเจ็กต์ ส่วนใหญ่สามารถใช้ได้โดยผู้ใช้ส่วนใหญ่. ผู้ใช้จะถูกปฏิเสธอย่างชัดแจ้ง (explicit) ในการเข้าถึงอ็อบเจ็กต์ที่เป็นความลับและอ่อนไหวต่อความปลอดภัย มากกว่าการมีสิทธิอย่างชัดแจ้งในการใช้ทุกอ็อบเจ็กต์. ในบางระบบที่ต้องการ ความปลอดภัยสูงจะมีวิธีการที่ตรงกันข้าม และให้สิทธิของอ็อบเจ็กต์เฉพาะที่จำเป็น ต้องใช้เท่านั้น. ในระบบเหล่านั้น, อ็อบเจ็กต์ส่วนใหญ่ถูกสร้างขึ้นมาโดยกำหนด สิทธิพับลิกเป็น *EXCLUDE.

iSeries เป็นระบบแบบอ็อบเจ็กต์ (object-based) ที่มีอ็อบเจ็กต์ประเภทต่างๆ หลายประเภท. ประเภทของอ็อบเจ็กต์โดยส่วนใหญ่ จะไม่มีข้อมูลที่เป็นความลับอยู่ หรือไม่มีการทำงาน ที่เกี่ยวข้องกับความปลอดภัย. ในฐานะผู้บริหารความปลอดภัยในระบบ iSeries ที่ต้องการ ความปลอดภัยแบบทั่วๆ ไป, คุณอาจต้องมุ่งความสนใจของคุณไปยังอ็อบเจ็กต์ที่ต้องการ การป้องกัน เช่น ไฟล์และโปรแกรมฐานข้อมูล. สำหรับอ็อบเจ็กต์ชนิดอื่นๆ คุณเพียงแต่ กำหนดสิทธิพับลิกที่เพียงพอต่อแอ็พพลิเคชันของคุณ, ประเภทของอ็อบเจ็กต์ส่วนใหญ่ ต้องการสิทธ์ *USE.

คุณสามารถใช้คำสั่ง Print Public Authority (PRTPUBAUT) เพื่อพิมพ์ข้อมูลของ อ็อบเจ็กต์ที่ผู้ใช้พับลิกสามารถเข้าถึงได้. (**ผู้ใช้พับลิก–public user)** คือ ผู้ที่มีสิทธิ sign–on แต่ไม่มีสิทธิที่ชัดเจนในอ็อบเจ็กต์.) เมื่อคุณ ใช้คำสั่ง PRTPUBAUT, คุณสามารถระบุประเภทของอ็อบเจ็กต์, และไลบรารีหรือไดเร็กทอรี, ที่คุณต้องการตรวจสอบ.มีอ็อพชันในเมนู SECBATCH และ SECTOOLS เพื่อพิมพ์ Publicly Authorized Object Report ของประเภทของอ็อบเจ็กต์ส่วนใหญ่ที่ปกติมีความปลอดภัยโดยนัย. คุณสามารถพิมพ์เวอร์ชันส่วนที่เปลี่ยนแปลง (changed version) ของรายงานนี้อย่างสม่ำเสมอ เพื่อหาว่ามีอ็อบเจ็กต์ใดที่คุณต้องให้ความสนใจ.

การจัดการสิทธิในการใช้งานสำหรับอ็อบเจ็กต์ใหม่ๆ

OS/400 มีฟังก์ชันที่ช่วยคุณจัดการสิทธิและความเป็นเจ้าของของอ็อบเจ็กต์ใหม่ ในระบบของคุณ. เมื่อผู้ใช้สร้างอ็อบเจ็กต์ใหม่, ระบบจะทำการพิจาราณาสิ่งต่างๆ ต่อไปนี้:

- ผู้ที่จะเป็นเจ้าของอ็อบเจ็กต์นี้
- สิทธิพับลิกสำหรับอ็อบเจ็กต์นี้
- อ็อบเจ็กต์มีสิทธิไพรเวตใดๆ หรือไม่
- ที่อยู่ของอ็อบเจ็กต์นี้ (ในไลบรารีหรือไดเร็กทอรีใด)
- มีการตรวจสอบการเข้าถึงอ็อบเจ็กต์นี้หรือไม่

ระบบจะใช้ค่ากำหนดของระบบ, พารามิเตอร์ของไลบรารี, และพารามิเตอร์ของโปรไฟล์ผู้ใช้ในการตัดสินใจ. “Assigning Authority and Ownership to New Objects” ในบทที่ 5 ของหนังสือ *iSeries Security Reference* มีตัวอย่างหลายตัวอย่าง ของอ็อพชันต่างๆ ที่มี.

คุณสามารถใช้คำสั่ง PRTUSRPRF เพื่อพิมพ์พารามิเตอร์โปรไฟล์ผู้ใช้ที่กระทบ ต่อความเป็นเจ้าของ และสิทธิของอ็อบเจ็กต์ใหม่. รูปที่ 5 ในหน้า 65 แสดงตัวอย่างของรายงานนี้.

การมอนิเตอร์ authorization list

คุณสามารถจัดกลุ่มอ็อบเจ็กต์ที่ต้องการความปลอดภัยที่คล้ายคลึงกันโดยใช้ authorization list. ตามหลักการ, authorization list จะบรรจุรายการของผู้ใช้ และสิทธิที่ผู้ใช้นั้นมีไปยังอ็อบเจ็กต์ทีทำให้ปลอดภัยโดยรายการนั้น. Authorization lists มีวิธีที่มีประสิทธิภาพเพื่อจัดการสิทธิในอ็อบเจ็กต์ที่ คล้ายคลึงกันในระบบ. อย่างไรก็ตาม, ในบางกรณี, ก็ทำให้เกิดความยุ่งยากในการ ติดตามสิทธิในอ็อบเจ็กต์.

คุณสามารถใช้คำสั่ง Print Private Authority (PRTPVTAUT) เพื่อพิมพ์ข้อมูลของ การให้สิทธิของ authorization list. รูปที่ 3 ในหน้า 61 แสดงตัวอย่างของรายงาน.

```
                              Private Authorities (Full Report)
SYSTEM4
Authorization                 Primary                              List  ----------Object----------  ------------Data------------
List            Owner         Group         User         Authority  Mgt   Opr  Mgt  Exist  Alter  Ref  Read  Add  Upd  Dlt  Execute
LIST1           QSECOFR       *NONE         *PUBLIC      *EXCLUDE
LIST2           BUDNIKR       *NONE         BUDNIKR      *ALL        X     X    X     X      X     X    X     X    X    X      X
                                            *PUBLIC      *CHANGE           X                              X     X    X    X      X
LIST3           QSECOFR       *NONE         *PUBLIC      *EXCLUDE
LIST4           CJWLDR        *NONE         CJWLDR       *ALL        X     X    X     X      X     X    X     X    X    X      X
                                            GROUP1       *ALL              X    X     X      X     X    X     X    X    X      X
                                            *PUBLIC      *EXCLUDE
```

รูปที่ 3. Private Authorities Report ของ Authorization Lists

รายงานนี้แสดงข้อมูลเดียวกันกับที่คุณเห็นในหน้าจอ Edit Authorization List (EDTAUTL). ประโยชน์ของรายงานนี้ คือ การให้ข้อมูลเกี่ยวกับ authorization lists ทั้งหมด ไว้ในที่เดียวกัน. ตัวอย่างเช่น, ถ้าคุณจัดเตรียมความปลอดภัยสำหรับกลุ่มใหม่ ของอ็อบเจ็กต์, คุณสามารถมองอย่างรวดเร็ว เพื่อหาว่า authorization lists ที่มีอยู่ตรงกับความต้องการของคุณสำหรับอ็อบเจ็กต์เหล่านั้นหรือไม่.

คุณสามารถพิมพ์เวอร์ชันส่วนที่เปลี่ยนแปลงของรายงานนี้เพื่อดู authorization list ใหม่หรือ authorization list ที่มีการเปลี่ยนแปลงสิทธิหลังจากที่คุณได้พิมพ์ รายงานนี้ในครั้งที่แล้ว. คุณยังมีอ็อพชันของการพิมพ์รายการของอ็อบเจ็กต์ที่ ถูกทำให้ปลอดภัยโดยแต่ละ authorization list. รูปที่ 4แสดงตัวอย่าง ของรายงานสำหรับหนึ่ง authorization list:

```
                      Display Authorization List Objects
Authorization list . . . . . :   CUSTAUTL
Library  . . . . . :     QSYS
Owner  . . . . . :   AROWNER
Primary group  . . . . . :   *NONE

                                                          Primary
Object          Library         Type          Owner       group          Text
CUSTMAS         CUSTLIB         *FILE         AROWNER     *NONE
CUSTORD         CUSTORD         *FILE         OEOWNER     *NONE
```

รูปที่ 4. รายงานการแสดงผลอ็อบเจ็กต์ของ authorization list

ตัวอย่างในการใช้รายงานนี้, เช่น, เพื่อทำความเข้าใจผลกระทบจากการเพิ่ม ผู้ใช้ใหม่ไปยัง authorization lists (เพื่อดูสิทธิที่ผู้ใช้นั้นได้รับ).

การใช้ authorization lists

iSeries Navigator มีคุณลักษณะพิเศษเกี่ยวกับความปลอดภัยที่ถูกออกแบบมาเพื่อช่วยเหลือคุณในการพัฒนาแผนการ และ นโยบายเกี่ยวกับความปลอดภัย, รวมทั้งการปรับแต่งค่าระบบของคุณให้ตรงกับความต้องการของบริษัทของคุณ. ฟังก์ชันหนึ่งที่สามารถใช้ได้ก็คือ การใช้ authorization list.

authorization list มีคุณลักษณะดังต่อไปนี้.

- authorization list รวมอ็อบเจ็กต์ที่มีความต้องการด้านความปลอดภัยที่เหมือนกัน เข้าเป็นกลุ่มเดียวกัน.

- ตามหลักการ authorization list จะบรรจุรายการของผู้ใช้และกลุ่ม และสิทธิที่ผู้ใช้ และกลุ่มนั้นมีในอ็อบเจ็กต์ทีทำให้ปลอดภัยโดย authorization list นั้น.
- แต่ละผู้ใช้และกลุ่มสามารถมีสิทธิที่ต่างกันในชุดของอ็อบเจกต์ที่ authorization list นั้นทำให้ปลอดภัย.
- การให้สิทธิสามารถทำในรูปแบบของรายการแทนที่จะเป็นแบบแต่ละผู้ใช้และกลุ่ม .

งานที่สามารถทำได้โดยการใช้ authorization list รวมไปถึงงานต่อไปนี้.

- สร้าง authorization list
- เปลี่ยน authorization list.
- เพิ่มผู้ใช้และกลุ่ม.
- เปลี่ยนการอนุญาตผู้ใช้ (user permissions).
- แสดงอ็อบเจ็กต์ที่ถูกทำให้ปลอดภัย.

ในการใช้ฟังก์ชันนี้, ให้ดำเนินการตามขั้นตอนดังต่อไปนี้:

1. จากการรักษาความปลอดภัยของ iSeries Navigator, ให้ทำการขยายเนื้อที่ของเซิร์ฟเวอร์ —>. คุณจะมองเห็น **Authorization List** และ **Policy**.
2. คลิ๊กเมาส์ปุ่มขวาบน **Authorization Lists** และเลือก **New Authorization List**. **New Authorization List**อนุญาตให้คุณกระทำสิ่งต่อไปนี้.
   - **Use:** อนุญาตการเข้าถึงแอ็ตทริบิวต์ของอ็อบเจ็กต์ และการใช้อ็อบเจ็กต์. พับลิกอาจมองเห็น, แต่ไม่เปลี่ยนแปลงอ็อบเจ็กต์.
   - **Change:** อนุญาตให้เปลี่ยนแปลงสิ่งที่อยู่ภายในอ็อบเจ็กต์ (ที่มีบาง exception).
   - **All:** อนุญาตให้ดำเนินการทุกอย่างกับอ็อบเจ็กต์, เว้นแต่ว่าการกระทำเหล่านั้นถูกจำกัดไว้ให้กับเจ้าของเท่านั้น. ผู้ใช้หรือกลุ่มสามารถควบคุมการมีอยู่ของอ็อบเจ็กต์ (object's existence), กำหนดความปลอดภัยให้กับอ็อบเจ็กต์, เปลี่ยนแปลงอ็อบเจ็กต์, และทำฟังก์ชันพื้นฐานบนอ็อบเจ็กต์. ผู้ใช้หรือกลุ่มยังสามารถเปลี่ยนความเป็นเจ้าของของอ็อบเจ็กต์ได้ด้วย.
   - **Exclude:**ห้ามดำเนินการใดๆ บนอ็อบเจ็กต์. ไม่มีการอนุญาตให้เข้าถึงหรือดำเนินการใดๆ กับอ็อบเจ็กต์สำหรับผู้ใช้หรือกลุ่มที่มีการอนุญาตนี้. ระบุให้พับลิกไม่ได้รับอนุญาตให้ใช้อ็อบเจ็กต์นี้.

เมื่อทำงานกับ authorization list คุณจะต้องการให้การอนุญาตทั้งอ็อบเจ็กต์และข้อมูล. การอนุญาตในอ็อบเจ็กต์ (object permission) ที่คุณสามารถเลือกได้มีดังนี้.

- **Operational:** ให้การอนุญาตในการดูคำอธิบายของอ็อบเจ็กต์ และใช้อ็อบเจ็กต์นั้น ตามที่พิจารณาโดยการอนุญาตในข้อมูล (data permission) ที่ผู้ใช้หรือกลุ่มมีอยู่กับอ็อบเจ็กต์นั้น.
- **Management:** ให้การอนุญาตในการระบุความปลอดภัยของอ็อบเจ็กต์, ย้ายหรือเปลี่ยนชื่ออ็อบเจ็กต์, และเพิ่มสมาชิกให้กับไฟล์ฐานข้อมูล.
- **Existence:** ให้การอนุญาตในการควบคุมการมีอยู่ของอ็อบเจ็กต์และความเป็นเจ้าของ. ผู้ใช้หรือกลุ่มสามารถลบอ็อบเจ็กต์, ทำสื่อบันทึกของอ็อบเจ็กต์ให้ว่าง, ดำเนินการบันทึกและกู้คืนอ็อบเจ็กต์,และย้ายความเป็นเจ้าของของอ็อบเจ็กต์. ถ้าผู้ใช้หรือกลุ่มมีการอนุญาตให้มีการบันทึกแบบพิเศษ, ผู้ใช้หรือกลุ่มไม่จำเป็นต้องมีการอนุญาต existence ในอ็อบเจ็กต์.
- **Alter** (ใช้กับไฟล์ฐานข้อมูลและแพ็กเกจ SQL เท่านั้น): ให้การอนุญาตในการเปลี่ยนแอ็ตทริบิวต์ของอ็อบเจ็กต์. ถ้าผู้ใช้หรือกลุ่มมีการอนุญาตนี้บนไฟล์ฐานข้อมูล, ผู้ใช้หรือกลุ่มจะสามารถ

เพิ่มและลบทริกเกอร์, เพิ่มและลบข้อจำกัด referential และ unique, และเปลี่ยนแอ็ตทริบิวต์ของไฟล์ฐานข้อมูล. ถ้าผู้ใช้หรือกลุ่มมีการอนุญาตนี้บนแพ็กเกจ SQL, ผู้ใช้หรือกลุ่มนั้นจะสามารถเปลี่ยนแอ็ตทริบิวต์ของแพ็กเกจ SQL. การอนุญาตนี้ใช้ได้กับไฟล์ฐานข้อมูล และแพ็กเกจ SQL เท่านั้น.

- **Reference**(ใช้กับไฟล์ฐานข้อมูลและแพ็กเกจ SQL): ให้การอนุญาตในการอ้างอิงอ็อบเจ็กต์จากอ็อบเจ็กต์อื่น ที่การดำเนินการบนอ็อบเจ็กต์นั้นอาจถูกควบคุมโดยอ็อบเจ็กต์อื่น. ถ้าผู้ใช้หรือกลุ่มมีการอนุญาตนี้บนฟิสิคัลไฟล์, ผู้ใช้หรือกลุ่มสามารถเพิ่มข้อจำกัดreferential ที่ฟิสิคัลไฟล์เป็นแหล่งกำเนิด. ในปัจจุบัน การอนุญาตนี้ใช้กับไฟล์ฐานข้อมูลเท่านั้น.

การอนุญาตในข้อมูล (data permission) ที่คุณสามารถเลือกได้มีดังนี้.

- **Read**: ให้การอนุญาตในการได้รับและแสดงผลสิ่งที่อยู่ภายในอ็อบเจ็กต์, เช่น การดูเร็กคอร์ดภายในไฟล์.
- **Add**: ให้การอนุญาตในการเพิ่ม entry ให้กับอ็อบเจ็กต์, เช่น การเพิ่มข้อความให้กับ message queue หรือการเพิ่มเร็กคอร์ดให้กับไฟล์.
- **Update**: ให้การอนุญาตในการเปลี่ยนแปลง entry ในอ็อบเจ็กต์, เช่น การเปลี่ยนแปลงเร็กคอร์ดในไฟล์.
- **Delete**: ให้การอนุญาตในการลบ entry จากอ็อบเจ็กต์, เช่น การลบข้อความจาก message queue หรือการลบเร็กคอร์ดออกจากไฟล์.
- **Execute**: ให้การอนุญาตในการรันโปรแกรม, เซอร์วิสโปรแกรม หรือ แพ็กเกจ SQL. ผู้ใช้ยังสามารถหาตำแหน่งของอ็อบเจ็กต์ในไลบรารีหรือไดเร็กทอรี.

สำหรับข้อมูลเพิ่มเติมเกี่ยวกับแต่ละกระบวนการเกี่ยวกับการสร้าง หรือ แก้ไข authorization list ของคุณ, ใช้คำอธิบายออนไลน์ที่มีอยู่ใน iSeries Navigator.

การเข้าไปใช้ Policy ใน iSeries Navigator

คุณสามารถใช้ iSeries Navigator ในการเรียกดูและจัดการ policy ให้กับเซิร์ฟเวอร์ iSeries ของคุณ. iSeries Navigator มี policy ด้วยกันห้าสาขาคือ:

- **Audit policy**
  อนุญาตให้คุณทำการติดตั้งการมอนิเตอร์สำหรับ action ที่จำเพาะเจาะจงและการเข้าถึงรีซอร์สที่จำเพาะเจาะจงบนระบบของคุณ.
- **Security policy**
  อนุญาตให้คุณระบุระดับของความปลอดภัยและตัวเลือกเพิ่มเติมที่เกี่ยวข้องกับความปลอดภัยของระบบ.
- **Password policy**
  อนุญาตให้คุณระบุระดับของรหัสผ่านสำหรับระบบ.
- **Restore policy**
  อนุญาตให้คุณระบุว่าอ็อบเจ็กต์ต่างๆ ถูกเรียกคืนมาบนระบบได้อย่างไร.
- **Sign-on policy**
  อนุญาตให้คุณระบุวิธีที่ผู้ใช้สามารถ sign – on เข้าไปยังระบบ.

การเรียกดูหรือเปลี่ยน policy ด้วย iSeries Navigator, ให้ทำตามขั้นตอนต่อไปนี้:

1. จากiSeries Navigator, ให้ทำการขยายเนื้อที่บนเซิร์ฟเวอร์ —> **ความปลอดภัย**.
2. กดเมาส์ปุ่มขวามือเลือก **Policies** และเลือก **Explore** เพื่อแสดงผลรายการของ policy ที่สามารถสร้างขึ้นและจัดการได้. โปรดดูที่คำอธิบาย iSeries Navigator สำหรับคำเฉพาะที่อยู่ในหัวข้อนี้.

การมอนิเตอร์สิทธิไพรเวตของอ็อบเจ็กต์

อ็อพชันของเมนู SECBATCH:
12 *เพื่อส่งงานทันที* **41** *เพื่อใช้ตารางเวลางาน*

คุณสามารถใช้คำสั่ง Print Private Authority (PRTPVTAUT) เพื่อพิมพิมพ์รายการ ของสิทธิไพรเวตทั้งหมดสำหรับอ็อบเจ็กต์ประเภทที่กำหนดที่อยู่ในไลบรารีที่กำหนด.

คุณสามารถใช้รายงานนี้เพื่อช่วยคุณตรวจจับสิทธิใหม่ๆ ในอ็อบเจ็กต์ . และยังช่วยคุณรักษาโครงร่างของสิทธิไพรเวตไว้จากความยุ่งเหยิงและไม่สามารถจัดการได้.

การมอนิเตอร์การเข้าถึงเอาต์พุตและคิวงาน

บางครั้งผู้บริหารความปลอดภัยทำหน้าที่ในการปกป้องการเข้าถึงไฟล์ได้ดีเยี่ยม แต่ลืมเกี่ยวกับสิ่งที่เกิดขึ้นเมื่อสิ่งที่อยู่ในไฟล์นั้นถูกพิมพ์. เซิร์ฟเวอร์ iSeries จะมีฟังก์ชันสำหรับคุณเพื่อใช้ในการปกป้องเอาต์พุตคิวและคิวงานที่เป็นความลับ . คุณป้องกันเอาต์พุตคิว เพื่อให้ผู้ใช้ที่ไม่ได้รับอนุญาตจะไม่สามารถดู หรือทำสำเนาข้อมูลที่เป็นความลับ จากที่พักสพูลไฟล์เพื่อรอการพิมพ์ เป็นต้น. คุณป้องกันคิวงานเพื่อให้ผู้ใช้ ที่ไม่ได้รับอนุญาตจะไม่สามารถเปลี่ยนทิศทางของงานที่เป็นความลับไปยังเอาต์พุตคิว ที่ไม่เป็นความลับ หรือยกเลิกงานทั้งหมด.

อ็อพชันของเมนู SECBATCH:
24 เพื่อส่งงานทันที 63 *เพื่อใช้ตารางเวลางาน*

Basic system security and planning ใน Information Center และหนังสือ *iSeries Security Reference* อธิบายเกี่ยวกับวิธิการป้องกันเอาต์พุตคิว และคิวงานของคุณ.

คุณสามารถใช้คำสั่ง Print Queue Authority (PRTQAUT) เพื่อพิมพ์ค่าติดตั้ง ด้านความปลอดภัยสำหรับคิวงาน และเอาต์พุตคิวในระบบของคุณ. เพื่อคุณจะสามารถประเมิน งานพิมพ์ที่พิมพ์ข้อมูลที่เป็นความลับ และมั่นใจว่างานนั้นจะไปยังเอาต์พุตคิว และคิวงานที่คุณป้องกันไว้แล้ว.

สำหรับเอาต์พุตคิวและคิวงานที่คุณพิจารณาว่าต้องระวังเรื่องความปลอดภัย, คุณสามารถเปรียบเทียบค่าติดตั้งด้านความปลอดภัยกับข้อมูลในภาคผนวก D ของหนังสือ *iSeries Security Reference* . ตารางในภาคผนวก D จะบอกถึงค่าติดตั้งที่ ต้องการสำหรับการทำงานต่างๆ ของเอาต์พุตคิวและคิวงาน.

การมอนิเตอร์สิทธิพิเศษต่างๆ

เมื่อผู้ใช้ในระบบของคุณมีสิทธิพิเศษที่ไม่จำเป็น, ความพยายามในการสร้าง โครงร่างสิทธิ์อ็อบเจ็กต์ของคุณอาจสูญเปล่า. สิทธิอ็อบเจ็กต์จะไม่มีความหมาย เมื่อโปรไฟล์ผู้ใช้มีสิทธิพิเศษ *ALLOBJ. ผู้ใช้ที่มีสิทธิพิเศษ *SPLCTL สามารถดูไฟล์ในที่พักใดๆ ของระบบได้, ไม่ว่าคุณจะพยายามทำให้เอาต์พุตคิว ของคุณปลอดภัยเพียงใด. ผู้ใช้ที่มีสิทธิพิเศษ *JOBCTL สามารถส่งผลกระทบกับ การทำงานของระบบและเปลี่ยนทิศทางของงานได้. ผู้ใช้ที่มีสิทธิพิเศษ *SERVICE จะสามารถใช้เครื่องมือบริการ (service tools) เพื่อเข้าถึงข้อมูลโดยไม่ต้องผ่าน ระบบปฏิบัติการ.

อ็อพชันของเมนู SECBATCH:

29 เพื่อส่งงานทันที 68 *เพื่อใช้ตารางเวลางาน*

คุณสามารถใช้คำสั่ง Print User Profile (PRTUSRPRF) เพื่อพิมพ์ข้อมูล เกี่ยวกับสิทธิพิเศษและคลาสผู้ใช้ของโปรไฟล์ผู้ใช้ในระบบของคุณ. เมื่อคุณรันรายงานนี้, คุณมีอ็อพชันหลายอ็อพชัน ดังนี้:

- โปรไฟล์ผู้ใช้ทั้งหมด
- โปรไฟล์ผู้ใช้ที่มีสิทธิพิเศษที่กำหนด
- โปรไฟล์ผู้ใช้ที่มีคลาสผู้ใช้ที่กำหนด
- โปรไฟล์ผู้ใช้ที่ไม่ตรงกันระหว่างคลาสผู้ใช้และสิทธิพิเศษ.

รูปที่ 5แสดงตัวอย่างของรายงานที่แสดงถึงสิทธิพิเศษของ โปรไฟล์ผู้ใช้ทั้งหมด:

```
                                  User Profile Information
  Report type  . . . . . . . . . :   *AUTINFO
  Select by  . . . . . . . . . . :   *SPCAUT
  Special authorities  . . . . . :   *ALL
                    ------------Special Authorities-------------
                                *IO                                                          Group
User      Group     *ALL  *AUD  SYS  *JOB  *SAV  *SEC  *SER  *SPL  User                Group       Authority   Limited
Profile   Profiles   OBJ   IT   CFG   CTL   SYS   ADM  VICE   CTL  Class      Owner    Authority   Type        Capability
USERA     *NONE      X     X    X     X     X     X     X     X    *SECOFR    *USRPRF  *NONE       *PRIVATE    *NO
USERB     *NONE                       X     X                       *PGMR      *USRPRF  *NONE       *PRIVATE    *NO
USERC     *NONE      X     X    X     X     X     X     X     X    *SECOFR    *USRPRF  *NONE       *PRIVATE    *NO
USERD     *NONE                                                     *USER      *USRPRF  *NONE       *PRIVATE    *NO
```

รูปที่ 5. รายงานข้อมูลของผู้ใช้: ตัวอย่างที่ 1

รายงานยังแสดงส่วนเพิ่มเติมจากสิทธิพิเศษ, ดังต่อไปนี้:

- โปรไฟล์ผู้ใช้มีความสามารถจำกัดหรือไม่.

- ผู้ใช้หรือกลุ่มของผู้ใช้เป็นเจ้าของอ็อบเจ็กต์ใหม่ที่ผู้ใช้สร้างหรือไม่.
- สิทธิใดที่กลุ่มของผู้ใช้จะได้รับในอ็อบเจ็กต์ใหม่ที่ผู้ใช้สร้าง โดยอัตโนมัติ.

รูปที่ 6แสดงตัวอย่างของสิทธิพิเศษและคลาสผู้ใช้ที่ไม่ตรงกัน:

```
User Profile Information
Report type  . . . . . :   *AUTINFO
Select by  . . . . . :   *MISMATCH
------------------------------Special Authorities-------------
                              *IO                                                                  Group
User      Group     *ALL  *AUD  SYS  *JOB  *SAV  *SEC  *SER  *SPL  User                Group       Authority   Limited
Profile   Profiles   OBJ   IT   CFG   CTL   SYS   ADM  VICE   CTL  Class      Owner    Authority   Type        Capability
USERX     *NONE       X               X     X                 X    *SYSOPR    *USRPRF  *NONE       *PRIVATE    *NO
USERY     *NONE                                   X               *USER      *USRPRF  *NONE       *PRIVATE    *NO
USERZ                                             X               *USER      *USRPRF  *NONE       *PRIVATE    *NO
          QPGMR                        X     X
```

รูปที่ 6. รายงานข้อมูลของผู้ใช้: ตัวอย่างที่ 2

ใน รูปที่ 6, ให้สังเกตสิ่งต่อไปนี้:

- USERX มีคลาสผู้ใช้เป็น system operator (*SYSOPR) แต่มีสิทธิพิเศษ *ALLOBJ และ *SPLCTL.
- USERY มีคลาสผู้ใช้เป็น user (*USER) แต่มีสิทธิพิเศษ *SECADM.
- USERZ ก็มีคลาสเป็น user (*USER) และมีสิทธิพิเศษ *SECADM เช่นกัน. คุณยัง สามารถเห็นว่า USERZ เป็นสมาชิกของกลุ่ม QPGMR, ซึ่งมีสิทธิพิเศษ *JOBCTL และ *SAVSYS.

คุณสามารถรันรายงานนี้อย่างสม่ำเสมอเพื่อช่วยคุณเฝ้าสังเกตการบริหารโปรไฟล์ผู้ใช้.

การมอนิเตอร์สภาวะแวดล้อมของ

บทบาทหนึ่งของโปรไฟล์ผู้ใช้คือ การกำหนดสภาพแวดล้อมสำหรับผู้ใช้ ซึ่งรวมถึง อาต์พุตคิว, เมนูเริ่มต้น, และคำอธิบายงาน (job description). สภาพแวดล้อมของผู้ใช้ มีผลต่อวิธีการที่ผู้ใช้มองเห็นระบบ, และในบางแง่ก็คือ, สิ่งที่ผู้ใช้ได้รับอนุญาต ให้ทำ. ผู้ใช้ต้องมีสิทธิในอ็อบเจ็กต์ที่กำหนดไว้ในโปรไฟล์ผู้ใช้. อย่างไรก็ตาม, ถ้าโครงร่างสิทธิของคุณยังอยู่ในระหว่างการปรับปรุง หรือยังไม่เข้มงวด, สภาพแวดล้อมผู้ใช้ที่กำหนดในโปรไฟล์ผู้ใช้อาจทำให้เกิดผลที่คุณไม่ต้องการให้เป็น. ดังตัวอย่างต่อไปนี้:

อ็อพชันของเมนู SECBATCH:

29 *เพื่อส่งงานทันที* 68 *เพื่อใช้ตารางเวลางาน*

- คำอธิบายงานของผู้ใช้อาจกำหนดโปรไฟล์ผู้ใช้ที่มีสิทธิมากกว่าผู้ใช้.
- ผู้ใช้อาจมีเมนูเริ่มต้นที่ไม่มีบรรทัดรับคำสั่ง. อย่างไรก็ตาม, โปรแกรม attention-key-handling ของผู้ใช้อาจมีบรรทัดรับคำสั่ง.
- ผู้ใช้อาจมีสิทธิในการรันรายงานที่เป็นความลับ. อย่างไรก็ตาม, เอาต์พุตของ ผู้ใช้อาจมีทิศทางไปยังเอาต์พุตคิวที่มีไว้สำหรับผู้ใช้ที่ไม่ควรดูรายงานนี้.

คุณสามารถใช้อ็อพชัน *ENVINFO ของคำสั่ง Print User Profile (PRTUSRPRF) เพื่อช่วยคุณเฝ้าสังเกตสภาพแวดล้อมที่กำหนดให้กับผู้ใช้ระบบ. รูปที่ 7แสดงตัวอย่างของรายงานนี้:

```
                                   User Profile Information
  Report type  . . . . . . . . . :   *ENVINFO
  Select by  . . . . . . . . . . :   *USRCLS
                          Initial       Initial          Job          Message       Output        Attention
User            Current   Menu/         Program/     Description/     Queue/        Queue/        Program/
Profile         Library   Library       Library        Library        Library       Library       Library
AUDSECOFR       AUDITOR   MAIN          *NONE          QDFTJOBD       QSYSOPR       *WRKSTN       *SYSVAL
                          *LIBL                        QGPL            QSYS
USERA           *CRTDFT   OEMENU        *NONE          QDFTJOBD       USERA         *WRKSTN       *SYSVAL
                          *LIBL                        QGPL            QUSRSYS
USERB           *CRTDFT   INVMENU       *NONE          QDFTJOBD       USERB         *WRKSTN       *SYSVAL
                          *LIBL                        QGPL            QUSRSYS
USERC           *CRTDFT   PAYROLL       *NONE          QDFTJOBD       USERC         PAYROLL       *SYSVAL
                          *LIBL                        QGPL            QUSRSYS        PRPGMLIB
```

รูปที่ 7. ตัวอย่างการพิมพ์โปรไฟล์ผู้ใช้ - สภาวะแวดล้อมของผู้ใช้

การจัดการเซอร์วิสทูลต่างๆ

เซอร์วิสทูลถูกใช้ในการปรับแต่งค่า, จัดการ, และให้บริการ เซิร์ฟเวอร์ของคุณ. เซอร์วิสทูลสามารถถูกเข้าไปใช้งานจาก dedicated service tools (DST) หรือ system service tools (SST). user ID ของเซอร์วิสทูลเป็นสิ่งที่จำเป็นในการเข้าไปใช้ DST, SST, และในการใช้ฟังก์ชัน iSeries Navigator สำหรับการจัดการโลจิคัลพาร์ติชัน (LPAR) และการจัดการดิสก์ยูนิต.

DST จะสามารถทำงานได้เมื่อ Licensed Internal Code ถูกเรียกใช้งาน, ถึงแม้ว่า OS/400 ถูกโหลดขึ้นมา. SST จะสามารถทำงานได้จาก OS/400. ตารางต่อไปนี้แสดงความแตกต่างระหว่าง DST และ SST โดยคร่าวๆ .

ลักษณะ	DST	SST
เข้าไปใช้งานได้อย่างไร	การเข้าไปใช้งานแบบฟิสิคัลผ่านทางคอนโซลในขณะที่ IPL ทำงานแบบ manual หรือโดยการเลือกตัวเลือก 21 บนคอนโทรลพาเนล.	การเข้าไปใช้งานผ่านทางงานแบบโต้ตอบด้วยความสามารถในการ sign on ด้วย QSRV หรือการให้สิทธิดังต่อไปนี้: • คำสั่ง CL ที่ได้รับการให้สิทธิ STRSST (เริ่มการทำงานของ SST). • บริการสิทธิพิเศษ (*SERVICE) หรือ สิทธิพิเศษสำหรับอ็อบเจ็กต์ทั้งหมด (*ALLOBJ). • สิทธิพิเศษของฟังก์ชันในการใช้ SST.
เมื่อใช้งานได้	ใช้งานได้แม้กระทั่งในกรณีที่เซิร์ฟเวอร์มีความสามารถจำกัด. OS/400 ไม่จำเป็นที่จะต้องเข้าไปใช้ DST.	ใช้งานได้เมื่อ OS/400 เริ่มทำงาน. OS/400 จำเป็นต้องมีการเข้าไปใช้ SST.
ตรวจสอบสิทธิได้อย่างไร	จำเป็นต้องใช้ user ID และ รหัสผ่านของเซอร์วิสทูล.	จำเป็นต้องใช้user ID และ รหัสผ่านของเซอร์วิสทูล.

โปรดดูที่ iSeries Information Center—>Security—>Service tools สำหรับข้อมูลเกี่ยวกับการใช้เซอร์วิสทูลในการดำเนินงานดังต่อไปนี้:

- การเข้าถึงเซอร์วิสทูลด้วย DST
- การเข้าถึงเซอร์วิสทูลด้วย SST
- การเข้าถึงเซอร์วิสทูลด้วย iSeries Navigator
- การสร้าง user ID ของเซอร์วิสทูล
- การเปลี่ยนแปลงสิทธิพิเศษในการทำงานสำหรับ user ID ของเซอร์วิสทูล
- การเปลี่ยนแปลงรายละเอียดสำหรับ user ID ของเซอร์วิสทูล
- การแสดง user ID ของ เซอร์วิสทูล
- การอนุญาตให้ user ID ของเซอร์วิสทูลใช้งานได้ หรือ ใช้งานไม่ได้
- การลบ user ID ของเซอร์วิสทูล
- การเปลี่ยนแปลง user ID และ รหัสผ่าน ของเซอร์วิสทูล โดยการใช้ SST หรือ DST
- การเปลี่ยนแปลง user ID ของคุณสำหรับเซอร์วิสทูล โดยการใช้ STRSST
- การเปลี่ยนแปลง user ID และรหัสผ่านของ เซอร์วิสทูล โดยการใช้
- การเปลี่ยนแปลง user ID ของเซอร์วิสทูล (QSYCHGDS) API
- การรีเซ็ต QSECOFR ที่เป็นรหัสผ่านของโปรไฟล์ผู้ใช้ใน OS/400
- การรีเซ็ต user ID และรหัสผ่าน ของเซอร์วิสทูล QSECOFR
- บันทึกข้อมูลความปลอดภัยของเซอร์วิสทูล และ การเรียกคืนข้อมูลความปลอดภัยของเซอร์วิสทูล
- การสร้าง user ID ของเซอร์วิสทูล QSECOFR ที่เป็นเวอร์ชันของคุณเอง

- การปรับแต่งค่าของเซิร์ฟเวอร์เซอร์วิสทูล สำหรับ DST
- การปรับแต่งค่าของเซิร์ฟเวอร์เซอร์วิสทูลสำหรับ OS/400
- การมอนิเตอร์การใช้เซอร์วิสฟังก์ชันผ่านทาง DST
- การมอนิเตอร์การใช้เซอร์วิสทูลผ่านทางไฟล์บันทึกการตรวจสอบความปลอดภัยของ OS/400

โปรดดูที่ “สิ่งที่ต้องรู้ก่อนและข้อมูลที่เกี่ยวข้อง” ในหน้า xiii สำหรับข้อมูลที่ใช้ในการเข้าถึง iSeries Information Center.

บทที่ 7. การใช้การรักษาความปลอดภัยแบบโลจิคัลพาร์ติชัน (Logical partitions - LPAR)

การที่มีลอจิคัลพาร์ติชันหลายๆ พาร์ติชันบนเซิร์ฟเวอร์iSeriesเพียงเซิร์ฟเวอร์เดียว สามารถแสดงให้เห็นถึงผลประโยชน์ที่จะได้รับ ในเหตุการณ์ดังต่อไปนี้.

- **การรักษาสถานภาพการเป็นระบบอิสระ**: โดยการเสียสละรีซอร์สจำนวนหนึ่ง (ดิสก์ที่เป็นหน่วยเก็บข้อมูล, โพรเซสเซอร์, หน่วยความจำ, และ อุปกรณ์ I/O) ให้กับพาร์ติชัน ในการทำให้เกิดการแยกกัน (รีซอร์สออก)แบบโลจิคัลของซอฟต์แวร์ . ลอจิ คัลพาร์ติชันจะมี fault tolerance ในส่วนของฮาร์ดแวร์อยู่ด้วย ในกรณีที่มีการตั้งค่าอย่างเหมาะสม. เวิร์กโหลดแบบโต้ตอบ และแบบแบ็ตช์ที่อาจจะทำงานร่วมกันได้ไม่ดีนักบนเครื่องเดียวกัน สามารถถูกแยกออกจากกันและทำงานอย่างมีประสิทธิภาพได้ในพาร์ติชันที่แยกจากกัน.
- **Consolidation** : ระบบที่ถูกทำพาร์ติชันแบบลอจิคัลสามารถลดจำนวนระบบของเซิร์ฟเวอร์ iSeries ที่จำเป็นภายในหน่วยงานหนึ่งๆ ได้. โดยการรวมหลายๆ ระบบให้เป็น ระบบที่มีการแบ่งพาร์ติชันแบบลอจิคัลเพียงระบบเดียว. ซึ่งจะเป็นการตัดความต้องการ, และค่าใช้จ่าย, ของอุปกรณ์เพิ่มเติม. คุณสามารถย้ายรีซอร์สจากลอจิคัลพาร์ติชันหนึ่ง ไปยังอีกลอจิคัลพาร์ติชันได้ตามความต้องการ.
- **การสร้างสภาวะแวดล้อมแบบผสมของระบบทำงานประจำและระบบทดสอบ**: คุณสามารถสร้างสภาวะแวดล้อมที่รวมระบบกระบวนการทำงานประจำและระบบทดสอบไว้ในเครื่องเดียวกัน. คุณสามารถสร้างพาร์ติชันระบบทำงานประจำ (production partition) เดี่ยว หนึ่งพาร์ติชันในพาร์ติชันหลัก (primary partition). แต่สำหรับพาร์ติชันระบบทำงานประจำแบบหลายพาร์ติชัน, โปรดดูที่ *การสร้างสภาวะแวดล้อมของพาร์ติชันระบบทำงานประจำแบบหลายพาร์ติชัน*ข้างล่างนี้.

  ลอจิคัลพาร์ติชันหนึ่งๆ เป็นได้ทั้งพาร์ติชันทดสอบหรือพาร์ติชันของระบบทำงานประจำำอย่างใดอย่างหนึ่ง. พาร์ติชันระบบทำงานประจำรันแอ็พพลิเคชันที่เป็นงานหลักของคุณ. ความล้มเหลวที่เกิดขึ้นในพาร์ติชันระบบทำงานประจำ ขัดขวางการดำเนินการที่สำคัญ และเป็นเหตุให้เสียเวลา และเสียเงิน. พาร์ติชันทดสอบทำหน้าที่ทดสอบซอฟต์แวร์. ความล้มเหลวที่เกิดขึ้นในพาร์ติชันทดสอบ, ทั้งที่ไม่ได้เตรียมการไว้, จะไม่ส่งผลกระทบต่อการดำเนินงานโดยปกติ.
- **การสร้างสภาวะแวดล้อมให้กับหลายๆ พาร์ติชันระบบทำงานประจำ**: ควรสร้างหลายๆ พาร์ติชันระบบทำงานประจำไว้เฉพาะในพาร์ติชันระดับรองๆ ลงไปเท่านั้น. ในสถานการณ์เช่นนี้, คุณจะสละ้พาร์ติชันหลักให้กับส่วนของการจัดการของพาร์ติชัน (partition management).
- **Hot backup**: เมื่อพาร์ติชันระดับรองทำการ replicate ไปยังอีกลอจิคัลพาร์ติชันหนึ่งภายในระบบเดียวกัน, การสลับไปทำงานบนพาร์ติชันรองในขณะที่มีความล้มเหลวเกิดขึ้นในพาร์ติชันนั้นจะช่วยให้เกิดการความไม่สะดวกให้น้อยที่สุดเท่าที่จะเป็นไปได้. configuration นี้ยังช่วยลดผลกระทบของการสำรองข้อมูลซึ่งต้องใช้เวลานาน. คุณสามารถทำการออฟไลน์พาร์ติชันสำรองและทำการสำรองข้อมูลของมัน, ในขณะที่ลอจิคัลพาร์ติชันอื่นยังคงดำเนินงานของระบบทำงานประจำต่อไป. คุณจำเป็นจะต้องมีซอฟต์แวร์พิเศษในการใช้กลยุทธ์ hot backup นี้.
- **คลัสเตอร์รวม (Integrated cluster)**: การใช้ OptiConnect/400, และแอ็พพลิเคชันซอฟต์แวร์ที่สร้าง high availability ให้ระบบ, ทำให้ระบบที่ถูกแบ่งพาร์ติชันเอาไว้ของคุณสามารถรันเป็น

แบบคลัสเตอร์รวมได้. คุณสามารถใช้คลัสเตอร์รวมในการป้องกันระบบของคุณจากความล้มเหลวที่เกิดขึ้นแบบไม่ได้คาดคิดส่วนใหญ่ที่เกิดขึ้นภายในพาร์ติชันระดับรองได้.

หมายเหตุ: เมื่อจัดเตรียมพาร์ติชันระดับรอง, จำเป็นจะต้องมีการพิจารณาเพิ่มเติมในเรื่องตำแหน่งของการ์ด.ถ้า Input/Output Processor (IOP) ที่คุณเลือกสำหรับคอนโซลนั้นมีการ์ด LAN อยู่แล้วและการ์ด LAN นั้นไม่ได้มีไว้สำหรับ การใช้งานร่วมกับ Operations Console, การ์ดนั้นจะถูกเรียกให้ทำงานโดยคอนโซล และคุณอาจจะไม่สามารถใช้การ์ดนั้นเพื่อจุดประสงค์อื่นที่ต้องการ. สำหรับข้อมูลเพิ่มเติมในเรื่องการทำงานกับ Operations Console, ดูได้ใน บทที่ 8, “iSeries Operations Console”, ในหน้า 75.

อ้างอิงถึง ″Logical Partitions″ ใน iSeries Information Center สำหรับข้อมูลเพิ่มเติมในหัวข้อนี้.

การจัดการการรักษาความปลอดภัยสำหรับโลจิคัลพาร์ติชัน

งานที่เกี่ยวข้องกับความปลอดภัยที่กระทำในระบบที่มีการแบ่งพาร์ติชัน จะเหมือนกันกับในระบบทีไม่มีลอจิคัลพาร์ติชัน. อย่างไรก็ตาม, เมื่อคุณสร้างลอจิคัลพาร์ติชัน, คุณจะทำงานกับระบบอิสระที่มากกว่าหนึ่งระบบ. ดังนั้นคุณจะต้องทำงานแบบเดียวกัน ในแต่ละลอจิคัลพาร์ติชัน แทนที่จะทำงานเพียงครั้งเดียว ในระบบที่ไม่มีลอจิคัลพาร์ติชัน.

ต่อไปนี้คือ กฎพื้นฐานบางข้อที่ต้องจดจำไว้ เมื่อกระทำการที่เกี่ยวข้องกับความปลอดภัยบนลอจิคัลพาร์ติชัน:

- เพิ่มผู้ใช้ให้กับระบบ ครั้งละหนึ่งลอจิคัลพาร์ติชัน. คุณจำเป็นต้องเพิ่มผู้ใช้ให้กับแต่ละพาร์ติชันที่ต้องการให้ผู้ใช้เข้าไปใช้งานได้.
- จำกัดจำนวนของผู้ที่มีสิทธิที่จะเข้าไปยัง dedicated service tools (DST) และ system service tools (SST) บนพาร์ติชันหลัก.อ้างอิงถึงหัวข้อ ″Manage logical partitions by using iSeries Navigator, DST and SST″ ใน iSeries Information Center สำหรับ ข้อมูลเกี่ยวกับ DST และ SST. โปรดดูที่ “การจัดการเซอร์วิสทูลต่างๆ” ในหน้า 67 สำหรับข้อมูลเรื่องการใช้โปรไฟล์ผู้ใช้เซอร์วิสทูล เพื่อควบคุมการเข้าถึงการทำงานในพาร์ติชัน.

  หมายเหตุ: คุณต้องทำการ initialize ค่า Service Tools Server (STS) ก่อนการใช้ iSeries Navigator ในการเข้าถึงฟังก์ชัน LPAR. โปรดดูที่ iSeries Information Center—>Security—>Service tools สำหรับข้อมูลที่เกี่ยวข้อง. โปรดดูที่ “สิ่งที่ต้องรู้ก่อนและข้อมูลที่เกี่ยวข้อง” ในหน้า xiii สำหรับข้อมูลในการเข้าไปใช้งานในiSeries Information Center.
- พาร์ติชันระดับรองไม่สามารถมองเห็นหรือใช้แหล่งเก็บข้อมูลหลักและดิสก์ยูนิตของอีกลอจิคัลพาร์ติชันหนึ่งได้.
- พาร์ติชันระดับรองสามารถมองเห็นเพียงรีซอร์สทางฮาร์ดแวร์ของตัวมันเองเท่านั้น.
- พาร์ติชันหลักสามารถมองเห็นรีซอร์สทางฮาร์ดแวร์ของระบบทั้งหมดในหน้าจอ Work with System Partitions ของ DST และ SST.
- ระบบปฏิบัติการของพาร์ติชันหลักยังคงมองเห็นเพียงรีซอร์สของตัวมันเองที่สามารถใช้งานได้เท่านั้น.

- คอนโทรลพาเนลของระบบทำการควบคุมพาร์ติชันหลัก. เมื่อคุณตั้งค่าโหมดของพาเนลให้เป็น Secure, จะไม่สามารถกระทำการใดๆ บนหน้าจอ Work with Partition Status จาก SST ได้. ในการบังคับใช้ DST จากคอนโทรลพาเนลของระบบ, คุณจะต้องเปลี่ยนโหมดให้เป็น Manual.
- เมื่อคุณกำหนดโหมดการปฏิบัติการของพาร์ติชันระดับรองให้เป็น secure, คุณได้จำกัดการใช้งานของ Work with Partition Status ด้วยวิธีการเหล่านี้:
  - คุณสามารถใช้เพียง DST บนพาร์ติชันระดับรองเท่านั้น ในการเปลี่ยนสถานะของพาร์ติชัน; คุณไม่สามารถใช้ SST ในการเปลี่ยนสถานะของพาร์ติชัน.
  - คุณสามารถบังคับใช้ DST บนพาร์ติชันระดับรองจากหน้าจอ Work with Partition Status โดยการใช้ DST หรือ SST ของพาร์ติชันหลักเท่านั้น.
  - คุณสามารถใช้ได้เพียง DST บนพาร์ติชันหลักเท่านั้น ในการเปลี่ยนโหมดของพาร์ติชันระดับรอง จากค่า secure ไปเป็นค่าอื่นใดๆ .

เมื่อโหมดของพาร์ติชันระดับรองไม่เป็น secure, คุณสามารถใช้ได้ทั้ง DST และ SST บนพาร์ติชันรองในการเปลี่ยนสถานะของพาร์ติชัน.

สำหรับข้อมูลเพิ่มเติมเกี่ยวกับการรักษาความปลอดภัยบนเซิร์ฟเวอร์ iSeries, ให้อ้างอิงถึงหนังสืออ้างอิงเกี่ยวกับการรักษาความปลอดภัย และ การรักษาความปลอดภัยระดับต้น และ หน้าที่เกี่ยวกับการวางแผนของ iSeries Information Center.

บทที่ 8. iSeries Operations Console

Operations Console อนุญาตให้คุณใช้พีซีของคุณในการเข้าถึงและควบคุมเซิร์ฟเวอร์ iSeries ของคุณ. คอนโซลของการดำเนินการจะรวมเอาการสนับสนุนสำหรับพีซีรีโมตที่ dial-in ไปยังเซิร์ฟเวอร์ iSeries โดยจะไม่มีอุปกรณ์คอนโซล, ซึ่งอนุญาตให้พีซีรีโมตในการกลายเป็นคอนโซล. เมื่อคุณใช้ Operations Console, ให้สังเกตสิ่งต่างๆ ต่อไปนี้:

- คุณสามารถทำงานใดๆ ที่คุณทำได้จากคอนโซลแบบดั้งเดิมบน Operations Console. ตัวอย่าง เช่น, โปรไฟล์ผู้ใช้ที่มีสิทธิพิเศษ *SERVICE หรือ *ALLOBJ สามารถที่จะ sign on ไปยังเซสชันของ Operations Console, แม้ว่าจะถูกไม่ให้ทำงานก็ตาม.
- Operations Console ใช้ Service Tools User Profiles และรหัสผ่านเพื่อทำให้สามารถเชื่อมต่อไปยังเซิร์ฟเวอร์ iSeries ได้. ซึ่งทำให้การเปลี่ยนแปลง Service Tools User Profiles และรหัสผ่านของคุณมีความสำคัญมาก. นักเจาะระบบมักจะคุ้นเคยกับค่าดีฟอลต์ของเซอร์วิสทูลสำหรับโปรไฟล์ผู้ใช้อันได้แก่ userid และ รหัสผ่าน, และสามารถใช้ในการที่จะทำให้เกิดเซสชันรีโมตคอนโซลไปยังเซิร์ฟเวอร์ iSeries ของคุณ. ดูที่ “การเปลี่ยนแปลงรหัสผ่านที่รู้จักแล้ว” ในหน้า 21 และ “หลีกเลี่ยงการใช้รหัสผ่านดีฟอลต์” ในหน้า 27 สำหรับคำแนะนำในเรื่องของรหัสผ่าน.
- เพื่อป้องกันข้อมูลของคุณเมื่อใช้ Remote Console, ให้ใช้อ็อพชัน call back ของ Windows Dial-Up Networking.
- เมื่อจัดเตรียมพาร์ติชันรอง, จำเป็นต้องมีการพิจารณาเพิ่มเติมในเรื่องตำแหน่งของการ์ด. ถ้า Input/Output Processor (IOP) ที่คุณเลือกเป็นคอนโซลมีการ์ด LAN card และการ์ด LAN นั้นไม่ได้กำหนดไว้สำหรับการใช้งานกับ Operations Console, จะมีการเรียกการ์ดนั้นทำงานสำหรับคอนโซล และคุณอาจไม่สามารถใช้การ์ดนั้นในจุดประสงค์อื่น.

ใน V5R1, มีการพัฒนา Operations Console ที่ให้กิจกรรมของคอนโซลสามารถกระทำข้าม local area network (LAN) ได้. การพิสูจน์ตัวจริงและการเข้ารหัสข้อมูลที่พัฒนาขึ้น ทำให้กระบวนการของคอนโซลมีความปลอดภัยด้านเครือข่าย. เพื่อที่จะใช้ Operations Console with LAN connectivity, คุณควรที่จะติดตั้งผลิตภัณฑ์ต่อไปนี้เป็นอย่างยิ่ง:

- ผู้ให้บริการ Cryptographic Access Provider, 5722-AC2 หรือ 5722-AC3 บนระบบ iSeries
- Client Encryption, 5722-CE2 หรือ 5722-CE3 บน Operations Console PC ของคุณ

เพื่อที่จะให้ข้อมูลในคอนโซลถูกเข้ารหัส, เซิร์ฟเวอร์ iSeries ต้องมีผลิตภัณฑ์ของ Cryptographic Access Provider product ติดตั้งอยู่ **และ** พีซีจะต้องมีผลิตภัณฑ์ของ Client Encryption products ติดตั้งอยู่ .

หมายเหตุ: หากไม่มีการติดตั้งผลิตภัณฑ์ในการเข้ารหัส, ก็จะไม่มีข้อมูลใดถูกเข้ารหัส.

ตารางต่อไปนี้เป็นการสรุปผลของการเข้ารหัสของผลิตภัณฑ์ที่มีอยู่ในปัจจุบัน:

ตารางที่ 13. ผลลัพธ์ของการเข้ารหัส

ผู้ให้บริการการเข้าถึงแบบ Cryptographic บนเซิร์ฟเวอร์ iSeries ของคุณ	Client Encryption บนพีซี Operations Console ของคุณ	ผลลัพธ์ในการเข้ารหัสข้อมูล
None	None	None
5722–AC2	5722–CE2	56 บิต
5722–AC2	5722–CE3	56 บิต
5722–AC3	5722–CE2	56 บิต
5722–AC3	5722–CE3	128 บิต

สำหรับข้อมูลเพิ่มเติมเกี่ยวกับการตั้งค่า และการบริหารระบบ iSeries Operations Console, โปรดดูที่ iSeries Information Center.

Operations Console ภาพรวมของการรักษาความปลอดภัย

ความปลอดภัยของ Operations Console ประกอบด้วย:

- การพิสูจน์อุปกรณ์คอนโซล (console device authentication)
- การพิสูจน์ผู้ใช้ (user authentication)
- ความเป็นส่วนตัวของข้อมูล (data privacy)
- integrity ของข้อมูล (data integrity)

Operations Console ที่มีภาวะเชื่อมต่อโดยตรงมีการพิสูจน์อุปกรณ์โดยนัย, ความเป็นส่วนตัวของข้อมูล, และ integrity ของข้อมูล เนื่องจากมีการเชื่อมต่อแบบ point–to–point. การพิสูจน์ผู้ใช้จำเป็นต้องใช้ในการ sign on ไปยังหน้าจอของคอนโซล.

การตรวจสอบอุปกรณ์คอนโซล

การพิสูจน์อุปกรณ์คอนโซลเป็นการยืนยันว่า อุปกรณ์เชิงฟิสิคัลใดคือคอนโซล. Operations Console ที่มีภาวะเชื่อมต่อโดยตรงใช้การเชื่อมต่อทางฟิสิคัลเหมือนกันกับคอนโซล twinaxial. Operations Console ที่ใช้การเชื่อมต่อโดยตรงอาจมีความปลอดภัยทางฟิสิคัลที่เหมือนกับการเชื่อมต่อ twinaxial ในการควบคุมการเข้าถึงอุปกรณ์คอนโซลเชิงฟิสิคัล.

Operations Console with LAN connectivity ใช้ secure sockets layer (SSL) ในเวอร์ชันที่สนับสนุนการพิสูจน์อุปกรณ์และผู้ใช้ แต่ไม่มีการใช้ certificate. สำหรับรูปแบบของการติดต่อนี้, การพิสูจน์อุปกรณ์จะมาจากโปรไฟล์อุปกรณ์ของ service tool. ดูรายละเอียดเพิ่มเติมได้ใน 77.

การพิสูจน์ผู้ใช้

การพิสูจน์ผู้ใช้เป็นการยืนยันผู้ใดที่กำลังใช้อุปกรณ์คอนโซล. ทุกประเด็นที่เกี่ยวข้องกับการพิสูจน์ผู้ใช้มีลักษณะเหมือนกันโดยไม่คำนึงถึงประเภทของคอนโซล.

ความเป็นส่วนตัวของข้อมูล

ความเป็นส่วนตัวของข้อมูล ทำให้เกิดความมั่นใจว่า มีเพียงผู้รับที่กำหนดไว้เท่านั้น ที่จะสามารถอ่านข้อมูลของคอนโซลได้. Operations Console ที่มีภาวะเชื่อมต่อโดยตรงใช้การเชื่อมต่อทางฟิสิคัลที่เหมือนกันกับคอนโซล twinaxial หรือการเชื่อมต่อเครือข่ายที่ปลอดภัยสำหรับภาวะเชื่อมต่อ LAN เพื่อปกป้องข้อมูลของคอนโซล. Operations Console ที่ใช้การเชื่อมต่อโดยตรงมีความเป็นส่วนตัวของข้อมูลที่เหมือนกับการเชื่อมต่อ twinaxial. ถ้าการเชื่อมต่อเชิงฟิสิคัลยังคงปลอดภัย, นั่นคือ ยังคงมีการปกป้องข้อมูลของคอนโซลไว้.

Operations Console with LAN connectivity จะใช้การเชื่อมต่อเครือข่ายที่ปลอดภัย หากมีการติดตั้งผลิตภัณฑ์ในการเข้ารหัสที่เหมาะสม (ACx และ CEx). เซสชันคอนโซลใช้งานการเข้ารหัสที่มีประสิทธิภาพที่สุดที่เป็นไปได้ที่ขึ้นอยู่กับผลิตภัณฑ์การแปลงข้อมูลเป็นโค้ดที่ติดตั้งบน บนเซิร์ฟเวอร์ iSeries และ PC ที่รัน Operations Console.

หมายเหตุ: หากไม่มีการติดตั้งผลิตภัณฑ์ในการเข้ารหัส, ก็จะไม่มีข้อมูลใดถูกเข้ารหัส.

Data integrity

integrity ของข้อมูลทำให้เกิดความมั่นใจว่าไม่มีการเปลี่ยนแปลงของข้อมูลคอนโซล ในเส้นทางที่ไปยังผู้รับ. Operations Console ที่มีภาวะเชื่อมต่อโดยตรงใช้การเชื่อมต่อทางฟิสิคัล ที่เหมือนกันกับคอนโซล twinaxial หรือการเชื่อมต่อเครือข่ายที่ปลอดภัยสำหรับภาวะเชื่อมต่อ LAN เพื่อปกป้องข้อมูลของคอนโซล. Operations Console ที่ใช้การเชื่อมต่อโดยตรงมี integrity ของข้อมูลที่เหมือนกับการเชื่อมต่อ twinaxial. ถ้าการเชื่อมต่อเชิงฟิสิคัลยังคงปลอดภัย, นั่นคือ ยังคงมีการปกป้องข้อมูลของคอนโซลไว้.

Operations Console with LAN connectivity จะใช้การเชื่อมต่อเครือข่ายที่ปลอดภัย หากมีการติดตั้งผลิตภัณฑ์ในการเข้ารหัสที่เหมาะสม (ACx และ CEx). คอนโซลเซสชันใช้งานการเข้ารหัสที่มีประสิทธิภาพที่สุดที่เป็นไปได้ที่ขึ้นอยู่กับ ผลิตภัณฑ์การแปลงข้อมูลเป็นโค้ดที่ติดตั้งอยู่บนเซิร์ฟเวอร์iSeries และ PC ที่รัน Operations Console.

หมายเหตุ: หากไม่มีการติดตั้งผลิตภัณฑ์ในการเข้ารหัส, ก็จะไม่มีข้อมูลใดถูกเข้ารหัส.

Use Operations Console with LAN connectivity

หมายเหตุ: อุปกรณ์ Operations Console ใดๆ สามารถเป็นคอนโซลได้, แต่จะมีเพียงคอนฟิกูเรชันที่อยู่บน LAN เท่านั้นที่จะใช้เซอร์วิสทูลสำหรับโปรไฟล์ผู้ใช้.

เซิร์ฟเวอร์ iSeries จะผลิตออกมาโดยมีโปรไฟล์อุปกรณ์เซอร์วิสทูลที่เป็นค่าดีฟอลต์ของ QCONSOLE ด้วยรหัสผ่านที่เป็นค่าดีฟอลต์ของ QCONSOLE. Operations Console with LAN

connectivity จะเปลี่ยนรหัสผ่านเมื่อการเชื่อมต่อแต่ละครั้งประสบผลสำเร็จ. ดู “การใช้งานวิซาร์ดตั้งค่า Operations Console”สำหรับข้อมูลเพิ่มเติม.

หากต้องการทราบข้อมูลเพิ่มเติมเกี่ยวกับ iSeries Operations Console with LAN connectivity, โปรดดูที่หัวข้อ, การกำหนดคอนโซลการดำเนินการด้วยการเชื่อมต่อแบบ LAN ,ใน Information Center.

การป้องกัน Operations Console with LAN connectivity

เมื่อมีการใช้ Operations Console with LAN connectivity, ขอแนะนำให้ทำตามข้อต่อไปนี้:

- สร้าง service tools device profile อีกชุดด้วยแอ็ตทริบิวต์ของคอนโซล และเก็บข้อมูลโปรไฟล์นั้นไว้ในที่ปลอดภัย.
- ติดตั้ง Cryptographic Access Provider, 5722–AC2 หรือ 5722–AC3 บนเซิร์ฟเวอร์ iSeries ของคุณและ Client Encryption, 5722–CE2 หรือ 5722–CE3 Operations Console PC ของคุณ.
- เลือกรหัสผ่านของข้อมูลอุปกรณ์เซอร์วิสที่สำคัญ.
- ปกป้องพีซี Operations Console ในลักษณะเดียวกันกับการปกป้องคอนโซล twinaxial ของคุณ หรือการปกป้อง Operations Console ที่มีภาวะเชื่อมต่อโดยตรง.

การใช้งานวิซาร์ดตั้งค่า Operations Console

setup wizard จะเพิ่มข้อมูลที่จำเป็นให้กับพีซีที่ใช้ Operations Console with LAN connectivity. setup wizard จะถามถึง service tools device profile, รหัสผ่านของ service tools device profile, และรหัสผ่านเพื่อปกป้องข้อมูล service tools device profile.

หมายเหตุ: รหัสผ่านของข้อมูล service tools device profile ใช้ในการล็อกและปลดล็อกข้อมูล service tools device profile (service tools device profile และรหัสผ่าน) บนพีซี.

เมื่อมีการสร้างการเชื่อมต่อของเครือข่าย, Operations Console setup wizard จะแสดงพร้อมต์ให้คุณป้อนรหัสผ่านของข้อมูล service device เพื่อเข้าถึง service tools device profile และรหัสผ่านที่มีการเข้ารหัสไว้. และจะมีการแสดงพร้อมต์สำหรับค่า user ID และรหัสผ่านที่ถูกต้องของ service tools.

บทที่ 9. การตรวจพบโปรแกรมที่น่าสงสัย

แนวโน้มใหม่ในเรื่องการใช้คอมพิวเตอร์ ได้เพิ่มโอกาสที่ระบบของคุณจะมีโปรแกรม มาจากแหล่งที่ไม่น่าเชื่อถือ หรือโปรแกรมที่มีการทำงานที่เราไม่ทราบ. ต่อไปนี้คือตัวอย่าง:

- ผู้ใช้เครื่องคอมพิวเตอร์ส่วนบุคคล บางครั้งได้รับโปรแกรมจากผู้ใช้พีซี เครื่องอื่น. ถ้าพีซีถูกพ่วงติดอยู่กับระบบ iSeries ของคุณ, โปรแกรมนั้นสามารถส่งผลกระทบต่อเซิร์ฟเวอร์ iSeries ของคุณได้.
- ผู้ใช้ที่เชื่อมต่อกับเครือข่ายสามารถได้รับโปรแกรม ตัวอย่างเช่น จากกระดาน ข่าวสาร (bulletin board).
- นักเจาะระบบมีความเคลื่อนไหวมากขึ้นและเป็นที่รู้จัก. พวกเขามักจะเผยแพร่วิธีการและผลลัพธ์ของเขา. ซึ่งอาจทำให้เกิดการเลียนแบบจากโปรแกรมเมอร์ซึ่งปกติ เป็นผู้ที่เคารพกฎหมาย.

แนวโน้มนำไปสู่ปัญหาในความปลอดภัยของคอมพิวเตอร์ที่เรียกว่า **ไวรัสคอมพิวเตอร์ (computer virus)**. ไวรัส คือโปรแกรม ที่สามารถเปลี่ยนโปรแกรมอื่น ซึ่งรวมถึงการก็อบปีตัวเอง. โปรแกรมอื่นที่ถูกกระทำ จะเรียกว่าติดไวรัส. นอกเหนือจากนั้น, ไวรัสสามารถทำงานบางอย่างที่ใช้รีซอร์ส ของระบบ หรือทำลายข้อมูล.

สถาปัตยกรรมของเซิร์ฟเวอร์ iSeries จะมีการปกป้องการลักษณะการติดไวรัสคอมพิวเตอร์. “การปกป้องไวรัสคอมพิวเตอร์”อธิบายเรื่องนี้. ผู้บริหารความปลอดภัยของเซิร์ฟเวอร์ iSeries จำเป็นที่จะต้องให้ความใส่ใจเกี่ยวกับโปรแกรมที่กระทำฟังก์ชันที่ไม่ได้รับอนุญาต. หัวข้อที่เหลือในบทนี้จะอธิบายถึงวิธีการที่บุคคลที่ประสงค์ร้ายอาจจัดเตรียม โปรแกรมที่สามารถทำอันตรายมาทำงานในระบบของคุณ. รวมทั้งให้คำแนะนำสำหรับการป้องกัน โปรแกรมจากการทำฟังก์ชันที่ไม่ได้รับอนุญาต.

Security tip

สิทธิอ็อบเจ็กต์มักจะเป็นด่านแรกในการป้องกันของคุณ. ถ้าคุณไม่มีแผนที่ดี สำหรับการป้องกันอ็อบเจ็กต์ของคุณ, ระบบของคุณก็จะไม่มีการป้องกันเลย. ข้อมูลนี้จะกล่าวถึงวิธีที่ผู้ใช้ที่มีสิทธิอาจลองใช้ประโยชน์ของ loop-holes ในรูปแบบของสิทธิอ็อบเจ็กต์.

การปกป้องไวรัสคอมพิวเตอร์

คอมพิวเตอร์ที่ติดไวรัสมีโปรแกรมที่สามารถเปลี่ยนโปรแกรมอื่นได้. สถาปัตยกรรม แบบอ็อบเจ็กต์ของ iSeries ทำให้เป็นการยากที่ผู้ประสงค์ร้ายจะสร้างและกระจายไวรัสชนิดนี้ มากกว่าที่จะทำกับสถาปัตยกรรมคอมพิวเตอร์แบบอื่นๆ . บนเซิร์ฟเวอร์ iSeries นี้, คุณสามารถใช้คำสั่งและวิธีการโดยเฉพาะในการทำงานกับอ็อบเจ็กต์แต่ละชนิด. คุณไม่สามารถใช้คำสั่งเครื่อง เกี่ยวกับไฟล์เพื่อเปลี่ยนแปลงอ็อบเจ็กต์โปรแกรมที่ทำงานได้ (operable program object) ซึ่งเป็นสิ่งที่ผู้สร้าง

ไวรัสส่วนใหญ่ทำ. และคุณก็ไม่สามารถที่จะสร้างโปรแกรม ที่เปลี่ยนโปรแกรมอ็อบเจ็กต์อื่นได้ง่ายๆ. ในการทำเช่นนี้จะต้องใช้เวลา, ความพยายาม และความเชี่ยวชาญมาก และยังต้องการการเข้าถึงเครื่องมือและเอกสารที่ ไม่สามารถหาได้โดยทั่วไป.

อย่างไรก็ตาม, ดังที่ฟังก์ชันของเซิร์ฟเวอร์ iSeries ใหม่ได้ถูกนำมาใช้ในสภาวะแวดล้อมแบบระบบเปิด, บางส่วนของฟังก์ชันที่มีการปกป้องแบบ object-based ของเซิร์ฟเวอร์ iSeries ก็ไม่สามารถใช้งานได้อีกต่อไป. ตัวอย่างเช่น, ด้วย integrated file system (IFS), ผู้ใช้สามารถดำเนินการเกี่ยวกับอ็อบเจ็กต์ในไดเร็กทอรี่โดยตรง, อาทิเช่นไฟล์ stream.

ทั้งนี้, ถึงแม้ว่าสถาปัตยกรรมของเซิร์ฟเวอร์ iSeries จะทำให้ไวรัสแพร่กระจายไประหว่างโปรแกรมในเซิร์ฟเวอร์ iSeries ได้ยาก, สถาปัตยกรรมของมันก็ไม่ได้ป้องกันเซิร์ฟเวอร์ iSeries จากการเป็นพาหะของไวรัส. ดังเช่นไฟล์เซิร์ฟเวอร์, เซิร์ฟเวอร์ iSeries สามารถเก็บโปรแกรมที่มีผู้ใช้พีซีหลายๆ คนใช้ร่วมกันอยู่. โปรแกรมใดโปรแกรมหนึ่งอาจจะมีไวรัสที่เซิร์ฟเวอร์ iSeries ไม่สามารถตรวจพบได้. เพื่อป้องกัน ไวรัสประเภทนี้จากเครื่องพีซีที่มีไวรัสและต่อเข้ากับเซิร์ฟเวอร์ iSeries ของคุณ, คุณต้องใช้ซอฟต์แวร์สแกนไวรัสของพีซี.

ฟังก์ชันหลายๆ ฟังก์ชันที่มีอยู่บนเซิร์ฟเวอร์ iSeries เพื่อการป้องกันบุคคลใดๆจากการใช้ภาษาระดับต่ำที่มีความสามารถเป็นตัวชี้ในการเปลี่ยนแปลงโปรแกรมเชิงอ็อบเจ็กต์ที่ปฏิบัติการได้:

- ถ้าระบบของคุณทำงานที่ระดับความปลอดภัย 40 หรือสูงกว่า, integrity protection จะมีการป้องการเปลี่ยนแปลงโปรแกรมอ็อบเจ็กต์รวมอยู่ด้วย. ตัวอย่างเช่น, คุณไม่สามารถรันโปรแกรมที่มีคำสั่งเครื่องที่ blocked หรือ protected ไว้ได้.
- ค่าของการตรวจสอบโปรแกรมนั้นมีไว้เพื่อปกป้อง คุณเมื่อคุณเรียกคืนโปรแกรมที่บันทึก (และมีการเปลี่ยนแปลง) ไว้ในระบบอื่น. บทที่ 2 ในหนังสือ *iSeries Security Reference* อธิบายถึงฟังก์ชัน integrity protection ที่ระดับความปลอดภัย 40 และสูงกว่า, รวมถึงค่าการตรวจสอบโปรแกรม.

  หมายเหตุ: ค่าการตรวจสอบโปรแกรมไม่ใช่ว่าจะให้ความปลอดภัยเต็มที่, และไม่ใช่การแทนที่ ความระมัดระวังในการประเมินโปรแกรมที่ถูกเรียกคืนมายังระบบของคุณ.

มีเครื่องมือหลายตัวที่ช่วยเหลือคุณตรวจจับการนำโปรแกรมที่ถูกเปลี่ยนแปลง เข้าสู่ระบบของคุณ:

- คุณสามารถใช้คำสั่ง Check Object Integrity (CHKOBJITG) เพื่อสแกนอ็อบเจ็กต์ (ที่ทำงานได้) ที่ตรงกับค่าที่คุณค้นหา เพื่อให้มั่นใจว่าอ็อบเจ็กต์เหล่านี้ ไม่ได้ถูกเปลี่ยนแปลง. ซึ่งจะเหมือนกันกับฟังก์ชันสแกนไวรัส.
- คุณสามารถใช้ฟังก์ชันการตรวจสอบความปลอดภัยเพื่อเฝ้าสังเกตโปรแกรมที่ ถูกเปลี่ยนแปลงหรือถูกเรียกคืน. ค่า *PGMFAIL, *SAVRST, และ *SECURITY สำหรับค่าระดับของสิทธิ (authority level) จะให้ บันทึกการตรวจสอบที่สามารถช่วยคุณตรวจจับความพยายามที่จะนำโปรแกรมประเภทไวรัสเข้าสู่ ระบบของคุณ. ในบทที่ 9 และภาคผนวก F ของหนังสือ *iSeries Security Reference* มีข้อมูลเพิ่มเติมเกี่ยวกับค่าการตรวจสอบและรายการในเจอร์นัลตรวจสอบ.
- คุณสามารถใช้พารามิเตอร์ force create (FRCCRT) ของคำสั่ง Change Program (CHGPGM) เพื่อสร้างโปรแกรมใดๆ ที่ถูก เรียกคืนมายังระบบของคุณใหม่. ระบบใช้ template ของโปรแกรมในการสร้างโปรแกรมขึ้นมาใหม่. ถ้ามีการเปลี่ยนแปลงโปรแกรมอ็อบเจ็กต์หลังจากที่ถูก

คอมไพล์, ระบบจะสร้างอ็อบเจ็กต์ ที่เปลี่ยนแปลงขึ้นมาใหม่และแทนที่โปรแกรมเดิม. ถ้า template ของโปรแกรมนั้นมีวิธีการใช้ที่ถูกป้องกันเอาไว้, ระบบจะไม่สามารถสร้างโปรแกรมขึ้นมาใหม่ได้.

- คุณสามารถใช้ค่ากำหนดของระบบ QFRCCVNRST (ต้องมีการแปลงค่าในขณะบันทึก) ในการสร้างโปรแกรมใดๆ ขึ้นมาใหม่ ดังที่ถูกเรียกคืนมายังระบบของคุณ. ระบบใช้ template ของโปรแกรมในการสร้างโปรแกรมขึ้นมาใหม่. ค่ากำหนดของระบบนี้มีหลากหลายตัวเลือกสำหรับโปรแกรมที่จะสร้างขึ้นใหม่.
- คุณสามารถใช้ค่ากำหนดของระบบ QVFYOBJRST (verify objects on restore) เพื่อป้องกันการเรียกคืน โปรแกรมที่ไม่มีลายเซ็นดิจิตอลหรือไม่มี ลายเซ็นดิจิตอลที่ถูกต้อง. เมื่อลายเซ็นดิจิตอลไม่ถูกต้อง, นั่นหมายความว่า มีการเปลี่ยนแปลงโปรแกรมนั้นตั้งแต่มีการ sign โดยนักพัฒนาโปรแกรมนั้น. APIs ที่มีอยู่อนุญาตให้คุณ sign โปรแกรมของคุณเอง, บันทึกไฟล์, และสตรีมไฟล์.

สำหรับข้อมูลเพิ่มเติมในเรื่องการ sign และวิธีใช้งานเพื่อป้องกัน การโจมตีระบบของคุณ, ดูได้จาก “การ sign อ็อบเจ็กต์” ในหน้า 92.

การมอนิเตอร์การใช้งานของสิทธิที่รับมา

บนเซิร์ฟเวอร์ iSeries , คุณสามารถสร้างโปรแกรมที่รับสิทธิของเจ้าของโปรแกรมมาใช้ได้. ซึ่งหมายความว่า ผู้ใช้ที่เรียกใช้โปรแกรมจะมีสิทธิ (สิทธิไพรเวต และสิทธิพิเศษ) เช่นเดียวกับโปรไฟล์ผู้ใช้ที่เป็นเจ้าของโปรแกรม.

สิทธิที่รับมา (adopted authority) เป็นเครื่องมือด้านความปลอดภัยที่มีค่า ถ้ามีการใช้งานอย่างถูกต้อง. “การเพิ่มประสิทธิภาพให้กับเมนูแอ็คเซสคอนโทรลด้วยความปลอดภัยของอ็อบเจ็กต์” ในหน้า 49, เป็นตัวอย่างของการอธิบาย วิธีการที่รวมสิทธิที่รับมาและเมนูที่ช่วยเหลือคุณให้อยู่เหนือการควบคุมการเข้าถึงเมนู. คุณสามารถใช้สิทธิที่รับมาป้องกันไฟล์ที่สำคัญของคุณจากการเปลี่ยนแปลงภายนอก แอ็พพลิเคชันโปรแกรมที่คุณอนุญาต ในขณะที่คุณยังอนุญาตให้สอบถามข้อมูลในไฟล์ได้.

ในฐานะผู้บริหารความปลอดภัย, คุณต้องแน่ใจว่ามีการใช้สิทธิที่รับมาอย่างเหมาะสม:

- โปรแกรมควรรับสิทธิของโปรไฟล์ผู้ใช้ที่มีสิทธิเพียงพอต่อการทำงานที่จำเป็น, ไม่ใช่สิทธิที่มากเกินไป. คุณต้องให้ความสังเกตเป็นพิเศษกับโปรแกรมที่รับเอาสิทธิ ของโปรไฟล์ผู้ใช้ที่มีสิทธิพิเศษ *ALLOBJ หรือเป็นเจ้าของอ็อบเจ็กต์ที่สำคัญ.
- โปรแกรมที่รับสิทธิมาต้องมีฟังก์ชันที่เฉพาะ, และจำกัด และต้องไม่สามารถป้อน คำสั่งได้.
- โปรแกรมที่รับสิทธิมาจะต้องมีความปลอดภัยที่เหมาะสม.
- การใช้สิทธิที่รับมามากเกินไป อาจมีผลกระทบทางลบต่อประสิทธิภาพของระบบคุณ. เพื่อช่วยคุณหลีกเลี่ยงปัญหาด้านประสิทธิภาพ, ให้ตรวจสอบโฟลว์ชาร์ตการตรวจสอบสิทธิ (authority-checking flowchart) และคำแนะนำในการใช้สิทธิที่รับมาอยู่ในบทที่ 5 ของหนังสือ *iSeries Security Reference* .

อ็อพชันของเมนู SECBATCH:
1 *เพื่อส่งงานทันที* 40 เพื่อใช้ตารางเวลางาน

คุณสามารถใช้คำสั่ง Print Adopting Objects (PRTADPOBJ) หรือ (อ็อพชัน 21 ใน เมนู SECTOOLS) ช่วยคุณเฝ้าสังเกตการใช้สิทธิที่รับมาในระบบของคุณ.

รายงานแสดงสิทธิพิเศษของโปรไฟล์ผู้ใช้ที่ถูกระบุไว้,โปรแกรมที่รับสิทธิของโปรไฟล์ผู้ใช้มานั้น, เช่นเดียวกันกับอุปกรณ์ ASP ที่ใช้สิทธิที่เป็นของโปรไฟล์นั้นๆ . หลังจากที่คุณได้เริ่มมีข้อมูลพื้นฐานของคุณแล้ว, คุณสามารถรันรายงานใน เวอร์ชันส่วนที่เปลี่ยนแปลง (changed version) ของอ็อบเจ็กต์ที่รับสิทธิมา ได้เป็นประจำ. โดยจะแสดงรายการของโปรแกรมใหม่ที่รับสิทธิมา และโปรแกรมที่ ถูกเปลี่ยนเพื่อรับสิทธิมาตั้งแต่คุณรันรายงานเมื่อครั้งก่อน.

ถ้าคุณสงสัยว่าสิทธิที่รับมาจะถูกใช้โดยไม่ถูกต้องในระบบของคุณ, คุณสามารถกำหนด ค่าของระบบ QAUDLVL ให้มีค่า *PGMADP รวมอยู่ด้วย. เมื่อค่านี้แอ็คทีฟ, ระบบจะสร้างรายการเจอร์นัลตรวจสอบเมื่อมี ผู้เริ่มหรือสิ้นสุดโปรแกรมที่รับสิทธิมา. ในรายการจะมีชื่อของผู้ใช้ที่เริ่มโปรแกรม และชื่อโปรแกรมรวมอยู่ด้วย.

การจำกัดการใช้งานของสิทธิที่รับมา

เมื่อโปรแกรม iSeries ทำงาน, โปรแกรมสามารถใช้สิทธิที่รับมาในการเข้าถึงอ็อบเจ็กต์ ได้สองวิธี:

- ตัวโปรแกรมเองสามารถได้รับสิทธิจากเจ้าของโปรแกรม. โดยการระบุในพารามิเตอร์ user profile (USRPRF) ของโปรแกรมหรือเซอร์วิสโปรแกรม.
- โปรแกรมสามารถใช้ (สืบทอด) สิทธิที่รับมาจากโปรแกรมก่อนหน้าที่ยังคงอยู่ใน call stack ของงาน. โปรแกรมสามารถสืบทอดสิทธิที่รับมาจากโปรแกรมก่อนหน้านี้ ถึงแม้ว่า ตัวโปรแกรมเองจะไม่ได้รับสิทธินั้น. พารามิเตอร์ use adopted authority (USEADPAUT) ของโปรแกรมหรือเซอร์วิสโปรแกรม จะควบคุมโปรแกรมที่สืบทอดสิทธิที่รับมาจากโปรแกรมก่อนหน้านี้ในโปรแกรมสแต็ก.

ต่อไปนี้ เป็นตัวอย่างของการทำงานในการใช้สิทธิที่รับมาจากโปรแกรมก่อนหน้านี้.

สมมุติว่าโปรไฟล์ผู้ใช้ ICOWNER มีสิทธิ *CHANGE ในไฟล์ ITEM และสิทธิพับลิก ในไฟล์ ITEM เป็น *USE.ไม่มีโปรไฟล์ผู้ใช้อื่นที่มีสิทธิที่กำหนดอย่างชัดแจ้งในไฟล์ ITEM. ตารางที่ 14 แสดงแอ็ตทริบิวต์ของสามโปรแกรมที่ใช้ไฟล์ ITEM:

ตารางที่ 14. ตัวอย่างของ Use Adopted Authority (USEADPAUT)

ชื่อโปรแกรม	เจ้าของโปรแกรม	ค่า USRPRF	ค่า USEADPAUT
PGMA	ICOWNER	*OWNER	*YES
PGMB	ICOWNER	*USER	*YES
PGMC	ICOWNER	*USER	*NO

ตัวอย่าง 1–การรับสิทธิ:

1. USERA รันโปรแกรม PGMA.
2. โปรแกรม PGMA พยายามจะเปิดไฟล์ ITEM ด้วยความสามารถในการอัพเดต (update capability).

ผลลัพธ์: ความพยายามประสบผลสำเร็จ. USERA มีสิทธิ *CHANGE เข้าถึงไฟล์ ITEM เนื่องจาก PGMA รับสิทธิจาก ICOWNER.

ตัวอย่างที่ 2–การใช้สิทธิที่รับมา:

1. USERA รันโปรแกรม PGMA.
2. โปรแกรม PGMA เรียกโปรแกรม PGMB.
3. โปรแกรม PGMB พยายามจะเปิดไฟล์ ITEM ด้วยความสามารถในการอัพเดต (update capability).

ผลลัพธ์: ความพยายามประสบผลสำเร็จ. แม้ว่าโปรแกรม PGMB จะไม่ได้รับสิทธิมา (*USRPRF คือ *USER), แต่ยอมให้ใช้สิทธิที่ได้รับมาก่อนหน้านี้ (*USEADPAUT เป็น *YES). โปรแกรม PGMA ยังคงอยู่ในโปรแกรมสแต็ก. ดังนั้น, USERA จะได้สิทธิ *CHANGE เข้าถึงไฟล์ ITEM เนื่องจาก PGMA รับสิทธิจาก ICOWNER.

ตัวอย่างที่ 3–ไม่มีการใช้สิทธิที่รับมา:

1. USERA รันโปรแกรม PGMA.
2. โปรแกรม PGMA เรียกโปรแกรม PGMC.
3. โปรแกรม PGMC พยายามจะเปิดไฟล์ ITEM ด้วยความสามารถในการอัพเดต (update capability).

ผลลัพธ์: ความพยายามล้มเหลว. โปรแกรม PGMC ไม่ได้รับสิทธิ. โปรแกรม PGMC ยังไม่ยอมให้ใช้ให้ใช้สิทธิที่รับมาจากโปรแกรมก่อนหน้านี้. ถึงแม้ว่า PGMA จะยังคงอยู่ใน call stack, แต่ไม่มีการใช้สิทธิที่รับมา.

การป้องกันโปรแกรมใหม่ๆ จากการใช้สิทธิที่รับมา

การผ่านสิทธิที่รับมาไปยังโปรแกรมที่ตามมาในสแต็ก ทำให้โปรแกรมเมอร์ที่มี ความรู้ดีมีโอกาสที่จะสร้างโปรแกรมม้าโทรจัน (Trojan horse program). โปรแกรมม้าโทรจัน สามารถขึ้นกับโปรแกรมก่อนหน้า ในสแต็ก เพื่อรับเอาสิทธิที่ต้องการในการทำสิ่งที่อันตราย. เพื่อป้องกันสิ่งนี้, คุณสามารถจำกัดผู้ใช้ที่ได้รับอนุญาตให้สร้างโปรแกรมที่ใช้สิทธิที่รับมาจาก โปรแกรมก่อนหน้านี้.

เมื่อคุณสร้างโปรแกรมใหม่, ระบบจะตั้งค่าพารามิเตอร์ USEADPAUT เป็น *YES โดยอัตโนมัติ. ถ้าคุณไม่ต้องการให้โปรแกรมสืบทอดสิทธิที่รับมา, คุณต้องใช้คำสั่ง Change Program (CHGPGM) หรือคำสั่ง Change Service Program (CHGSRVPGM) เพื่อกำหนด ค่าพารามิเตอร์ USEADPAUT เป็น *NO.

คุณสามารถใช้ authorization list และใช้ค่ากำหนดของระบบของสิทธิที่รับมา (QUSEADPAUT) ในการควบคุมผู้ที่สามารถสร้างโปรแกรมที่สืบทอดสิทธิที่รับมา. เมื่อคุณระบุชื่อ authorization list ลงในค่ากำหนดของระบบ QUSEADPAUT, ระบบจะใช้ authorization list นี้ในการพิจารณาวิธีการสร้าง โปรแกรมใหม่.

เมื่อผู้ใช้สร้างโปรแกรมหรือเซอร์วิสโปรแกรม, ระบบจะตรวจสอบสิทธิของผู้ใช้ใน authorization list. หากผู้ใช้มีสิทธิ *USE, พารามิเตอร์ USEADPAUT สำหรับ โปรแกรมใหม่parameter จะมีค่าเป็น *YES. สิทธิของผู้ใช้ใน authorization list ไม่สามารถได้มาจาก adopted authority.

authorization list ที่คุณระบุในค่ากำหนดของระบบ QUSEADPAUT ยังควบคุมว่าผู้ใช้ สามารถใช้คำสั่ง CHGxxx เพื่อกำหนดค่า USEADPAUT สำหรับโปรแกรมหรือเซอร์วิสโปรแกรม ได้หรือไม่.

หมายเหตุ:

1. คุณไม่จำเป็นต้องเรียก authorization list QUESADPAUT ของคุณ. คุณสามารถสร้าง authority list โดยใช้ชื่ออื่น. จากนั้น ระบุ authorization list นั้นให้กับค่า QUSEADPAUT. ในคำสั่งของตัวอย่างนี้, แทนค่าชื่อของ authorization list ของคุณ.
2. ค่ากำหนดของระบบ QUSEADPAUT ไม่ส่งผลกระทบกับโปรแกรมที่มีอยู่ในระบบของคุณ. ใช้คำสั่ง CGHPGM หรือ CHGSRVPGM เพื่อกำหนดพารามิเตอร์ USEADPAUT ให้กับโปรแกรม ที่มีอยู่แล้ว.

ในสภาพแวดล้อมที่เข้มงวดมากกว่า: หากคุณต้องการ ให้ผู้ใช้ส่วนใหญ่สร้างโปรแกรมใหม่ด้วยพารามิเตอร์ USEADPAUT ที่กำหนดค่าเป็น *NO, ทำดังต่อไปนี้:

1. กำหนดให้สิทธิพับลิกของ authorization list เป็น *EXCLUDE, โดยพิมพ์ต่อไปนี้ :

   ```
   CHGAUTLE AUTL(QUSEADPAUT) USER(*PUBLIC)
      AUT(*EXCLUDE)
   ```

2. จัดเตรียมผู้ใช้เฉพาะเพื่อสร้างโปรแกรมที่ใช้สิทธิที่รับมาของโปรแกรมก่อนหน้านี้, ให้พิมพ์ดังนี้:

   ```
   ADDAUTLE AUTL(QUSEADPAUT) USER(user-name)
      AUT(*USE)
   ```

ในสภาพแวดล้อมที่เข้มงวดน้อยกว่า: หากคุณต้องการ ให้ผู้ใช้ส่วนใหญ่สร้างโปรแกรมใหม่ ด้วยพารามิเตอร์ USEADPAUT ที่กำหนดค่าเป็น *YES, ทำดังต่อไปนี้:

1. ปล่อยให้สิทธิพับลิกของ authorization list มีค่าเป็น *USE.
2. ป้องกันผู้ใช้บางคนจากการสร้างโปรแกรมที่ใช้สิทธิที่รับมาจากโปรแกรมก่อนหน้านี้, ให้พิพม์ดังนี้:

   ```
   ADDAUTLE AUTL(QUSEADPAUT)
      USER(user-name) AUT(*EXCLUDE)
   ```

การมอนิเตอร์การใช้งานของทริกเกอร์โปรแกรม

DB2® UDB มีขีดความสามารถในการเชื่อมความสัมพันธ์ระหว่างทริกเกอร์โปรแกรมกับ ไฟล์ฐานข้อมูล. ขีดความสามารถด้านทริกเกอร์โปรแกรมเป็นเรื่องปกติในธุรกิจของ ระบบจัดการฐานข้อมูลที่มีขีดความสามารถสูง.

เมื่อคุณโยงความสัมพันธ์ทริกเกอร์โปรแกรมเข้ากับไฟล์ฐานข้อมูล, จะเป็นการระบุว่า เมื่อไรที่ทริกเกอร์โปรแกรมจะทำงาน. ตัวอย่างเช่น, คุณสามารถจัดเตรียมไฟล์คำสั่ง ซื้อของลูกค้ารันทริกเกอร์โปรแกรมเมื่อใดก็ตามที่มีการเพิ่มเร็กคอร์ดใหม่เข้าไปยังไฟล์. เมื่อยอดค้างจ่ายของลูกค้าเกินจำนวนเครดิตที่กำหนด, ทริกเกอร์โปรแกรมจะสามารถ พิมพ์จดหมายเตือนไปยังลูกค้า และส่งข้อความไปยังผู้จัดการลูกหนี้.

ทริกเกอร์โปรแกรมเป็นวิธีการที่มีประสิทธิภาพในการเพิ่มขีดความสามารถของ แอ็พพลิเคชันและในการจัดการกับข้อมูล. แต่ทริกเกอร์โปรแกรมก็ทำให้บุคคลที่มี ความประสงค์ร้ายสามารถสร้าง "ม้าโทรจัน (Trojan horse)" ในระบบของคุณ. โปรแกรมที่เป็นอันตรายอาจอยู่ และรอคอยที่จะทำงาน เมื่อมีบางเหตุการณ์เกิดขึ้น ในไฟล์ฐานข้อมูลในระบบของคุณ.

หมายเหตุ: ในประวัติศาสตร์, ม้าโทรจันเป็นม้า ขนาดใหญ่ที่สร้างจากไม้โดยภายในกลวง เพื่อให้ทหารกรีกอยู่ ภายในนั้น. หลังจากที่ม้าถูกนำเข้าสู่ภายในกำแพงของกรุงทรอย, ทหารได้ปีนออกมา จากม้าและต่อสู้กับชาวทรอย (โทรจัน). ในโลกคอมพิวเตอร์, โปรแกรมที่ซ่อนฟังก์ชัน ที่เป็นอันตรายไว้ มักจะถูกเรียกว่า ม้าโทรจัน.

อ็อพชันของเมนู SECBATCH:

27 *เพื่อส่งงานทันที* 66 *เพื่อใช้ตารางเวลางาน*

เมื่อระบบคุณมาในครั้งแรก, ความสามารถในการเพิ่มทริกเกอร์โปรแกรมให้กับ ไฟล์ฐานข้อมูลถูกจำกัดไว้. ถ้าคุณจัดการสิทธิอ็อบเจ็กต์อย่างระมัดระวัง, ผู้ใช้ทั่วไปจะไม่มีสิทธิเพียงพอที่จะเพิ่มทริกเกอร์โปรแกรมให้กับไฟล์ฐานข้อมูล. (ภาคผนวก D ในหนังสือ *iSeries Security Reference* อธิบายถึงสิทธิที่ต้องการหรือทุกคำสั่ง, รวมถึงคำสั่ง Add Physical File Trigger (ADDPFTRG).

คุณสามารถใช้คำสั่ง Print Trigger Programs (PRTTRGPGM) เพื่อพิมพ์รายชื่อของ ทริกเกอร์โปรแกรมทั้งหมดในไลบรารีที่กำหนดหรือในไลบรารีทั้งหมด.

คุณสามารถใช้รายงานเริ่มต้นเป็นพื้นฐานในการประเมินทริกเกอร์โปรแกรมที่มี อยู่แล้วในระบบของคุณ. จากนั้น, คุณสามารถพิมพ์รายงานส่วนที่เปลี่ยนแปลงเป็นประจำ เพื่อดูว่ามีทริกเกอร์โปรแกรมใหม่ที่เพิ่มเข้าไปในระบบของคุณหรือไม่.

เมื่อคุณประเมินทริกเกอร์โปรแกรม, ให้พิจารณาสิ่งต่อไปนี้:

- ผู้สร้างทริกเกอร์โปรแกรม? คุณสามารถใช้คำสั่ง Display Object Description (DSPOBJD) ในการพิจารณา.
- สิ่งที่โปรแกรมทำ? ในการพิจารณา คุณจะต้องดูในซอร์สโปรแกรม หรือสนทนากับ ผู้สร้างโปรแกรมนี้. ตัวอย่างเช่น, ทริกเกอร์โปรแกรมตรวจสอบว่าใครคือผู้ใช้หรือไม่? อาจเป็นไปได้ว่าทริกเกอร์โปรแกรมรอผู้ใช้คนหนึ่งโดยเฉพาะ (QSECOFR) ในการเข้าถึง รีซอร์สของระบบ.

หลังจากที่คุณมีข้อมูลพื้นฐานแล้ว, คุณสามารถพิมพ์รายงานส่วนที่เปลี่ยนแปลง ได้เป็นประจำ เพื่อสังเกตการเพิ่มทริกเกอร์โปรแกรมใหม่เข้ามาในระบบของคุณ.

การตรวจสอบสำหรับโปรแกรมที่ซ่อนอยู่

ทริกเกอร์โปรแกรมไม่ใช้วิธีการเดียวที่สามารถนำม้าโทรจันเข้าสู่ระบบของคุณ. ทริกเกอร์โปรแกรมเป็นตัวอย่างหนึ่งของ **โปรแกรมทางออก (exit program)**. เมื่อเหตุการณ์บางอย่างเกิดขึ้น เช่น การอัพเดตไฟล์ในกรณี ของทริกเกอร์โปรแกรม, ระบบจะรันโปรแกรมทางออกที่สัมพันธ์กับเหตุการณ์นั้น.

ตารางที่ 15แสดงถึงตัวอย่างอื่นๆ ของโปรแกรมทางออกที่อาจอยู่ในระบบของคุณ. คุณอาจใช้วิธีการเดียวกันในการประเมินการใช้และสิ่งที่อยู่ในโปรแกรมทางออกเหล่านี้ เช่นเดียวกับที่คุณใช้กับทริกเกอร์โปรแกรม.

หมายเหตุ: ตารางที่ 15ไม่ใช่รายการทั้งหมดของโปรแกรมทางออกที่เป็นไปได้.

.

ตารางที่ 15. โปรแกรมทางออกที่ระบบจัดหาให้

ชื่อโปรแกรม	เมื่อโปรแกรมรัน
ชื่อที่ผู้ใช้กำหนดในเน็ตเวิร์กแอ็ตทริบิวต์ DDMACC.	เมื่อผู้ใช้พยายามจะเปิดไฟล์ DDM ในระบบหรือ ทำการเชื่อมต่อ DRDA .
ชื่อที่ผู้ใช้กำหนดในเน็ตเวิร์กแอ็ตทริบิวต์ PCSACC.	เมื่อผู้ใช้พยายามใช้ฟังก์ชัน Client Access™ โดยใช้ Original Clients เพื่อเข้าถึงอ็อบเจ็กต์ในระบบของคุณ.
ชื่อที่ผู้ใช้กำหนดในค่ากำหนดของระบบ QPWDVLDPGM	เมื่อผู้ใช้รันฟังก์ชัน Change Password.
ชื่อที่ผู้ใช้กำหนดในค่ากำหนดของระบบ QRMTSIGN	เมื่อผู้ใช้พยายาม sign on แบบโต้ตอบจากระบบรีโมต.
QSYS/QEZUSRCLNP	เมื่อฟังก์ชัน automatic cleanup ทำงาน.
ชื่อที่ผู้ใช้กำหนดในพารามิเตอร์ EXITPGM ของคำสั่ง CHGBCKUP.	เมื่อคุณใช้ฟังก์ชันสำรองข้อมูล Operation Assistant.
ชื่อที่ผู้ใช้กำหนดในคำสั่ง CRTPRDLOD.	ก่อนและหลังจากคุณบันทึก, เรียกคืน, หรือลบ ผลิตภัณฑ์ที่ถูกสร้างด้วยคำสั่งนี้.
ชื่อที่ผู้ใช้กำหนดในพารามิเตอร์ DFTPGM ของคำสั่ง CHGMSGD.	ถ้ามีการกำหนดดีฟอลต์โปรแกรมให้กับข้อความ, ระบบ จะรันโปรแกรมนั้นเมื่อมีการแสดงข้อความ. เนื่องจากมีความอธิบายข้อความเป็นจำนวนมาก ในระบบทั่วๆ ไป, การใช้ดีฟอลต์โปรแกรมจะทำให้ยากต่อการเฝ้าสังเกต. เพื่อป้องกัน ผู้ใช้พับลิกไม่ให้เพิ่มดีฟอลต์โปรแกรมให้กับข้อความ, ให้พิจารณาการกำหนดสิทธิพับลิก ให้กับไฟล์ข้อความ (อ็อบเจ็กต์ *MSGF) เป็น *USE.
ชื่อที่ผู้ใช้กำหนดในพารามิเตอร์ FKEYPGM ของคำสั่ง STREML3270.	เมื่อผู้ใช้กดฟังก์ชันคีย์ในเซสชันของ 3270 device emulation. ระบบคืนการควบคุมไปยังเซสชัน 3270 device emulation เมื่อโปรแกรมทางออกสิ้นสุดการทำงาน.
ชื่อที่ผู้ใช้กำหนดในพารามิเตอร์ EXITPGM ของคำสั่งในการเฝ้าสังเกตประสิทธิภาพ	เพื่อประมวลข้อมูลที่เก็บรวบรวมโดยคำสั่งเหล่านี้: STRPFRMON, ENDPFRMON, ADDPFRCOL และ CHGPFRCOL. โปรแกรมจะรันเมื่อการรวบรวมข้อมูลสิ้นสุด.
ชื่อที่ผู้ใช้กำหนดในพารามิเตอร์ EXITPGM ของคำสั่ง RCVJRNE.	สำหรับแต่ละ journal entry หรือกลุ่มของ journal entry ที่อ่านจากเจอร์นัลและ journal receiver ที่กำหนด.

ตารางที่ 15. โปรแกรมทางออกที่ระบบจัดหาให้ (ต่อ)

ชื่อโปรแกรม	เมื่อโปรแกรมรัน
ชื่อที่ผู้ใช้กำหนดใน QTNADDCR API.	ระหว่างการทำ COMMIT หรือ ROLLBACK.
ชื่อที่ผู้ใช้กำหนดใน QHFRGFS API.	เพื่อทำฟังก์ชันของระบบไฟล์.
ชื่อที่ผู้ใช้กำหนดในพารามิเตอร์ SEPPGM ของคำอธิบายอุปกรณ์การพิมพ์	เพื่อพิจารณาสิ่งที่จะพิมพ์ในหน้าตัวแบ่ง (separator page) ก่อนหรือหลังไฟล์ที่เก็บพัก (spooled file) หรืองานพิมพ์.
QGPL/QUSCLSXT	เมื่อไฟล์ฐานข้อมูลถูกปิด เพื่อยอมให้มี การเก็บข้อมูลการใช้ไฟล์.
ชื่อที่ผู้ใช้กำหนดในพารามิเตอร์ FMTSLR ของไฟล์แบบลอจิคัล.	เมื่อมีการเขียนเร็กคอร์ดในไฟล์ฐานข้อมูล และไม่มี ชื่อรูปแบบเร็กคอร์ดรวมอยู่ในโปรแกรมภาษาชั้นสูง. โปรแกรมตัวเลือกได้รับเร็กคอร์ด นั้นเป็นอินพุต, ตรวจสอบรูปแบบเร็กคอร์ดที่ใช้, และส่งคืนกลับไปยังฐานข้อมูล.
ชื่อที่ผู้ใช้กำหนดที่ระบุในค่ากำหนดของระบบ QATNPGM, พารามิเตอร์ ATNPGM ในโปรไฟล์ผู้ใช้, หรือพารามิเตอร์ PGM ของคำสั่ง SETATNPGM.	เมื่อผู้ใช้กดคีย์ Attention.
ชื่อที่ผู้ใช้กำหนดในพารามิเตอร์ EXITPGM ของคำสั่ง TRCJOB.	ก่อนเริ่มต้นโพรซีเดอร์ Trace Job.

สำหรับคำสั่งที่อนุญาตให้คุณกำหนดโปรแกรมทางออก, คุณต้องแน่ใจว่าไม่มีการ เปลี่ยนคำสั่งดีฟอลต์เพื่อกำหนดโปรแกรมทางออก. คุณยังต้องแน่ใจว่าสิทธิพับลิก ของคำสั่งเหล่านี้ไม่เพียงพอที่จะเปลี่ยนคำสั่งดีฟอลต์. คำสั่ง CHGCMDDFT ต้องการ สิทธิ *OBJMGT ในคำสั่ง. คุณไม่จำเป็นต้องมีสิทธิ *OBJMGT เพื่อรันคำสั่ง.

การประเมินผลโปรแกรมทางออกที่ได้รับการลงทะเบียนแล้ว

คุณสามารถใช้ฟังก์ชันการลงทะเบียนของระบบเพื่อลงทะเบียนโปรแกรมทางออกที่ต้องรัน เมื่อมีเหตุการณ์บางเหตุการณ์เกิดขึ้น. เพื่อแสดงรายการของข้อมูลการลงทะเบียนในระบบ ของคุณ, ให้พิมพ์ `WRKREGINF OUTPUT(*PRINT)`. รูปที่ 8 ในหน้า 88 แสดงตัวอย่างของรายงานนี้:

```
                Work with Registration Information
Exit point . . . . . . . . . . . . . . . :   QIBM_QGW_NJEOUTBOUND
Exit point format  . . . . . . . . . . . :   NJE00100
Exit point registered  . . . . . . . . . :   *YES
Allow deregister . . . . . . . . . . . . :   *YES
Maximum number of exit programs  . . . . :   *NOMAX
Current number of exit programs  . . . . :   0
Preprocessing for add  . . . . . . . . . :   *NONE
  Library  . . . . . . . . . . . . . . . :
  Format . . . . . . . . . . . . . . . . :
Preprocessing for remove . . . . . . . . :   *NONE
  Library  . . . . . . . . . . . . . . . :
  Format . . . . . . . . . . . . . . . . :
Preprocessing for retrieve . . . . . . . :   *NONE
  Library  . . . . . . . . . . . . . . . :
```

รูปที่ 8. Work with Registration Information - ตัวอย่าง

สำหรับแต่ละจุดทางออกในระบบ, รายงานจะแสดงว่ามีโปรแกรมทางออกใดบ้างที่ลงทะเบียนได้. เมื่อจุดทางออกมีโปรแกรมที่ลงทะเบียนไว้แล้ว, คุณสามารถเลือกอ็อพชัน 8 (Display programs) จากเวอร์ชันหน้าจอของ WRKREGINF เพื่อแสดงข้อมูลเกี่ยวกับโปรแกรม:

```
                    Work with Registration Information

Type options, press Enter.
5=Display exit point   8=Work with exit programs

                           Exit
     Exit                  Point
Opt  Point                 Format    Registered  Text
     QIBM_QGW_NJEOUTBOUND  NJE00100     *YES     Network Job Entry outbound ex
8    QIBM_QHQ_DTAQ         DTAQ0100     *YES     Original Data Queue Server
     QIBM_QLZP_LICENSE     LICM0100     *YES     Original License Mgmt Server
     QIBM_QMF_MESSAGE      MESS0100     *YES     Original Message Server
     QIBM_QNPS_ENTRY       ENTR0100     *YES     Network Print Server - entry
     QIBM_QNPS_SPLF        SPLF0100     *YES     Network Print Server - spool
     QIBM_QNS_CRADDACT     ADDA0100     *YES     Add CRQ description activity
     QIBM_QNS_CRCHGACT     CHGA0100     *YES     Change CRQ description activi
```

ใช้วิธีการเดียวกันกับที่คุณใช้กับโปรแกรมทางออกอื่นๆ และทริกเกอร์โปรแกรม เพื่อประเมินโปรแกรมทางออกเหล่านี้.

การตรวจสอบโปรแกรมที่ได้กำหนดเวลาเอาไว้

iSeries มีหลายวิธีการในการจัดตารางเวลางานให้ทำงานในภายหลัง, รวมทั้งตารางเวลางาน (job scheduler). โดยปกติ, วิธีการเหล่านี้ไม่ได้ทำให้เกิด การละเมิดความปลอดภัย เนื่องจากผู้ใช้ที่สามารถจัดตารางเวลางานจะต้องมีสิทธิ เดียวกับที่ต้องการในการส่งงานไปยังแบตช์.

อย่างไรก็ตาม, คุณควรที่จะตรวจตารางเวลางานในอนาคตเป็นระยะๆ . ผู้ใช้ที่ไม่พอใจ ซึ่งปัจจุบันไม่ได้ทำงานอยู่ในองค์กรแล้ว อาจใช้วิธีนี้ในการตั้งเวลาที่จะสร้าง ความเสียหาย.

การจำกัดความสามารถในการบันทึกและเรียกคืน

ผู้ใช้ส่วนใหญ่ไม่จำเป็นต้องบันทึกและเรียกคืนอ็อบเจ็กต์ในระบบของคุณ. คำสั่ง save ทำให้เป็นไปได้ที่จะเกิดการสำเนาข้อมูลที่สำคัญขององค์กรคุณไปยังสื่อ หรือระบบอื่น. คำสั่ง save ส่วนใหญ่สนับสนุนการบันทึกไฟล์ที่สามารถจะถูกส่งไป ยังระบบอื่น (โดยการใช้คำสั่งไฟล์ SNDNETF) โดยไม่มีการเข้าถึงสื่อหรืออุปกรณ์ในการบันทึก/เรียกคืน.

คำสั่ง restore ทำให้มีโอกาสที่จะเรียกคืนอ็อบเจ็กต์ที่ไม่ได้รับอนุญาต เช่น โปรแกรม, คำสั่ง หรือไฟล์ เข้าสู่ระบบของคุณ. คุณยังสามารถเรียกคืนข้อมูลโดยไม่มี การเข้าถึงสือหรืออุปกรณ์บันทึก/เรียกคืนโดยการใช้ไฟล์บันทึก (save file). ไฟล์บันทึกสามารถถูกส่งจากระบบอื่นโดยการใช้คำสั่ง SNDNETF หรือโดยใช้ฟังก์ชัน FTP.

ต่อไปนี้เป็นคำแนะนำสำหรับการควบคุมการบันทึกและเรียกคืนในระบบของคุณ:

- ควบคุมผู้ใช้ที่มีสิทธิพิเศษ *SAVSYS. สิทธิพิเศษ *SAVSYS อนุญาตให้ผู้ใช้ บันทึกและเรียกคืนอ็อบเจ็กต์ แม้ว่าผู้ใช้จะไม่มีสิทธิที่จำเป็นต่ออ็อบเจ็กต์นั้น.
- ควบคุมการเข้าถึงทางกายภาพของอุปกรณ์บันทึกและเรียกคืน.
- ควบคุมการเข้าถึงคำสั่ง save และ restore. เมื่อคุณติดตั้ง OS/400 licensed program, สิทธิพับลิกสำหรับคำสั่ง RSTxxx คือ *EXCLUDE. และสิทธิพับลิก SAVxxx คือ *USE. ให้พิจารณาการเปลี่ยนสิทธิพับลิกสำหรับคำสั่ง SAVxxx เป็น *EXCLUDE. และระมัดระวังการจำกัดผู้ใช้ที่คุณอนุญาตให้ใช้คำสั่ง RSTxxx.
- ใช้ค่ากำหนดของระบบ QALWOBJRST เพื่อควบคุมการเรียกคืนของ โปรแกรม system-state, โปรแกรม ที่ได้รับสิทธิมา, และอ็อบเจ็กต์ที่มีข้อผิดพลาดด้านการตรวจสอบ.
- ใช้ค่ากำหนดของระบบ QVFYOBJRST ควบคุมการเรียกคืน signed object ในระบบของคุณ.
- ใช้ค่ากำหนดของระบบ QFRCCVNRST ในการควบคุมการสร้างใหม่ของอ็อบเจ็กต์ที่ชัดเจนที่กำลังถูกเรียกคืนมาบนระบบ.
- ใช้การตรวจสอบความปลอดภัยเพื่อเฝ้าสังเกตการเรียกคืน. รวมทั้ง *SAVRST ในค่ากำหนดของระบบ QAUDLVL, และพิมพ์เร็กคอร์ดการตรวจสอบที่ถูกสร้าง โดยการเรียกคืนอย่างสม่ำเสมอ. (บทที่ 9 และภาคผนวก F ของหนังสือ *iSeries Security Reference* มีข้อมูลเพิ่มเติมเกี่ยวกับการดำเนินการบันทึกการตรวจสอบ.)

การตรวจสอบสำหรับอ็อบเจ็กต์ของผู้ใช้ในไลบรารีที่ได้รับการปกป้องเอาไว้

เซิร์ฟเวอร์ iSeries ทุกตัวมีรายชื่อไลบรารี. รายชื่อไลบรารีจะกำหนดลำดับในการค้นหา อ็อบเจ็กต์หากไม่มีการระบุชื่อไลบรารีให้กับชื่ออ็อบเจ็กต์. ตัวอย่างเช่น, เมื่อคุณเรียก โปรแกรมโดยไม่ ระบุที่อยู่ของโปรแกรม, ระบบจะค้นหารายชื่อไลบรารีของคุณตามลำดับและรันโปรแกรม ที่เป็นก็อปปีแรกที่พบ.

หนังสือ *iSeries Security Reference* มีข้อมูลเกี่ยวกับจุดอ่อนด้าน ความปลอดภัยของรายชื่อไลบรารีและการเรียกโปรแกรมโดยไม่มีชื่อไลบรารี (เรียกว่า **การเรียกที่ไม่เหมาะสม-unqualified call**). และยังมีคำแนะนำ ในการควบคุม สิ่งที่อยู่ในรายชื่อ ไลบรารีและความสามารถในการเปลี่ยนรายชื่อไลบรารีของระบบ.

เพื่อให้ระบบของคุณทำงานอย่างเหมาะสม, บางไลบรารีของระบบ เช่น QSYS และ QGPL จะต้องอยู่ในรายชื่อไลบรารีของทุกงาน. คุณควรใช้สิทธิอ็อบเจ็กต์ควบคุมผู้ที่สามารถ เพิ่มโปรแกรมลงในไลบรารีเหล่านี้. ซึ่งจะช่วยป้องกันไม่ให้มีการใส่โปรแกรมหลอกลวง (imposer program) ในไลบรารีโดยใช้ชื่อเดียวกันกับโปรแกรมที่ปรากฏอยู่ในไลบรารี ที่มาภายหลังในรายชื่อไลบรารี.

คุณควรประเมินผู้ที่มีสิทธิในการใช้คำสั่ง CHGSYSLIBL และเฝ้าสังเกต เร็กคอร์ด SV ในเจอร์นัลการตรวจสอบความปลอดภัย. ผู้ใช้ที่ไม่ประสงค์ดีอาจวาง ไลบรารีไว้ก่อนหน้า QSYS ในรายชื่อไลบรารี และจะทำให้ผู้ใช้อื่นๆ รันคำสั่งที่ ไม่ได้รับอนุญาต โดยการใช้ชื่อเดียวกับคำสั่งที่ IBM จัดหาให้.

อ็อพชันของเมนู SECBATCH:

28 *เพื่อส่งงานทันที* 67 *เพื่อใช้ตารางเวลางาน*

คุณสามารถใช้คำสั่ง Print User Objects (PRTUSROBJ) ในการพิมพ์รายชื่ออ็อบเจ็กต์ของผู้ใช้ (อ็อบเจ็กต์ที่ไม่ได้ถูกสร้างโดย IBM) ที่อยู่ในไลบรารีที่ถูกระบุเอาไว้. จากนั้น คุณสามารถประเมินโปรแกรมในรายชื่อเพื่อพิจารณาหาผู้สร้างและฟังก์ชัน การทำงานของโปรแกรมเหล่านั้น.

อ็อบเจ็กต์ผู้ใช้ที่ไม่ใช่โปรแกรมก็สามารถเป็นจุดอ่อนด้านความปลอดภัยได้ เมื่ออยู่ในไลบรารีของระบบ. ตัวอย่างเช่น, ถ้าโปรแกรมเขียนข้อมูลที่เป็นความลับ ไปยังไฟล์ที่ชื่อไม่เหมาะสม โปรแกรมอาจถูกหลอกให้เปิดเวอร์ชันที่หลอกลวงของ ไฟล์นั้นในไลบรารีระบบ.

บทที่ 10. การป้องกันและการตรวจหาความพยายามในการเจาะทำลายระบบ

ข้อมูลนี้เป็นการรวบรวมคำแนะนำต่างๆ ที่หลากหลาย เพื่อช่วยในการตรวจหาช่องโหว่ในด้านความปลอดภัยที่สามารถเกิดขึ้นได้ รวมไปถึงผู้ที่ประสงค์ร้ายอื่นๆ.

การรักษาความปลอดภัยในด้านกายภาพ

หน่วยของระบบ (system unit) ของคุณเทียบได้กับทรัพย์สินในทางธุรกิจที่มีความสำคัญ และยังเป็นทางเข้าสู่ระบบที่เหลือของคุณได้อีกด้วย. ส่วนประกอบของระบบบางส่วนภายในระบบของคุณนั้น ทั้งมีขนาดเล็กและมีค่า. คุณสมควรที่จะวางหน่วยระบบ (system unit) ในตำแหน่งที่มีการควบคุม เพื่อป้องกันบุคคลอื่นไม่ให้ทำการลบหรือเคลื่อนย้ายส่วนประกอบของระบบที่มีค่าออกไป.

หน่วยของระบบจะมีแผงควบคุม (control panel) ที่มีความสามารถในการทำฟังก์ชันพื้นฐานโดยไม่ต้องมีเวิร์กสเตชัน. ตัวอย่างเช่น, คุณสามารถใช้แผงควบคุมเพื่อทำสิ่งต่อไปนี้:

- หยุดการทำงานของระบบ.
- เริ่มการทำงานของระบบ.
- โหลดระบบปฏิบัติการ.
- เริ่มต้นฟังก์ชันการบริการ (service function).

กิจกรรมทั้งหมดที่กล่าวมานี้สามารถรบกวนผู้ใช้ในระบบของคุณ. และยังเป็นช่องโหว่ในด้านความปลอดภัยของระบบที่เป็นไปได้อีกด้วย. คุณสามารถใช้กุญแจล็อก (keylock) ที่มาพร้อมกับระบบของคุณ เพื่อควบคุมว่า เมื่อใดที่กิจกรรมเหล่านี้จะได้รับอนุญาต. เพื่อป้องกันการใช้แผงควบคุม, ให้หมุนกุญแจล็อกไปยังตำแหน่ง secure, ดึงกุญแจออก, และเก็บไว้ในที่ที่ปลอดภัย.

หมายเหตุ:

1. ถ้าคุณต้องการทำการรีโมต IPL (remote IPL) หรือทำการวินิจฉัยจากระยะไกล (remote diagnostics) ในระบบของคุณ, คุณอาจต้องเลือกค่าติดตั้งอย่างอื่นสำหรับกุญแจล็อกของคุณ. หัวข้อ Getting Started ใน iSeries Information Center จะให้ข้อมูลเพิ่มเติมเกี่ยวกับค่าติดตั้งของกุญแจล็อก (โปรดดูที่ “สิ่งที่ต้องรู้ก่อนและข้อมูลที่เกี่ยวข้อง” ในหน้า xiii สำหรับรายละเอียด).
2. มีบางรุ่นที่กุญแจล็อกไม่ได้มีมาเป็นมาตรฐาน .

การตรวจสอบกิจกรรมของโปรไฟล์ผู้ใช้

โปรไฟล์ผู้ใช้เป็นทางเข้าสู่ระบบของคุณ. พารามิเตอร์ในโปรไฟล์ผู้ใช้เป็น ตัวกำหนดสภาพแวดล้อมของผู้ใช้ ' และคุณลักษณะด้านความปลอดภัยของผู้ใช้ ' . ในฐานะของผู้บริหารความปลอดภัย, คุณจำเป็นต้องควบคุมและตรวจสอบการเปลี่ยนแปลงที่เกิดขึ้นกับโปรไฟล์ผู้ใช้ในระบบของคุณ.

คุณสามารถจัดเตรียมการตรวจสอบความปลอดภัย เพื่อที่ระบบของคุณบันทึกเร็กคอร์ดของการเปลี่ยนแปลงลงในโปรไฟล์ผู้ใช้. คุณสามารถใช้คำสั่ง DSPAUDJRNE เพื่อพิมพ์รายงานของการเปลี่ยนแปลงเหล่านั้น.

คุณสามารถสร้างโปรแกรมทางออก (exit program) เพื่อประเมินผลการกระทำที่ถูกร้องขอไปยังโปรไฟล์ผู้ใช้. ตารางที่ 16แสดง exit point ที่มีไว้สำหรับคำสั่งที่ใช้กับโปรไฟล์ผู้ใช้.

ตารางที่ 16. Exit points สำหรับกิจกรรมที่เกี่ยวกับโปรไฟล์ผู้ใช้

คำสั่งที่เกี่ยวกับโปรไฟล์ผู้ใช้	ชื่อของ exit point
Create User Profile (CRTUSRPRF)	QIBM_QSY_CRT_PROFILE
Change User Profile (CHGUSRPRF)	QIBM_QSY_CHG_PROFILE
Delete User Profile (DLTUSRPRF)	QIBM_QSY_DLT_PROFILE
Restore User Profile (RSTUSRPRF)	QIBM_QSY_RST_PROFILE

ความสามารถของโปรแกรมทางออกของคุณได้แก่ มองหาการเปลี่ยนแปลงที่อาจทำให้ผู้ใช้เรียกใช้โปรแกรมในเวอร์ชันที่ไม่ได้รับอนุญาต. การเปลี่ยนแปลงเหล่านี้อาจเป็นการกำหนดรายละเอียดของงานที่แตกต่างกัน หรือไลบรารีปัจจุบันอันใหม่ อย่างใดอย่างหนึ่ง. โปรแกรมทางออกของคุณอาจเลือกแจ้งให้ทราบผ่านทางคิวข้อความ (message queue) หรือกระทำการบางอย่าง (เช่น การเปลี่ยนแปลงหรือทำให้โปรไฟล์ผู้ใช้ไม่สามารถใช้งานได้) โดยจะขึ้นกับข้อมูลที่โปรแกรมทางออกได้รับ.

หนังสือ *iSeries Security Reference* มีข้อมูลเพิ่มเติมเกี่ยวกับโปรแกรมทางออกสำหรับการทำงานของโปรไฟล์ผู้ใช้.

การ sign อ็อบเจ็กต์

ข้อควรระวังที่เกี่ยวกับความปลอดภัยทั้งหมดที่คุณนำมาใช้จะไม่มีความหมาย ถ้ามีผู้ใดสามารถหลบเลี่ยงเข้าไปได้โดยการนำข้อมูลรบกวนเข้ามาในระบบของคุณ. เซิร์ฟเวอร์ iSeries มีคุณลักษณะพิเศษในตัวหลายอย่าง ซึ่งคุณสามารถใช้ในการกันซอฟต์แวร์รบกวนไม่ให้ถูกโหลดไปไว้บนระบบ, และเพื่อตรวจหาว่ามีซอฟต์แวร์ดังกล่าวอยู่บนระบบแล้วหรือไม่. มีการเพิ่มหนึ่งในเทคนิคเหล่านี้ไว้ใน V5R1 นั่นคือการ sign อ็อบเจ็กต์ (object signing).

การ sign อ็อบเจ็กต์ เป็นการที่เซิร์ฟเวอร์ iSeries นำคอนเซ็ปต์ cryptographic ไปปฏิบัติ ซึ่งรู้จักกันในชื่อของ "ลายเซ็นดิจิตอล (digital signature)." ความคิดนี้เป็นความสัมพันธ์แบบตรงไปตรงมา: เมื่อผู้ผลิตซอฟต์แวร์พร้อมที่จะส่งซอฟต์แวร์ให้กับลูกค้า, ผู้ผลิตจะทำการ "sign" ซอฟต์แวร์นั้น. ลายเซ็นนี้ไม่ได้เป็นการรับประกันว่าซอฟต์แวร์นั้นจะทำฟังก์ชันเฉพาะใดๆ. แต่มันจะใช้เป็นวิธีพิสูจน์ว่าซอฟต์แวร์นั้นมาจากผู้ผลิตที่ sign ซอฟต์แวร์นั้นไว้, และซอฟต์แวร์ไม่มีการเปลี่ยนแปลงใดๆ ตั้งแต่มีการผลิตและการ sign ซอฟต์แวร์เกิดขึ้น. นี่เป็นสิ่งที่มีความสำคัญเป็นอย่างยิ่ง ถ้าหากซอฟต์แวร์ถูกส่งผ่านข้ามอินเตอร์เน็ต หรือถูกบันทึกไว้ในสื่อที่คุณคิดว่าอาจมีการแก้ไขสื่อนั้นได้.

การใช้ลายเซ็นดิจิตอลทำให้คุณสามารถควบคุมในเรื่องของซอฟต์แวร์ที่จะถูกโหลดลงบนระบบของคุณได้มากขึ้น , และยอมให้คุณมีอำนาจมากขึ้นในการตรวจจับการเปลี่ยนแปลงเมื่อมีการโหลดซอฟต์แวร์นั้น. ค่าใหม่ของค่ากำหนดของระบบ Verify Object Restore (QVFYOBJRST) มีวิธี

สำหรับการตั้งค่า policy ที่เข้มงวด โดยต้องการให้ซอฟต์แวร์ทั้งหมดที่ถูกโหลดลงในระบบถูก sign โดยแหล่งที่มาของซอฟต์แวร์ที่เป็นที่รู้จัก. คุณยังสามารถเลือก policy ที่เปิดกว้างกว่านี้และใช้การตรวจสอบลายเซ็นอย่างง่ายได้ด้วย หากมีตัวเลือกเหล่านั้นให้คุณเลือก.

ซอฟต์แวร์ทั้งหมดของ OS/400, เช่นเดียวกันกับซอฟต์แวร์สำหรับอ็อพชันและ ไลเซนส์โปรแกรมของเซิร์ฟเวอร์ iSeries , จะถูก sign โดยซอร์สที่ได้รับความไว้วางใจจากระบบ. ลายเซ็นเหล่านี้ช่วยให้ระบบปกป้อง integrity ของมัน, และจะถูกตรวจสอบเมื่อมีการใช้โปรแกรมฟิกซ์กับระบบ เพื่อให้แน่ใจว่าโปรแกรมฟิกซ์มาจากซอร์สที่ได้รับความไว้วางใจจากระบบ และไม่ถูกเปลี่ยนแปลงในระหว่างการส่งผ่าน. ลายเซ็นเหล่านี้ยังสามารถถูกตรวจสอบได้ เมื่อซอฟต์แวร์อยู่บนระบบ. มีการใช้คำสั่ง CHKOBJITG (Check Object Integrity) เพื่อตรวจสอบลายเซ็น เพิ่มเติมจากคุณลักษณะ integrity อื่นๆ ของอ็อบเจ็กต์ในระบบ. นอกจากนี้, Digital Certificate Manager มีพาเนลที่คุณสามารถใช้ในการตรวจสอบลายเซ็นบนอ็อบเจ็กต์, รวมไปถึงอ็อบเจ็กต์ในระบบปฏิบัติการ.

เมื่อมีการ sign ระบบปฏิบัติการ, คุณควรใช้ลายเซ็นดิจิตอลในการปกป้อง integrity ของซอฟต์แวร์ซึ่งมีความสำคัญอย่างยิ่งต่อธุรกิจของคุณ. คุณอาจซื้อซอฟต์แวร์ที่มีการ sign โดยผู้ให้บริการซอฟต์แวร์, หรือคุณอาจ sign ซอฟต์แวร์ที่คุณได้ซื้อมาหรือเขียนขึ้นเอง. ส่วนหนึ่งของ policy ในด้านความปลอดภัย, ดังนั้น, อาจจะใช้ CHKOBJITG, หรือ Digital Certificate Manager, ในการตรวจสอบอย่างสม่ำเสมอว่า ลายเซ็นบนซอฟต์แวร์นั้นยังคงถูกต้อง — นั่นคือ อ็อบเจ็กต์ไม่ได้ถูกเปลี่ยนแปลง ตั้งแต่มีการ sign ในตอนแรก. คุณอาจต้องการให้ซอฟต์แวร์ทั้งหมดที่มีการกู้คืนในระบบของคุณ ถูก sign โดยคุณหรือซอร์สที่รู้จัก. อย่างไรก็ตาม, เนื่องจากซอฟต์แวร์ของเซิร์ฟเวอร์ iSeries ส่วนใหญ่ ซึ่งไม่ได้ถูกผลิตโดย IBM ยังไม่ได้รับการ sign ในปัจจุบัน, จึงอาจเป็นการเข้มงวดกับระบบของคุณจนเกินไป การสนับสนุนลายเซ็นดิจิตอลที่เพิ่มมาใหม่นี้ จะให้ความยืดหยุ่นแก่คุณในการตัดสินใจหาวิธีที่ดีที่สุดในการปกป้อง software integrity ของคุณ.

ลายเซ็นดิจิตอลที่ปกป้องซอฟต์แวร์เป็นเพียงวิธีการหนึ่งของการใช้งาน digital certificate. ข้อมูลเพิ่มเติมในเรื่องการจัดการ digital certificate สามารถดูได้จากหัวข้อ Digital certificate management ใน Information Center (โปรดดูที่ “สิ่งที่ต้องรู้ก่อนและข้อมูลที่เกี่ยวข้อง” ในหน้า xiii สำหรับรายละเอียด).

รายละเอียดของการมอนิเตอร์ระบบย่อย

เมื่อคุณเริ่มการทำงานของระบบย่อยบนเซิร์ฟเวอร์ iSeries , ระบบสร้างสภาวะแวดล้อมเพื่อรับงานเข้าไปในระบบและรันงานนั้น. คำอธิบายระบบย่อยจะกำหนดลักษณะของสภาพแวดล้อม. คำอธิบายระบบย่อย, สามารถเปิดโอกาสให้ผู้ใช้ที่ไม่ซื่อสัตย์. ผู้ประสงค์ร้ายอาจใช้คำอธิบายระบบย่อย เพื่อเริ่มต้นโปรแกรมโดยอัตโนมัติ หรือทำให้สามารถ sign on โดยไม่ต้องมีโปรไฟล์ผู้ใช้.

เมื่อคุณรันคำสั่ง Revoke Public Authority (RVKPUBAUT), ระบบจะกำหนดสิทธิพับลิกให้กับคำสั่งคำอธิบายระบบย่อยเป็น *EXCLUDE. ซึ่งจะป้องกันผู้ใช้ที่ไม่ได้รับสิทธิ (หรือผู้ที่ไม่มีสิทธิพิเศษ *ALLOBJ) ไม่ให้เปลี่ยนแปลงหรือสร้างคำอธิบายระบบย่อย.

หัวข้อต่อไปจะให้คำแนะนำสำหรับการตรวจคำอธิบายระบบย่อยที่อยู่ในระบบของคุณในขณะนี้. คุณสามารถใช้คำสั่ง Work with Subsystem Descriptions (WRKSBSD) เพื่อสร้างรายการ ของคำ

อธิบายระบบย่อยทั้งหมด. เมื่อคุณเลือกหมายเลข 5 (จอแสดงผล) จากรายการ, เมนูก็จะทำการแสดงผลรายละเอียดระบบตามที่คุณได้เลือกไป. โดยจะแสดงรายการของส่วนของสภาพแวดล้อมระบบย่อย.

คุณเลือกอ็อพชันเพื่อดูรายละเอียดของส่วนนั้น. ใช้คำสั่ง Change Subsystem Description (CHGSBSD) เพื่อเปลี่ยนสองรายการแรกในเมนู. เพื่อเปลี่ยนรายการอื่นๆ , ให้ใช้คำสั่งเพิ่ม, ลบ, หรือเปลี่ยนแปลง ที่เหมาะสมสำหรับประเภทของรายการ. ตัวอย่างเช่น, เพื่อเปลี่ยนรายการเกี่ยวกับเวิร์กสเตชัน, ให้ใช้คำสั่ง Change Workstation Entry (CHGWSE).

หนังสือ *Work Management* มีข้อมูลเพิ่มเติมเกี่ยวกับการทำงาน กับคำอธิบายระบบย่อย. และยังแสดงค่าที่ติดตั้งมาสำหรับคำอธิบายระบบย่อยที่ IBM จัดหาให้.

---

entry ของงานแบบ autostart

รายการงานที่เริ่มโดยอัตโนมัติบรรจุชื่อของคำอธิบายงานไว้. คำอธิบายงานอาจมี ข้อมูลร้องขอ (request data–RQSDTA) ที่ทำให้โปรแกรมหรือคำสั่งทำงาน. ตัวอย่างเช่น, RQSDTA อาจเป็น `CALL LIB1/PROGRAM1`. เมื่อระบบย่อยเริ่มทำงาน, ระบบจะรันโปรแกรม PROGRAM1 ในไลบรารี LIB1.

ดูที่รายการงานที่เริ่มต้นโดยอัตโนมัติของคุณและคำอธิบายงานที่สัมพันธ์กัน. ต้องแน่ใจว่าคุณเข้าใจการทำงานของโปรแกรมที่รันโดยอัตโนมัติเมื่อระบบย่อยเริ่มทำงาน.

ชื่อของเวิร์กสเตชัน และชนิดของเวิร์กสเตชัน

เมื่อระบบย่อยเริ่มทำงาน, จะมีการจัดสรรเวิร์กสเตชันทั้งหมดที่ยังไม่ถูกใช้ และแสดง (โดยการกำหนดหรือโดยทั่วไป) อยู่ในรายการของชื่อเวิร์กสเตชันและประเภท ของเวิร์กสเตชัน. เมื่อผู้ใช้ sign on, ผู้ใช้ที่กำลัง sign on เข้าไปในระบบย่อย ที่มีเวิร์กสเตชันที่จัดสรรไว้.

รายการเวิร์กสเตชันแสดงถึงคำอธิบายงานที่จะถูกใช้ เมื่องานเริ่มต้นทำงานที่ เวิร์กสเตชันนั้น. คำอธิบายงานอาจมีข้อมูลร้องขอที่ทำให้โปรแกรมหรือคำสั่งทำงาน. ตัวอย่างเช่น, พารามิเตอร์ RQSDTA อาจเป็น `CALL LIB1/PROGRAM1`. เมื่อผู้ใช้ sign on ไปยังเวิร์กสเตชันในระบบย่อยนั้น, ระบบจะรัน PROGRAM1 ใน LIB1.

ดูที่รายการเวิร์กสเตชันของคุณและคำอธิบายงานที่สัมพันธ์กัน. ต้องแน่ใจว่า ไม่มีใครทำการเพิ่มหรืออัพเดตรายการใดๆ เพื่อรันโปรแกรมที่คุณไม่ทราบ.

รายการเวิร์กสเตชันอาจมีการระบุโปรไฟล์ผู้ใช้ดีฟอลต์. สำหรับคอนฟิกูเรชันของ ระบบย่อยบางอย่าง, จะยอมให้ทำการ sign on ได้โดยง่าย โดยการกดคีย์ Enter. หากระดับความปลอดภัย (ค่ากำหนดของระบบ QSECURITY) ในระบบของคุณน้อยกว่า 40, คุณต้อง ตรวจสอบค่าผู้ใช้ดีฟอลต์ในรายการเวิร์กสเตชัน.

entry ของคิวงาน

เมื่อระบบย่อยเริ่มทำงาน, จะมีการจัดสรรคิวงานที่ยังไม่ถูกใช้และแสดงอยู่ใน คำอธิบายระบบย่อย. รายการคิวงานไม่ได้มีจุดอ่อนด้านความปลอดภัยโดยตรง. อย่างไรก็ตาม, ก็ยังทำให้เกิดโอกาสที่บางคนจะเข้าไปยุ่งกับประสิทธิภาพของระบบได้โดยการทำให้งานรันอยู่ในสภาพแวดล้อมที่ไม่ได้ตั้งใจ.

คุณต้องตรวจสอบรายการคิวงานในคำอธิบายระบบย่อยของคุณอย่างสม่ำเสมอ เพื่อทำให้ แน่ใจว่างานเป็นแบ็ตช์นั้นกำลังทำงานอยู่ในที่ที่คุณคาดคิดไว้.

entry ของการเราต์

รายการเส้นทางจะกำหนดสิ่งที่งานต้องทำเมื่อเข้าสู่ระบบย่อย. ระบบย่อยจะใช้รายการ เส้นทางสำหรับงานทุกประเภท: แบ็ตช์, แบบโต้ตอบ, และงานสื่อสาร. รายการเส้นทางจะระบุ ถึงสิ่งต่อไปนี้:

- คลาสของงาน. เช่นเดียวกับรายการคิวงาน, คลาสที่สัมพันธ์กับงานจะมีผลต่อ ประสิทธิภาพของงานแต่จะไม่เป็นจุดอ่อนด้านความปลอดภัย.
- โปรแกรมที่จะทำงานเมื่องานเริ่มต้น. ดูที่รายการเส้นทางและทำให้แน่ใจว่าไม่มีใคร ทำการเพิ่มหรืออัพเดตรายการใดๆ เพื่อรันโปรแกรมที่คุณไม่ทราบ.

Communications entr และชื่อตำแหน่งรีโมต

เมื่องานสื่อสารเข้าสู่ระบบของคุณ, ระบบจะใช้รายการสื่อสารและรายการชื่อรีโมตโลเคชัน ในระบบย่อยที่แอ็คทีฟเพื่อพิจารณาวิธีการทำงานของงานสื่อสาร. รายการเหล่านี้ประกอบด้วย:

- ระบบย่อยทั้งหมดมีขีดความสามารถที่จะทำงานสื่อสาร. ถ้าระบบย่อยที่คุณตั้งใจสำหรับ การสื่อสารไม่ได้ทำงานอยู่, งานที่พยายามเข้าระบบคุณอาจพบรายการคำอธิบายในระบบย่อยอื่น ที่ตรงกับความต้องการ. คุณจำเป็นต้องดูรายการในคำอธิบายระบบย่อยทั้งหมด.
- รายการสื่อสารจะมีคำอธิบายงาน (job description). คำอธิบายงานอาจมีข้อมูลร้องขอ ที่รันคำสั่งหรือโปรแกรม. ดูที่รายการสื่อสารของคุณ และคำอธิบายงานที่เกี่ยวข้อง เพื่อให้มั่นใจว่าคุณเข้าใจว่างานจะเริ่มต้นอย่างไร.
- รายการสื่อสารยังกำหนดโปรไฟล์ผู้ใช้ดีฟอลต์ที่ระบบจะใช้ในบางสถานการณ์. ให้แน่ใจว่า คุณเข้าใจบทบาทของดีฟอลต์โปรไฟล์. ถ้าระบบของคุณมีดีฟอลต์โปรไฟล์, คุณต้องแน่ใจว่า โปรไฟล์เหล่านั้นมีสิทธิน้อยที่สุด. ดู บทที่ 12, “การรักษาความปลอดภัยให้กับการสื่อสารแบบ APPC” สำหรับข้อมูลเพิ่มเติมเกี่ยวกับโปรไฟล์ผู้ใช้ที่เป็นดีฟอลต์.

  คุณสามารถใช้ คำสั่ง Print Subsystem Description (PRTSBSDAUT) เพื่อบ่งชี้รายการสื่อสารที่กระบุชื่อโปรไฟล์ผู้ใช้.

Prestart job entry

คุณสามารถใช้ prestart job entry เพื่อทำให้ระบบย่อยพร้อมสำหรับงานบางประเภท เพื่องานจะได้เริ่มต้นได้เร็วขึ้น. งานที่เริ่มต้นก่อน (prestart job) อาจเริ่มเมื่อระบบย่อยเริ่มทำงานหรือเมื่อเป็นที่ต้องการ. รายการงานที่เริ่มต้นก่อนกำหนดสิ่งเหล่านี้:

- โปรแกรมที่จะทำงาน

  โปรไฟล์ผู้ใช้ดีฟอลต์

  คำอธิบายงาน

สิ่งเหล่านี้จะทำให้เกิดจุดอ่อนของความปลอดภัยที่สำคัญได้. คุณต้องแน่ใจว่า prestart job entry ทำเฉพาะฟังก์ชันที่ต้องการและมีสิทธิเท่านั้น.

งานและรายละเอียดของงาน

คำอธิบายงานมีข้อมูลร้องขอ (request data) และข้อมูลเส้นทาง (routing data) ที่สามารถทำให้โปรแกรมที่กำหนดทำงาน เมื่อมีการใช้งานคำอธิบายงาน. เมื่อคำอธิบายงานกำหนดโปรแกรมในพารามิเตอร์ข้อมูลร้องขอ, ระบบจะรันโปรแกรมนั้น. เมื่อคำอธิบายงานกำหนดข้อมูลเส้นทาง, ระบบจะรันโปรแกรมที่ถูกกำหนดในรายการเส้นทาง ที่ตรงกับข้อมูลเส้นทาง.

ระบบจะใช้คำอธิบายงานทั้งงานที่เป็นแบบโต้ตอบและงานเป็นแบ็ตช์. สำหรับงานโต้ตอบ, รายการเวิร์กสเตชันจะระบุคำอธิบายงาน. โดยทั่วไป, ค่าของรายการเวิร์กสเตชันคือ *USRPRF, ดังนั้นระบบจะใช้คำอธิบายงานที่ระบุไว้ในโปรไฟล์ผู้ใช้. สำหรับงานเป็นแบ็ตช์, คุณกำหนดคำอธิบายงานเมื่อคุณทำการส่งงาน (submit).

คุณต้องตรวจดูคำอธิบายเป็นครั้งคราว เพื่อให้มั่นใจว่าคำอธิบายงานไม่ได้รันโปรแกรม ที่ไม่ต้องการ. คุณยังควรใช้สิทธิอ็อบเจ็กต์เพื่อป้องกันการเปลี่ยนแปลงที่เกิดขึ้นกับคำอธิบายงาน. สิทธิ *USE เพียงพอต่อการรันงานด้วยคำอธิบายงาน. ผู้ใช้ทั่วไปจึงไม่จำเป็นต้องมีสิทธิ *CHANGE ในคำอธิบายงาน.

อ็อพชันของเมนู SECBATCH:

15 *เพื่อส่งงานทันที* **54** *เพื่อใช้ตารางเวลางาน*

คำอธิบายงานสามารถกำหนดโปรไฟล์ผู้ใช้ที่งานจะรันอยู่ภายใต้ได้. ที่ระดับความปลอดภัย 40 หรือสูงกว่า, คุณต้องมีสิทธิ *USE ในคำอธิบายงานและโปรไฟล์ผู้ใช้ที่ระบุไว้ในคำอธิบายงาน. ที่ระดับความปลอดภัยต่ำกว่า 40, คุณต้องการสิทธิ *USE ในคำอธิบายงานเท่านั้น.

คุณสามารถใช้คำสั่ง Print Job Description Authority (PRTJOBDAUT) เพื่อพิมพ์รายการของคำอธิบายงาน ที่ระบุโปรไฟล์ผู้ใช้และมีสิทธิ *USE.

รายงานแสดงถึงสิทธิพิเศษของโปรไฟล์ผู้ใช้ที่กำหนดอยู่ในคำอธิบายงาน. ในรายงานยังมี สิทธิเศษของโปรไฟล์กลุ่มที่โปรไฟล์ผู้ใช้มี. คุณสามารถใช้คำสั่งต่อไปนี้แสดงสิทธิไพรเวตของโปรไฟล์ผู้ใช้:

```
DSPUSRPRF USRPRF(profile-name) TYPE(*OBJAUT)
```

คำอธิบายงานระบุรายชื่อไลบรารีที่งานจะต้องใช้เมื่องานนั้นทำงาน. หากมีผู้ใด ที่สามารถเปลี่ยนแปลงรายชื่อไลบรารีของผู้ใช้ได้, ผู้ใช้นั้นอาจรันโปรแกรมที่ไม่ต้องการในไลบรารีที่แตกต่างไป. คุณจึงต้องตรวจดูรายการไลบรารีที่ระบุในคำอธิบายงานของระบบคุณเป็นครั้งคราว.

ท้ายที่สุด, คุณต้องมั่นใจว่าค่าดีฟอลต์ของคำสั่ง Submit Job (SBMJOB) และคำสั่ง Create User Profile (CRTUSRPRF) ไม่ได้ถูกเปลี่ยนให้ชี้ไปยังคำอธิบายงานที่ไม่ต้องการ.

Architected transaction program name

การร้องขอของการสื่อสารบางอย่างส่งสัญญาณบางประเภทเข้าสู่ระบบของคุณ. การร้องขอนี้เรียกว่า **architecture transaction program name (TPN)** เนื่องจากชื่อของ transaction program เป็นส่วนหนึ่งของสถาปัตยกรรม APPC สำหรับระบบ. การร้องขอในการแสดงผลการร้องขอ display station pass-through เป็นตัวอย่างของสถาปัตยกรรม TPN. สถาปัตยกรรม TPN เป็นวิธีปกติในการสื่อสารไปยังฟังก์ชัน และไม่ได้ทำให้เกิดจุดอ่อนด้านความปลอดภัยโดยไม่จำเป็น. อย่างไรก็ตาม, สถาปัตยกรรม TPN อาจทำให้มีช่องทางที่ไม่คาดคิดเข้าสู่ระบบคุณ.

บาง TPN ไม่ได้ส่งโปรไฟล์ตามการร้องขอ. ถ้าการร้องขอสัมพันธ์กับรายการการสื่อสารที่ผู้ใช้ดีฟอลต์ คือ *SYS, การร้องขอนั้นอาจถูกเริ่มต้นในระบบของคุณ. อย่างไรก็ตาม, โปรไฟล์ *SYS สามารถรันได้แต่ฟังก์ชันของระบบ, ไม่ใช่แอ็พพลิเคชันของผู้ใช้.

ถ้าคุณไม่ต้องการให้สถาปัตยกรรม TPN รันด้วยโปรไฟล์ดีฟอลต์, คุณสามารถเปลี่ยนผู้ใช้ดีฟอลต์ในรายการการสื่อสาร จาก *SYS ไปเป็น *NONE . “คำร้องขอ Architected TPN” ในหน้า 98 แสดงรายการของสถาปัตยกรรม TPN และโปรไฟล์ผู้ใช้ที่สัมพันธ์กัน.

ถ้าคุณไม่ต้องการให้ TPN หนึ่ง รันในระบบของคุณอีกต่อไป, ให้ทำดังต่อไปนี้:

1. สร้างโปรแกรม CL ที่ยอมรับพารามิเตอร์หลายตัว. โปรแกรมจะไม่ทำฟังก์ชันใดๆ . แต่จะมีข้อความ Declare (DCL) สำหรับพารามิเตอร์และจบการทำงานเท่านั้น.
2. เพิ่มรายการเส้นทางสำหรับ TPN ไปยังแต่ละระบบย่อยทีมีรายการการสื่อสารหรือมีรายการ remote location name. รายการเส้นทางจะต้องกำหนดดังนี้:
   - ค่า *Compare value* (CMPVAL) เท่ากับชื่อชื่อโปรแกรมสำหรับ TPN (ดูใน คำร้องขอ Architected TPN) ด้วยตำแหน่งเริ่มต้น 37.
   - ค่า *Program to call* (PGM) เท่ากับชื่อของโปรแกรม ที่คุณสร้างขึ้นในขั้นตอนที่ 1. ซึ่งจะป้องกัน TPN จากการชี้ไปยังรายการอื่น, เช่น *ANY.

มีหลาย TPN ที่มีรายการเส้นทางในระบบย่อย QCMN อยู่แล้ว. แต่ยังถูกเพิ่มด้วยเหตุผลทางประสิทธิภาพ.

คำร้องขอ Architected TPN

ตารางที่ 17. โปรแกรมและผู้ใช้สำหรับการร้องขอ TPN

คำร้องขอ TPN	โปรแกรม	โปรไฟล์ผู้ใช้	คำอธิบาย
X'30F0F8F1'	AMQCRC6A	*NONE	Message queuing
X'06F3F0F1'	QACSOTP	QUSER	APPC sign-on transaction program
X'30F0F2D1'	QANRTP	QADSM	ADSM/400 APPC configuration
X'30F0F1F9'	QCNPCSUP	*NONE	Shared folders
X'07F0F0F1'	QCNTEDDM	QUSER	DDM
X'07F6C4C2'	QCNTEDDM	QUSER	Remote SQL-DRDA1
X'30F0F7F7'	QCQNRBAS	QSVCCS	SNA CC_Server
X'30F0F1F4'	QDXPRCV	QUSER	DSNX-PC receiver
X'30F0F1F3'	QDXPSEND	QUSER	DSNX-PC sender
X'30F0F2C4'	QEVYMAIN	QUSER	ENVY**/400 Server
X'30F0F6F0'	QHQTRGT	*NONE	PC data queue
X'30F0F8F0'	QLZPSERV	*NONE	Client Access license manager
X'30F0F1F7'	QMFRCVR	*NONE	PC message receiver
X'30F0F1F8'	QMFSNDR	*NONE	PC message sender
X'30F0F6F6'	QND5MAIN	QUSER	APPN 5394 workstation controller
DB2DRDA	QCNTEDDDM	QUSER	DB2DRDA
APINGD	QNMAPINGD	QUSER	APINGD
X'30F0F5F4'	QNMEVK	QUSER	System management utilities
X'30F0F2C1'	QNPSERVR	*NONE	PWS-I network print server
X'30F0F7F9'	QOCEVOKE	*NONE	Cross-system calendar
X'30F0F6F1'	QOKCSUP	QDOC	Directory shadowing
X'20F0F0F7'	QOQSESRV	QUSER	DIA Version 2
X'20F0F0F8'	QOQSESRV	QUSER	DIA Version 2
X'30F0F5F1'	QOQSESRV	QUSER	DIA Version 2
X'20F0F0F0'	QOSAPPC	QUSER	DIA Version 1
X'30F0F0F5'	QPAPAST2	QUSER	S/36—S/38 pass-through
X'30F0F0F9'	QPAPAST2	QUSER	Printer pass-through

ตารางที่ 17. โปรแกรมและผู้ใช้สำหรับการร้องขอ TPN (ต่อ)

คำร้องขอ TPN	โปรแกรม	โปรไฟล์ผู้ใช้	คำอธิบาย
X'30F0F4F6'	QPWFSTP0	*NONE	Shared Folders Type 2
X'30F0F2C8'	QPWFSTP1	*NONE	Client Access file server
X'30F0F2C9'	QPWFSTP2	*NONE	Windows** Client Access file server
	QRQSRVX	*NONE	Remote SQL-converged server
X'30F0F6F5'	QRQSRV0	*NONE	Remote SQL without commit
X'30F0F6F4'	QRQSRV1	*NONE	Remote SQL without commit
X'30F0F2D2'	QSVRCI	QUSER	SOC/CT
X'21F0F0F8'	QS2RCVR	QGATE	SNADS FS2 receiver
X'21F0F0F7'	QS2STSND	QGATE	SNADS FS2 sender
X'30F0F1F6'	QTFDWNLD	*NONE	PC transfer function
X'30F0F2F4'	QTIHNPCS	QUSER	TIE function
X'30F0F1F5'	QVPPRINT	*NONE	PC virtual print
X'30F0F2D3'	QWGMTP	QWGM	Ultimedia Mail/400 Server
X'30F0F8F3'	QZDAINIT	QUSER	PWS-I data access server
X'21F0F0F2'	QZDRCVR	QSNADS	SNADS receiver
X'21F0F0F1'	QZDSTSND	QSNADS	SNADS sender
X'30F0F2C5'	QZHQTRG	*NONE	PWS-I data queue server
X'30F0F2C6'	QZRCSRVR	*NONE	PWS-I remote command server
X'30F0F2C7'	QZSCSRVR	*NONE	PWS-I central server

วิธีการเฝ้าสังเกตเหตุการณ์ด้านความปลอดภัย

การจัดเตรียมความปลอดภัยไม่ใช่งานที่ทำเพียงครั้งเดียว. คุณจำเป็นต้องประเมินการเปลี่ยนแปลงในระบบของคุณ และความล้มเหลวในระบบความปลอดภัยอย่างสม่ำเสมอ. จากนั้นทำการปรับแต่งสภาพแวดล้อมด้านความปลอดภัยของคุณ เพื่อตอบสนองสิ่งที่คุณค้นพบ.

รายงานความปลอดภัยช่วยคุณเฝ้าสังเกตการเปลี่ยนแปลงที่เกี่ยวข้องกับความปลอดภัยที่เกิดขึ้นกับระบบของคุณ. ฟังก์ชันอื่นของระบบที่คุณสามารถใช้เพื่อช่วยคุณตรวจจับความล้มเหลวหรือจุดอ่อนด้านความปลอดภัยมีดังนี้:

- การตรวจสอบความปลอดภัย (security auditing) เป็นเครื่องมือที่มีประสิทธิภาพที่คุณสามารถใช้ในการ เฝ้าดูเหตุการณ์ที่เกี่ยวข้องกับความปลอดภัยหลายๆ ประเภท ที่เกิดขึ้นในระบบของคุณ. ตัวอย่างเช่น, คุณสามารถจัดเตรียมระบบให้บันทึกเร็กคอร์ดการตรวจสอบ (audit record)

ทุกครั้งที่ผู้ใช้เปิดฐานข้อมูลเพื่อทำการอัพเดต. คุณสามารถตรวจสอบการเปลี่ยนแปลงทั้งหมดของค่ากำหนดของระบบ. คุณสามารถตรวจสอบกิจกรรมที่เกิดขึ้นเมื่อผู้ใช้เรียกอ็อบเจ็กต์กลับคืน.

บทที่ 9 ในหนังสือ *iSeries Security Reference* มีข้อมูลทั้งหมดเกี่ยวกับฟังก์ชันการตรวจสอบความปลอดภัย. คุสามารถใช้คำสั่ง Change Security Auditing (CHGSECAUD) เพื่อจัดเตรียมการตรวจสอบความปลอดภัยในระบบของคุณ. คุณยังสามารถใช้คำสั่ง Display Audit Journal Entries (DSPAUDJRNE) เพื่อพิมพ์ข้อมูลที่เลือกจาก เจอร์นัลการตรวจสอบความปลอดภัย.

- คุณสามารถสร้างคิวข้อความ QSYSMSG เพื่อดักจับ ข้อความวิกฤตสำหรับผู้ควบคุมระบบ (critical system-operator message). คิวข้อความ QSYSOPR รับหลายข้อความที่มีความสำคัญแตกต่างกัน ในแต่ละวันทำงาน. ข้อความที่เกี่ยวข้องกับความปลอดภัย, ในระดับอันตรายอาจถูกมองข้ามไป เนื่องจากมีข้อความเป็นจำนวนมากอยู่ในคิวข้อความ QSYSOPR.

  ถ้าคุณสร้างคิวข้อความ QSYSMSG ในไลบรารี QSYS ในระบบของคุณ, ระบบจะทำการเปลี่ยนทิศทางของข้อความวิกฤตไปสู่คิวข้อความ QSYSMSG แทนที่จะไปสู่คิวข้อความ QSYSOPR.

  คุณสามารถสร้างโปรแกรมเพื่อเฝ้าสังเกตคิวข้อความ QSYSMSG, หรือคุณสามารถกำหนดคิวข้อความ QSYSMSG ในโหมดหยุด (break mode) ไปยังตัวคุณหรือผู้ใช้อื่นที่ไว้ใจได้.

ส่วนที่ 3. แอ็พพลิเคชันและการสื่อสารบนเน็ตเวิร์ก

บทที่ 11. การใช้ Integrated File System ในการรักษาความปลอดภัยให้กับไฟล์ต่างๆ

integrated file system ช่วยให้คุณมีหลายๆ วิธีในการเก็บข้อมูลและเรียกดูข้อมูลที่อยู่บนเซิร์ฟเวอร์ iSeries. integrated file system เป็นส่วนหนึ่งของระบบปฏิบัติการ OS/400 ที่สนับสนุนการทำงานอินพุต และเอาต์พุตแบบ stream. โดยจะมีวิธีการบริหารหน่วยความจำที่คล้ายคลึงกัน (และทำงานร่วมกันได้) กับระบบปฏิบัติการของคอมพิวเตอร์ส่วนบุคคล และระบบปฏิบัติการยูนิกซ์ (UNIX) แบบ®.

ด้วย integrated file system, อ็อบเจ็กต์ทุกตัวในระบบสามารถถูกมองเห็นได้จากมุมมองของโครงสร้างไดเร็กทอรีแบบเป็นลำดับชั้น (hierarchical directory structure). อย่างไรก็ตาม, ในกรณีส่วนใหญ่ผู้ใช้จะมองเห็นอ็อบเจ็กต์ในแบบสามัญที่สุดสำหรับระบบไฟล์นั้นๆ . ตัวอย่างเช่น, อ็อบเจ็กต์ "แบบเก่า" ของ iSeries ที่อยู่ในระบบไฟล์ QSYS.LIB. โดยทั่วไป, ผู้ใช้มองอ็อบเจ็กต์เหล่านี้จากมุมมองของไลบรารี. โดยทั่วไป ผู้ใช้จะมองเห็นอ็อบเจ็กต์ในระบบไฟล์ QDLS จากมุมมองของเอกสารที่อยู่ภายในโฟลเดอร์. ราก (root หรือ /), QOpenSys และระบบที่ผู้ใช้กำหนดขึ้นเอง (user-defined file system) แสดงโครงสร้างของไดเร็กทอรีแบบเป็นลำดับชั้น (ซ้อนกัน).

ในฐานะของผู้บริหารความปลอดภัย, คุณต้องเข้าใจในสิ่งต่างๆ ดังต่อไปนี้:

- ระบบไฟล์แบบใดที่ถูกนำมาใช้บนระบบของคุณ?
- ลักษณะความปลอดภัยที่เป็นเอกลักษณ์เฉพาะของแต่ละระบบไฟล์

หัวข้อต่อไปนี้จะกล่าวถึงสิ่งที่ควรพิจารณาโดยทั่วไปสำหรับการรักษาความปลอดภัยของ integrated file system.

แนวทางของ Integrated File System ที่มีต่อการรักษาความปลอดภัย

ระบบไฟล์ root (root file system) ทำหน้าที่เหมือนกับเป็นร่ม (หรือ เป็นรากฐาน) สำหรับระบบไฟล์อื่นๆ ทั้งหมดที่อยู่บน เซิร์ฟเวอร์ iSeries. ในระดับที่สูงขึ้นไป, จะมีการแสดงภาพรวมของอ็อบเจ็กต์ทุกตัวที่อยู่บนระบบ. ระบบไฟล์อื่นๆ ที่สามารถมีอยู่บนเซิร์ฟเวอร์ iSeries จะมีหลากหลายแนวทางในการจัดการและการรวมเข้าด้วยกันของอ็อบเจ็กต์, ขึ้นอยู่กับจุดประสงค์ที่สำคัญของ file system แต่ละตัว. ระบบไฟล์ QOPT (optical), เป็นตัวอย่าง, ที่อนุญาตให้แอ็พพลิเคชัน iSeries และเซิร์ฟเวอร์ (รวมไปถึง iSeries Access for Windows file server) เข้าถึงซีดีรอมไดร์ฟที่อยู่บนเซิร์ฟเวอร์ iSeries . ในลักษณะเดียวกัน, ระบบไฟล์ QFileSvr.400 อนุญาตให้แอ็พพลิเคชันสามารถเข้าถึงข้อมูล integrated file system ที่อยู่ในเซิร์ฟเวอร์ iSeriesแบบรีโมต . ระบบไฟล์ QLANSrv อนุญาตให้เข้าถึงไฟล์ที่เก็บอยู่ใน Integrated xSeries Server for iSeries หรือ เซิร์ฟเวอร์อื่นๆ ที่ต่ออยู่ภายในเครือข่าย.

แนวทางความปลอดภัยสำหรับแต่ละระบบไฟล์ขึ้นอยู่กับข้อมูลที่ระบบไฟล์อนุญาตให้ใช้ประโยชน์ได้. ตัวอย่างเช่น, ระบบไฟล์ QOPT ไม่มีความปลอดภัยในระดับอ็อบเจ็กต์ เนื่องจากยังไม่มีเทคโนโลยีที่ใช้เขียนข้อมูลเกี่ยวกับสิทธิ (authority information) ไปยังซีดีรอม. สำหรับระบบไฟล์

QFileSvr.400, แอ็คเซสคอนโทรลเกิดขึ้นที่ระบบรีโมต (ที่ซึ่งมีการบันทึกและจัดการกับไฟล์จริงๆ). สำหรับระบบไฟล์ เช่น QLANSrv, Integrated xSeries Server for iSeries จะมีแอ็คเซสคอนโทรลให้เช่นกัน. ถึงแม้ว่ามีความแตกต่างด้านรูปแบบความปลอดภัย, ระบบไฟล์หลายๆ ระบบยังรองรับการจัดการแอ็คเซสคอนโทรลแบบเดียวกัน ผ่านทางคำสั่งของระบบไฟล์รวม, เช่น คำสั่ง Change Authority (CHGAUT) และ Change Owner (CHGOWN).

นี่เป็นคำแนะนำบางอย่างที่เกี่ยวข้องกับจุดอ่อนของการรักษาความปลอดภัยของระบบไฟล์รวม. ระบบไฟล์รวมถูกออกแบบมาตามมาตรฐาน POSIX โดยให้ใกล้เคียงที่สุดเท่าที่เป็นไปได้. ซึ่งจะเป็นการนำไปสู่พฤติกรรมที่น่าสนใจบางอย่างที่สิทธิในการใช้งานเซิร์ฟเวอร์ iSeries และ การอนุญาตการใช้งานของ POSIX ถูก "ผสมผสาน" เข้าด้วยกัน:

1. ห้ามลบสิทธิไพรเวตสำหรับผู้ใช้ในไดเร็กทอรีที่ผู้ใช้นั้นเป็นเจ้าของ, ถึงแม้ว่าผู้ใช้จะได้สิทธิผ่านทางสิทธิพับลิก, ทางกลุ่ม, หรือทาง authorization list. ในการทำงานกับไลบรารีหรือโฟลเดอร์ที่อยู่ใน แบบจำลองการรักษาความปลอดภัยมาตรฐาน ของเซิร์ฟเวอร์ iSeries , การลบสิทธิไพรเวตของเจ้าของจะลดจำนวนของข้อมูลของสิทธิในการใช้งานที่ถูกบันทึกไว้สำหรับโปรไฟล์ผู้ใช้และจะไม่มีผลกระทบต่อปฏิบัติการอื่น ๆ. แต่, เนื่องด้วยวิธีการที่มาตรฐาน POSIX ได้กำหนดการถ่ายทอดการอนุญาต (permission) สำหรับไดเร็กทอรี, เจ้าของไดเร็กทอรีที่สร้างขึ้นใหม่จะมีสิทธิทางอ็อบเจ็กต์ในไดเร็กทอรี่นั้น เช่นเดียวกับสิทธิทางอ็อบเจ็กต์ที่เจ้าของไดเร็กทอรีบรรรพบุรุษมีต่อไดเร็กทอรีบรรพบุรุษ, ถึงแม้ว่าเจ้าของไดเร็กทอรี ที่สร้างขึ้นใหม่จะมีสิทธิไพรเวตอื่นไปยังไดเร็กทอรีบรรพบุรุษ. ซึ่งอาจจะยากต่อการทำความเข้าใจ, ดังนั้นขอให้ ดูจากตัวอย่างต่อไปนี้: USERA เป็นเจ้าของไดเร็กทอรี /DIRA, แต่มีการลบสิทธิไพรเวตของ USERA ออกไป. USERB มีสิทธิไพรเวตใน /DIRA. USERB สร้างไดเร็กทอรี /DIRA/DIRB. เนื่องจาก USERA ไม่มีสิทธิอ็อบเจ็กต์ใน /DIRA, ดังนั้น USERB จะไม่มีสิทธิอ็อบเจ็กต์ใน /DIRA/DIRB. USERB จะไม่สามารถเปลี่ยนชื่อหรือลบ /DIRA/DIRB ได้ หากไม่มีการเปลี่ยนแปลงสิทธิอ็อบเจ็กต์ของ USERB. และจะเป็นเช่นเดียวกันเมื่อสร้างไฟล์โดยใช้ API open() และใช้แฟล็ก O_INHERITMODE. ถ้า USERB สร้างไฟล์ /DIRA/FILEB, USERB จะไม่มีสิทธิอ็อบเจ็กต์และไม่มีสิทธิในการใช้ข้อมูลในไฟล์นั้น.ทำให้ USERB ไม่สามารถทำการเขียนลงในไฟล์ใหม่ได้.
2. สิทธิที่รับมา (Adopted authority) ไม่ได้รับการยอมรับโดยระบบไฟล์แบบฟิสิคัลส่วนใหญ่. ซึ่งรวมถึงระบบไฟล์ราก (root หรือ /), QOpenSys, QDLS และระบบไฟล์ที่ผู้ใช้กำหนด.
3. อ็อบเจ็กต์ใดๆ เป็นของโปรไฟล์ผู้ใช้ที่สร้างอ็อบเจ็กต์นั้น, ถึงแม้ว่าในฟิลด์ OWNER ของโปรไฟล์ผู้ใช้จะกำหนดเป็น *GRPPRF.
4. การทำงานของระบบไฟล์ส่วนใหญ่ต้องการสิทธิในการใช้ข้อมูล *RX ในทุกองค์ประกอบของพาธ (path), รวมถึงไดเร็กทอรีราก (/). เมื่อพบปัญหาเกี่ยวกับสิทธิในการใช้งาน, ให้ตรวจสอบสิทธิของผู้ใช้ในไดเร็กทอรีราก (root)ว่าถูกต้องหรือไม่.
5. การแสดงผลหรือการเรียกข้อมูลของไดเร็กทอรีปัจจุบันที่ทำงาน (DSPCURDIR, getcwd(), เป็นต้น) ต้องการสิทธิในการ ใช้ข้อมูล *RX ในทุกทุกองค์ประกอบในพาธ. แต่การเปลี่ยนไดเร็กทอรีปัจจุบันที่ทำงาน (CD, chdir(), เป็นต้น.) ต้องการเพียงสิทธิในการใช้ข้อมูล *X ในทุกองค์ประกอบเท่านั้น. ดังนั้น, ผู้ใช้อาจเปลี่ยนไดเร็กทอรีที่ ทำงานในขณะนี้ไปยังไดเร็กทอรีหนึ่งที่ต้องการ แต่จะไม่สามารถแสดงผลของพาธนั้นได้.
6. จุดประสงค์ของคำสั่ง COPY คือ การทำสำเนา (duplicate) ของอ็อบเจ็กต์. สิทธิที่กำหนดบนไฟล์ใหม่จะเหมือนกับต้นฉบับ ยกเว้นส่วนของเจ้าของเท่านั้น. ส่วนจุดประสงค์ของคำสั่ง

CPYTOSTMF, อย่างไรก็ตาม, โดยทั่วไปคือ การทำสำเนาข้อมูล. ผู้ใช้ไม่สามารถควบคุมสิทธิที่ตั้งค่าบนไฟล์ใหม่ได้. ผู้สร้าง/เจ้าของจะมีสิทธิในการใช้ข้อมูลเป็น *RWX, แต่สิทธิของกลุ่มหรือสิทธิพับลิกจะเป็น *EXCLUDE. ผู้ใช้ต้องใช้วิธีอื่น (เช่น CHGAUT, chmod(), เป็นต้น.) ในการกำหนดสิทธิที่ต้องการ.

7. เพื่อที่จะเรียกข้อมูลเกี่ยวกับสิทธิของอ็อบเจ็กต์ ผู้ใช้จะต้องเป็นเจ้าของหรือมีสิทธิอ็อบเจ็กต์ *OBJMGT ในอ็อบเจ็กต์นั้น . ซึ่งจะส่งผลกระทบในบางสถานการณ์ที่ไม่คาดคิด, เช่นเดียวกับ COPY, ที่จะต้องเรียกข้อมูลเกี่ยวกับ สิทธิในอ็อบเจ็กต์ต้นฉบับเพื่อกำหนดสิทธิที่เหมือนกันในอ็อบเจ็กต์เป้าหมาย.
8. เมื่อมีการเปลี่ยนเจ้าของหรือกลุ่มของอ็อบเจ็กต์, ผู้ใช้ไม่เพียงแต่จะต้องมีสิทธิที่เหมาะสมในอ็อบเจ็กต์นั้นเท่านั้น, แต่จะต้องมีสิทธิในการใช้ข้อมูล *ADD ในโปรไฟล์ของเจ้าของหรือกลุ่มใหม่ และมีสิทธิในการใช้ข้อมูล *DELETE ในโปรไฟล์ของเจ้าของหรือกลุ่มเก่าด้วย. สิทธิในการใช้ข้อมูลเหล่านี้ไม่เกี่ยวข้องกับสิทธิในการใช้ข้อมูลของระบบไฟล์. สามารถแสดงสิทธิในการใช้ข้อมูลเหล่านี้ด้วยการใช้คำสั่ง DSPOBJAUT และเปลี่ยนแปลงสิทธิได้โดยคำสั่ง EDTOBJAUT.ซึ่งทำให้เกิดผลที่ไม่คาดคิดในคำสั่ง COPY เมื่อมีการพยายามกำหนด ID กลุ่ม (group ID) สำหรับอ็อบเจ็กต์ใหม่.
9. คำสั่ง MOV มีแนวโน้มที่จะทำให้เกิดข้อผิดพลาดเกี่ยวกับความสับสนในเรื่องสิทธิ, โดยเฉพาะอย่างยิ่ง เมื่อมีการย้ายจากระบบไฟล์แบบฟิสิคัลระบบหนึ่งไปยังอีกระบบหนึ่ง, หรือเมื่อทำการแปลงข้อมูล. ในกรณีเหล่านี้, การย้ายจะกลายเป็นการทำการก๊อปปีและลบ. ดังนั้น, คำสั่ง MOV สามารถถูกกระทบโดยข้อพิจารณาด้านสิทธิทุกข้อเช่นเดียวกับ คำสั่ง COPY (ดูข้อ 7 หรือ 8 ข้างต้น), และคำสั่ง RMVLNK, เพิ่มเติมจากสิ่งที่ควรพิจารณาเฉพาะคำสั่ง MOV.

ในส่วนต่อไปนี้แสดงถึงข้อควรพิจารณาบางประการสำหรับระบบไฟล์หลายประเภท . สำหรับข้อมูลเพิ่มเติมเกี่ยวกับระบบไฟล์จำเพาะบนเซิร์ฟเวอร์ iSeries ของคุณ, คุณอาจจะต้องศึกษาเอกสารคู่มือสำหรับโปรแกรมที่ใช้ระบบไฟล์นั้น.

ระบบไฟล์ราก (Root หรือ /), QOpenSys, และระบบไฟล์ที่ผู้ใช้กำหนดขึ้นเอง

ข้อควรพิจารณาด้านความปลอดภัยสำหรับระบบไฟล์ราก, QOpenSys และระบบไฟล์ที่ผู้ใช้กำหนดมีดังนี้.

สิทธิในการใช้งานทำงานอย่างไร

ระบบไฟล์ราก (root), QOpenSys, และที่กำหนดขึ้นโดยผู้ใช้จะเป็นการจัดสรรการผสมผสานความสามารถของ เซิร์ฟเวอร์ iSeries , เครื่องคอมพิวเตอร์ส่วนบุคคล, และ UNIX** ทั้งในส่วนของการจัดการอ็อบเจ็กต์ และ การรักษาความปลอดภัย. เมื่อคุณใช้คำสั่ง integrated file system จากเซสชันของเซิร์ฟเวอร์ iSeries (WRKAUT และ CHGAUT), คุณสามารถตั้งค่าปกติของสิทธิอ็อบเจ็กต์ทั้งหมดของเซิร์ฟเวอร์ iSeries . รวมถึงสิทธิ *R, *W, และ *X ที่ทำงานร่วมกันได้กับ Spec 1170 (ระบบปฏิบัติการชนิดหนึ่งของยูนิกซ์).

หมายเหตุ: ระบบไฟล์ราก (/), QOpenSys และระบบไฟล์ที่ผู้ใช้กำหนด ในทางปฏิบัติแล้วมีค่าเท่าเทียมกัน. ระบบไฟล์ QOpenSys คำนึงถึงขนาดตัวพิมพ์. แต่ระบบไฟล์รากไม่เป็นเช่นนั้น. ระบบไฟล์ที่ผู้ใช้กำหนดสามารถกำหนดเป็นแบบคำนึงถึงตัวอักษรใหญ่เล็ก

ได้. เนื่องจากระบบไฟล์เหล่านี้ มีคุณสมบัติด้านความปลอดภัยเหมือนกัน, จึงถือได้ว่าชื่อของระบบไฟล์ที่อยู่ในหัวข้อต่อไปนั้นสามารถใช้แทนกันได้.

เมื่อคุณเข้าถึงระบบไฟล์รากในฐานะของผู้บริหารจากเซสชันของพีซี, คุณสามารถกำหนดแอ็ตทริบิวต์ของอ็อบเจ็กต์ ที่พีซีใช้ในการจำกัดการเข้าถึงบางประเภท:

- System
- Hidden
- Archive
- Read-only

แอ็ตทริบิวต์ของ พีซีเหล่านี้เป็นส่วนเพิ่มเติม, ไม่ใช่การแทนที่ค่าสิทธิในอ็อบเจ็กต์ของเซิร์ฟเวอร์ iSeries.

เมื่อผู้ใช้พยายามเข้าถึงอ็อบเจ็กต์ในระบบไฟล์ราก, OS/400 จะปฏิบัติตามค่าอำนาจของอ็อบเจ็กต์และแอ็ตทริบิวต์ ของอ็อบเจ็กต์ทุกอย่าง, โดยไม่สนใจว่าสิทธิเหล่านี้จะ "มองเห็น" จากอินเตอร์เฟสของผู้ใช้ได้หรือไม่. ตัวอย่างเช่น, สมมุติว่าแอ็ตทริบิวต์ read-only ของอ็อบเจ็กต์เป็น on. ผู้ใช้พีซีไม่สามารถลบอ็อบเจ็กต์ผ่าน ทางอินเตอร์เฟสของ iSeries Access. ผู้ใช้เซิร์ฟเวอร์ iSeries ที่ใช้เวิร์กสเตชันแบบจำกัดฟังก์ชันไม่สามารถลบอ็อบเจ็กต์ได้เช่นกัน, ถึงแม้ว่าผู้ใช้เซิร์ฟเวอร์ iSeries จะมีสิทธิพิเศษ *ALLOBJ. ก่อนที่อ็อบเจ็กต์จะถูกลบได้นั้น, ผู้ใช้ที่มีสิทธิจะต้องใช้ฟังก์ชันของพีซีเพื่อรีเซ็ตค่า read-only ให้เป็น `off`. ในลักษณะเดียวกัน, ผู้ใช้พีซีอาจไม่มีสิทธิของ OS/400 เพียงพอที่จะเปลี่ยนแอ็ตทริบิวต์ความปลอดภัย ที่เกี่ยวกับพีซีสำหรับอ็อบเจ็กต์ได้.

แอ็พพลิเคชันที่เป็น UNIX-type ที่ทำงานบนเซิร์ฟเวอร์ iSeries ใช้ application programming interfaces (APIs) ที่เป็นเหมือนยูนิกซ์ในการเข้าไปใช้ข้อมูลที่อยู่ในระบบไฟล์ราก. ด้วย APIs ที่เหมือนกับยูนิกซ์, แอ็พพลิเคชันสามารถรับรู้และรักษาข้อมูลด้านความปลอดภัยต่อไปนี้:

- Object owner (เจ้าของอ็อบเจ็กต์)
- Group owner (สิทธิในระดับกลุ่มหลัก ของเซิร์ฟเวอร์ iSeries)
- Read (ไฟล์)
- Write (เปลี่ยนแปลงเนื้อหา)
- Execute (รันโปรแกรมหรือค้นหาไดเร็กทอรี)

ระบบทำการจับคู่สิทธิในการใช้ข้อมูลเหล่านี้เข้ากับสิทธิอ็อบเจ็กต์ และสิทธิในการใช้ข้อมูลที่มีอยู่เดิมของเซิร์ฟเวอร์ iSeries :

- Read (*R) = *OBJOPR and *READ
- Write (*W) = *OBJOPR, *ADD, *UPD, *DLT
- Execute (*X) = *OBJOPR and *EXECUTE

แนวคิดของสิทธิอ็อบเจ็กต์อื่นๆ (*OBJMGT, *OBJEXIST, *OBJALTER, และ *OBJREF) ไม่มีในสภาพแวดล้อมแบบยูนิกซ์.

อย่างไรก็ตาม, สิทธิอ็อบเจ็กต์เหล่านี้มีอยู่ในทุกอ็อบเจ็กต์ในระบบไฟล์ราก. เมื่อคุณสร้างอ็อบเจ็กต์โดยใช้ API ที่เหมือนกับยูนิกซ์, อ็อบเจ็กต์นั้นจะสืบทอดสิทธิเหล่านี้จากไดเร็กทอรีบรรพบุรุษ (parent directory), ทำให้เกิดผลดังต่อไปนี้:

- เจ้าของของอ็อบเจ็กต์ใหม่ มีสิทธิอ็อบเจ็กต์ที่เหมือนกันกับเจ้าของไดเร็กทอรีบรรพบุรุษ .

- กลุ่มหลัก (primary group) ของอ็อบเจ็กต์กลุ่มใหม่จะมีสิทธิอ็อบเจ็กต์ที่เหมือนกับกลุ่มหลักของไดเร็กทอรีบรรพบุรุษ.
- กลุ่มผู้ใช้พับลิกของอ็อบเจ็กต์ใหม่มีสิทธิอ็อบเจ็กต์ที่เหมือนกับกลุ่มผู้ใช้พับลิกของไดเร็กทอรีบรรพบุรุษ.

มีการกำหนดสิทธิในการใช้ข้อมูลในอ็อบเจ็กต์ใหม่ของเจ้าของ, กลุ่มหลัก, และกลุ่มพับลิกบน API ด้วยพารามิเตอร์ mode. เมื่อสิทธิอ็อบเจ็กต์ทั้งหมดถูกกำหนดเป็น 'on', คุณจะได้สิทธิที่คุณอาจคาดหวังได้ในสภาพแวดล้อมแบบยูนิกซ์. จะเป็นการดีที่สุดที่จะกำหนดค่าเหล่านั้นทิ้งไว้เป็น 'on', นอกเสียจากคุณไม่ต้องการพฤติกรรมที่เหมือน POSIX.

เมื่อคุณรันแอ็พพลิเคชันที่ใช้ APIs ที่เหมือนกับยูนิกซ์, ระบบจะเป็นตัวกำหนดสิทธิอ็อบเจ็กต์ทั้งหมด, โดยไม่สนใจว่าสิทธิประเภทนั้นจะถูก "มองเห็น" ได้โดยแอพพลิเคชันประเภทยูนิกซ์หรือไม่. ตัวอย่างเช่น, ระบบจะบังคับใช้สิทธิของ authorization list แม้ว่าจะไม่มีแนวคิดของ authorization list อยู่ในระบบปฏิบัติการประเภทยูนิกซ์.

เมื่อคุณมีสภาพแวดล้อมที่มีแอ็พพลิเคชันหลายๆรูปแบบรวมกัน, คุณจำเป็นต้องแน่ใจว่าคุณไม่ได้เปลี่ยนแปลงสิทธิในสภาพแวดล้อมหนึ่ง แล้วส่งผลให้แอ็พพลิเคชันของคุณในสภาพแวดล้อมอื่นทำงานไม่ได้.

การทำงานเกี่ยวกับการรักษาความปลอดภัยสำหรับระบบไฟล์ราก (Root หรือ /), QOpenSys, และระบบไฟล์ที่ถูกกำหนดโดยผู้ใช้

พร้อมกันกับการแนะนำตัวของ integrated file system, เซิร์ฟเวอร์ iSeries ยังมีชุดคำสั่งใหม่สำหรับการทำงานกับอ็อบเจ็กต์ที่อยู่ในหลายๆ ระบบไฟล์. ชุดคำสั่งนี้ประกอบด้วยคำสั่งสำหรับการทำงานเกี่ยวกับการรักษาความปลอดภัย ดังนี้:

- Change Auditing (CHGAUD)
- Change Authority (CHGAUT)
- Change Owner (CHGOWN)
- Change Primary Group (CHGPGP)
- Display Authority (DSPAUT)
- Work with Authority (WRKAUT)

กลุ่มคำสั่งเหล่านี้ได้รวมสิทธิในการใช้ข้อมูลและสิทธิอ็อบเจ็กต์ต่อไปนี้ไว้ในเซ็ตย่อยของสิทธิที่เหมือนกับสิทธิในยูนิกซ์:

*__RWX__ Read/write/execute

*__RW__ Read/write

*__R__ Read

*__WX__ Write/execute

*__W__ Write

*__X__ Execute

นอกจากนี้, ยังมี APIs ที่เหมือนกับยูนิกซ์ API ที่มีไว้สำหรับทำงานเกี่ยวกับการรักษาความปลอดภัย.

สิทธิแบบพับลิกที่มีต่อไดเร็กทอรีราก

เมื่อระบบของคุณมาถึงในครั้งแรก, สิทธิพับลิกที่มีต่อไดเร็กทอรีราก คือ *ALL (สิทธิอ็อบเจ็กต์ทั้งหมดและสิทธิในการใช้ข้อมูลทั้งหมด). การตั้งค่านี้จะช่วยให้เกิดความยืดหยุ่นและการใช้แทนกันได้กับทั้งที่แอ็พพลิเคชันที่เหมือนยูนิกซ์ต้องการ และที่ผู้ใช้เซิร์ฟเวอร์ iSeries ทั่วๆ ไปต้องการ. ผู้ใช้เซิร์ฟเวอร์ iSeries ที่มีความสามารถใช้บรรทัดรับคำสั่งสามารถสร้างไลบรารีใหม่ในระบบไฟล์ QSYS.LIB อย่างง่ายดายด้วยการใช้คำสั่ง CRTLIB . โดยทั่วไป, สิทธิในการใช้งานบนเซิร์ฟเวอร์ iSeries โดยทั่วไปอนุญาตให้กระทำเช่นนี้. เช่นเดียวกับค่าติดตั้งเริ่มต้นของระบบไฟล์ราก, ผู้ใช้ทั่วไปสามารถสร้างไดเร็กทอรีใหม่ในระบบไฟล์ราก (เหมือนกับที่คุณสามารถสร้างไดเร็กทอรีใหม่บนเครื่องพีซีของคุณ).

ในฐานะผู้บริหารความปลอดภัย, คุณต้องให้ความรู้กับผู้ใช้ของคุณ เกี่ยวกับการป้องกันที่เพียงพอสำหรับ อ็อบเจ็กต์ที่พวกเขาสร้างขึ้น. เมื่อผู้ใช้สร้างไลบรารี, เป็นไปได้ที่สิทธิพับลิกในไลบรารีจะต้องไม่เป็น *CHANGE (ค่าดีฟอลต์). ผู้ใช้จะต้องกำหนดสิทธิพับลิกเป็น *USE หรือ *EXCLUDE โดยขึ้นกับเนื้อหาที่อยู่ในไลบรารี.

ถ้าผู้ใช้ต้องการสร้างไดเร็กทอรีใหม่ในระบบไฟล์ราก (/), ระบบไฟล์ QOpenSys หรือระบบไฟล์ที่ผู้ใช้กำหนด, คุณมีทางเลือกในการรักษาความปลอดภัยได้หลายทาง ได้แก่:

- คุณสามารถให้ความรู้แก่ผู้ใช้ของคุณให้ทำการแทนทับค่าสิทธิดีฟอลต์เดิม เมื่อพวกเขาสร้างไดเร็กทอรีใหม่. ค่าดีฟอลต์คือค่าที่สืบทอดมาจากไดเร็กทอรีบรรพบุรุษ. ในกรณีที่ไดเร็กทอรีใหม่อยู่ในไดเร็กทอรีราก, สิทธิพับลิกที่เป็นดีฟอลต์ จะเป็น *ALL.
- คุณสามารถสร้างไดเร็กทอรีย่อย "ต้นแบบ" ภายใต้ไดเร็กทอรีรากได้. ให้กำหนดสิทธิพับลิกบนไดเร็กทอรีต้นแบบ เป็นค่าที่เหมาะสมกับองค์กรของคุณ. จากนั้นแนะนำให้ผู้ใช้สร้างไดเร็กทอรีส่วนตัวภายใต้ไดเร็กทอรีต้นแบบนี้. ไดเร็กทอรีของผู้ใช้จะสืบทอดสิทธิจากไดเร็กทอรีต้นแบบ.
- คุณสามารถพิจารณาที่จะเปลี่ยนสิทธิพับลิกของไดเร็กทอรีราก เพื่อป้องกันไม่ให้ผู้ใช้สร้างอ็อบเจ็กต์ในไดเร็กทอรีนั้น. (โดยการลบสิทธิ *W, *OBJEXIST, *OBJALTER, *OBJREF, และ *OBJMGT) อย่างไรก็ตาม, คุณจำเป็นต้องประเมินดูว่าการเปลี่ยนแปลงนี้ จะก่อให้เกิดปัญหากับแอ็พพลิเคชันของคุณบ้างหรือไม่. ตัวอย่างเช่น, คุณอาจมีแอ็พพลิเคชันแบบยูนิกซ์ที่คาดว่าจะสามารถลบอ็อบเจ็กต์ออกจากไดเร็กทอรีรากได้.

คำสั่ง Print private authorities objects (PRTPVTAUT)

คำสั่ง Print Private Authorities (PRTPVTAUT) อนุญาตให้คุณพิมพ์รายงานของสิทธิไพรเวตทั้งหมดที่มีต่อชนิดของอ็อบเจ็กต์ที่กำหนดในไลบรารี, โฟลเดอร์, หรือไดเร็กทอรีที่กำหนด. ในรายงานแสดงถึงอ็อบเจ็กต์ทั้งหมดตามประเภทที่กำหนด และรายชื่อผู้ใช้ที่มีสิทธิในอ็อบเจ็กต์. ซึ่งเป็นวิธีการที่ใช้ตรวจสอบต้นทางที่แตกต่างกันของสิทธิในอ็อบเจ็กต์นั้น.

คำสั่งนี้พิมพ์รายงาน 3 ประเภทสำหรับอ็อบเจ็กต์ที่ถูกเลือก. รายงานฉบับแรก (รายงานฉบับเต็ม–Full Report) แสดงสิทธิไพรเวตทั้งหมดของแต่ละอ็อบเจ็กต์ที่ถูกเลือกไว้. รายงานฉบับที่สอง (รายงานส่วนที่เปลี่ยนแปลง–Changed Report) แสดงถึงส่วนที่เพิ่มเติมและเปลี่ยนแปลงของสิทธิไพรเวตในอ็อบเจ็กต์ ถ้าก่อนหน้านี้มีการรันคำสั่ง PRTPVTAUT ให้กับอ็อบเจ็กต์ที่กำหนดในไลบรารี, โฟลเดอร์, หรือไดเร็กทอรีที่กำหนด. จะมีการแสดงอ็อบเจ็กต์ใหม่ของประเภทที่ถูกเลือกไว้ใดๆ, สิทธิใหม่ของอ็อบเจ็กต์เดิม, หรือการเปลี่ยนแปลงของสิทธิเดิมในอ็อบเจ็กต์เดิม ในรายงานส่วนที่

เปลี่ยนแปลง (Changed Report). ถ้าไม่มีการรันคำสั่ง PRTPVTAUT มาก่อนให้กับอ็อบเจ็กต์ที่กำหนดในไลบรารี, โฟลเดอร์ หรือไดเร็กทอรีที่กำหนด, ก็จะไม่มีรายงานส่วนที่เปลี่ยนแปลง. และถ้ามีการรันคำสั่งนี้มาก่อนแต่ไม่มีการเปลี่ยนแปลงเกิดขึ้นกับสิทธิในอ็อบเจ็กต์, จะมีการพิมพ์รายการการเปลี่ยนแปลง แต่จะไม่มีอ็อบเจ็กต์แสดงไว้.

รายงานฉบับที่สาม (รายงานการลบ–Deleted Report) แสดงการลบของผู้ใช้ที่มีสิทธิไพรเวตจากอ็อบเจ็กต์ที่กำหนด เมื่อมีการรัน คำสั่ง PRTPVTAUT ไปก่อนหน้านี้. จะมีการแสดงอ็อบเจ็กต์ที่ถูกลบ หรือผู้ใช้ที่ถูกถอนออกจากผู้ใช้ที่มีสิทธิไพรเวตในรายงานการลบ(Deleted Report). หากไม่เคยมีการรันคำสั่ง PRTPVTAUT มาก่อน, จะไม่มีรายการการลบ. ถ้าเคยมีการรันคำสั่ง แต่ไม่มีการลบเกิดขึ้นกับอ็อบเจ็กต์, จะมีการพิมพ์รายงานการลบ แต่จะไม่มีอ็อบเจ็กต์แสดงไว้.

ข้อจำกัด: คุณต้องมีสิทธิพิเศษ *ALLOBJ ในการใช้คำสั่งนี้.

ตัวอย่าง:

คำสั่งนี้สร้างรายงานฉบับเต็ม, รายงานส่วนที่เปลี่ยนแปลง, และรายงานการลบของอ็อบเจ็กต์ไฟล์ทั้งหมดใน PAYROLLLIB:

```
PRTPVTAUT OBJTYPE(*FILE) LIB(PAYROLLLIB)
```

คำสั่งนี้สร้างรายงานฉบับเต็ม, รายงานส่วนที่เปลี่ยนแปลง, และรายงานการลบสำหรับอ็อบเจ็กต์สตรีมไฟล์ทั้งหมดใน ไดเร็กทอรี garry:

```
PRTPVTAUT OBJTYPE(*STMF) DIR(/GARRY) SCHSUBDIR(*NO)
```

คำสั่งนี้สร้างรายงานฉบับเต็ม, รายงานส่วนที่เปลี่ยนแปลง, และรายงานการลบสำหรับอ็อบเจ็กต์สตรีมไฟล์ทั้งหมด ในโครงสร้างไดเร็กทอรีย่อย ซึ่งเริ่มที่ไดเร็กทอรี garry:

```
PRTPVTAUT OBJTYPE(*STMF) DIR(/GARRY) SCHSUBDIR(*YES)
```

คำสั่ง Print publicly authorized objects (PRTPUBAUT)

คำสั่ง Print Publicly Authorized Objects (PRTPUBAUT) ยอมให้คุณพิมพ์รายงานของอ็อบเจ็กต์ที่กำหนดที่ไม่มีสิทธิพับลิกแบบ *EXCLUDE. สำหรับอ็อบเจ็กต์ *PGM, จะมีโปรแกรมที่ไม่มีสิทธิพับลิก *EXCLUDE ที่ผู้ใช้สามารถเรียกได้ (โปรแกรมที่เป็นโดเมนผู้ใช้หรือมีระดับความปลอดภัยของระบบ (ค่ากำหนดของระบบ QSECURITY) น้อยกว่าหรือเท่ากับ 30) รวมอยู่ในรายงานนี้. นี่เป็นวิธีในการตรวจสอบอ็อบเจ็กต์ที่ผู้ใช้ทุกคนในระบบมีสิทธิที่จะเข้าถึง.

คำสั่งนี้พิมพ์รายงาน 2 ประเภท. รายงานแรก (รายงานฉบับเต็ม) จะแสดงอ็อบเจ็กต์ที่กำหนดทั้งหมดที่ไม่มีสิทธิพับลิก *EXCLUDE. รายงานที่สอง (รายงานส่วนที่เปลี่ยนแปลง) จะแสดงอ็อบเจ็กต์ที่ไม่มีสิทธิพับลิก *EXCLUDE ในปัจจุบัน แต่อาจเคยมีสิทธิพับลิก *EXCLUDE หรือไม่มีอยู่เมื่อมีการรันคำสั่ง PRTPUBAUT ไปก่อนหน้านี้. ถ้าก่อนหน้านี้ไม่มีการรันคำสั่ง PRTPUBAUT ให้กับอ็อบเจ็กต์และไลบรารี, โฟลเดอร์ หรือไดเร็กทอรีที่กำหนด, จะไม่มีรายงานส่วนที่เปลี่ยนแปลง. แต่ถ้าก่อนหน้านี้มีการรันคำสั่งแต่ไม่มีอ็อบเจ็กต์ที่มีสิทธิพับลิก *EXCLUDE เพิ่มขึ้น, จะมีการพิมพ์รายการส่วนที่เปลี่ยนแปลงแต่จะไม่มีอ็อบเจ็กต์แสดงไว้.

ข้อจำกัด: คุณต้องมีสิทธิพิเศษ *ALLOBJ ในการใช้คำสั่งนี้.

ตัวอย่าง:

คำสั่งนี้สร้างรายงานฉบับเต็ม, รายงานส่วนที่เปลี่ยนแปลงสำหรับทุกอ็อบเจ็กต์ไฟล์ในไลบรารี GARRY ที่ไม่มีสิทธิพับลิก *EXCLUDE:

```
PRTPUBAUT OBJTYPE(*FILE) LIB(GARRY)
```

คำสั่งนี้สร้างรายงานฉบับเต็ม, รายงานส่วนที่เปลี่ยนแปลง, และรายงานการลบสำหรับอ็อบเจ็กต์สตรีมไฟล์ทั้งหมด ในโครงสร้างไดเร็กทอรีย่อย ซึ่งเริ่มที่ไดเร็กทอรี garry ที่ไม่มีสิทธิพับลิก *EXCLUDE:

```
PRTPUBAUT OBJTYPE(*STMF) DIR(GARRY) SCHSUBDIR(*YES)
```

การจำกัดการเข้าถึงระบบไฟล์ QSYS.LIB

เนื่องจากระบบไฟล์ราก (/) เป็นระบบไฟล์แบบร่ม, ระบบไฟล์ QSYS.LIB ปรากฏเป็นไดเร็กทอรีย่อยภายในไดเร็กทอรีราก. ดังนั้น,ผู้ใช้พีซีใดๆ ที่สามารถเข้าถึงเซิร์ฟเวอร์ iSeries ได้จะสามารถจัดการกับอ็อบเจ็กต์ที่ถูกเก็บอยู่ในไลบรารีของเซิร์ฟเวอร์ iSeries (ระบบไฟล์ QSYS.LIB) ด้วยคำสั่งและการทำงานโดยปกติของพีซี. ตัวอย่างเช่น, ผู้ใช้พีซีสามารถลากอ็อบเจ็กต์ QSYS.LIB (หรือไลบรารีที่มีไฟล์ข้อมูลที่สำคัญอย่างมากต่อคุณ) ไปยังเครื่องทำลาย (shredder หรือ trash).

ตามที่คุณได้เรียนรู้ใน “ระบบไฟล์ราก (Root หรือ /), QOpenSys, และระบบไฟล์ที่ผู้ใช้กำหนดขึ้นเอง” ในหน้า 105, ระบบจะปฏิบัติตามสิทธิอ็อบเจ็กต์ทั้งหมด ไม่ว่าจะสามารถมองผ่านไปยังอินเตอร์เฟสได้หรือไม่. ดังนั้น, ผู้ใช้ไม่สามารถทำลาย (ลบ) อ็อบเจ็กต์ได้ ถ้าผู้ใช้ไม่มี *OBJEXIST ในอ็อบเจ็กต์. อย่างไรก็ตาม, ถ้า iSeries ของคุณขึ้นกับความปลอดภัยของการเข้าถึงเมนู (menu access security) มากกว่าความปลอดภัยของอ็อบเจ็กต์ (object security), ผู้ใช้พีซีจะสามารถค้นพบอ็อบเจ็กต์ที่มีในระบบไฟล์ QSYS.LIB เพื่อจะทำลายได้.

การที่คุณขยายการใช้ระบบของคุณ และวิธีต่างๆ ในการเข้าถึงที่คุณจัดหาให้, คุณจะค้นพบในไม่ช้าว่าความปลอดภัยของการเข้าถึงเมนูไม่เพียงพอ. บทที่ 5, “ปกป้องข้อมูลทรัพย์สินด้วยสิทธิอ็อบเจ็กต์”, ในหน้า 47 กล่าวถึงกลยุทธ์สำหรับเสริมการควบคุมการเข้าถึงเมนูด้วยความปลอดภัยอ็อบเจ็กต์. อย่างไรก็ตาม, เซิร์ฟเวอร์ iSeries ยังมีวิธีง่ายๆ สำหรับคุณในการป้องกันการเข้าถึงระบบไฟล์ QSYS.LIB โดยผ่านทางโครงสร้างไดเร็กทอรีของระบบไฟล์ราก. คุณสามารถใช้ QPWFSERVER authorization list เพื่อควบคุมว่าผู้ใช้ใดสามารถเข้าถึงระบบไฟล์ QSYS.LIB ผ่านทางไดเร็กทอรีราก.

เมื่อสิทธิของผู้ใช้ใน PWFSERVER authorization list เป็น *EXCLUDE, ผู้ใช้ไม่สามารถเข้าไปในไดเร็กทอรี QSYS.LIB จากโครงสร้างไดเร็กทอรีราก. แต่เมื่อสิทธิของผู้ใช้เป็น *USE, ผู้ใช้จะสามารถเข้าไปในไดเร็กทอรีได้. เมื่อผู้ใช้มีสิทธิเข้าไปในไดเร็กทอรี,สิทธิอ็อบเจ็กต์จะประยุกต์กับการกระทำที่ผู้ใช้ต้องการดำเนินการกับอ็อบเจ็กต์ภายในระบบไฟล์ QSYS.LIB. หรือพูดอีกนัยหนึ่งก็คือ, สิทธิใน QPWFSERVER authorization list ทำหน้าที่เหมือนประตูสู่ระบบไฟล์ QSYS.LIB. สำหรับผู้ใช้ที่มีสิทธิ *EXCLUDE, ประตูจะปิดล็อก. และผู้ใช้ที่มีสิทธิ *USE (หรือสิทธิอื่นที่มากกว่านี้), ประตูนั้นจะเปิด.

ในสถานการณ์ส่วนใหญ่, ผู้ใช้ไม่จำเป็นต้องใช้ส่วนติดต่อไดเร็กทอรี (directory interface) เพื่อเข้าถึงอ็อบเจ็กต์ในระบบไฟล์ QSYS.LIB. เป็นไปได้ที่คุณต้องการกำหนดสิทธิพับลิกไปยัง QPWFSERVER authorization list เป็น *EXCLUDE. ให้ระลึกไว้เสมอว่าสิทธิใน authorization list เป็นการเปิดหรือปิดประตูไปยังทุกไลบรารีภายในระบบไฟล์ QSYS.LIB, ซึ่งรวมถึงไลบรารีผู้ใช้. ถ้าคุณมีผู้ใช้ที่คัดค้านการแยกสิทธินี้, คุณสามารถประเมินความต้องการเป็นกรณีๆ ไป. ถ้าเหมาะสม, คุณสามารถให้สิทธิผู้ใช้แต่ละคนไปยัง authorization. อย่างไรก็ตาม, คุณจำเป็นต้องแน่ใจว่าผู้ใช้มีสิทธิที่เหมาะสมในอ็อบเจ็กต์ที่อยู่ในระบบไฟล์ QSYS.LIB. มิฉะนั้น, ผู้ใช้อาจลบอ็อบเจ็กต์หรือทั้งไลบรารีโดยไม่ตั้งใจได้.

หมายเหตุ:

1. เมื่อระบบของคุณมาถึงในครั้งแรก, สิทธิพับลิกใน QPWFSERVER authorization list คือ *USE.
2. ถ้าคุณให้สิทธิแก่ผู้ใช้แต่ละราย, authorization list control จะเข้าถึงเฉพาะการบริการไฟล์ iSeries Access, การบริการไฟล์ NetServer และ การบริการไฟล์ระหว่างเซิร์ฟเวอร์ iSeries. ซึ่งไม่ได้ป้องกันการเข้าถึงไดเร็กทอรีเดียวกันโดยผ่านทาง FTP, ODBC หรือเครือข่ายอื่นๆ .

การรักษาความปลอดภัยให้กับไดเร็กทอรีต่างๆ

เพื่อเข้าถึงอ็อบเจ็กต์ภายในระบบไฟล์ราก, คุณต้องอ่านผ่านพาธทั้งหมดไปยังอ็อบเจ็กต์นั้น. ในการค้นหาไดเร็กทอรี, คุณต้องมีสิทธิ *X (*OBJOPR และ *EXECUTE) ในไดเร็กทอรีนั้น. ตัวอย่างเช่น, สมมุติว่าคุณต้องการเข้าถึงอ็อบเจ็กต์ดังนี้:

```
/companya/customers/custfile.dat
```

คุณต้องมีสิทธิ *X ในไดเร็กทอรี `companya` และในไดเร็กทอรี `customers` .

ด้วยระบบไฟล์ราก, คุณสามารถสร้างการเชื่อมโยงสัญลักษณ์ (symbolic link) ไปยังอ็อบเจ็กต์. โดยหลักการแล้ว, การเชื่อมโยงสัญลักษณ์ คือ alias สำหรับชื่อพาธ. ซึ่งปกติจะสั้นกว่าและง่ายต่อการจำมากกว่าชื่อพาธเต็ม. อย่างไรก็ตาม, การเชื่อมโยงสัญลักษณ์ไม่ได้สร้างพาธจริงไปยังอ็อบเจ็กต์. ผู้ใช้ยังต้องการสิทธิ *X ในทุกไดเร็กทอรีและไดเร็กทอรีย่อยในพาธจริงไปยังอ็อบเจ็กต์.

สำหรับอ็อบเจ็กต์ในระบบไฟล์ราก, คุณสามารถใช้ความปลอดภัยของไดเร็กทอรีเช่นเดียวกับที่คุณสามารถใช้ความปลอดภัยของไลบรารี กับระบบไฟล์ QSYS.LIB. ตัวอย่างเช่น, คุณสามารถกำหนดสิทธิพับลิกของไดเร็กทอรีเป็น *EXCLUDE เพื่อป้องกันผู้ใช้พับลิกจากการเข้าถึงอ็อบเจ็กต์ใดๆ ภายในไดเร็กทอรีนั้น.

การรักษาความปลอดภัยสำหรับอ็อบเจ็กต์ใหม่

เมื่อคุณสร้างอ็อบเจ็กต์ใหม่ในระบบไฟล์ราก, อินเตอร์เฟสที่คุณใช้เพื่อสร้างอ็อบเจ็กต์จะเป็นตัวกำหนดสิทธิของอ็อบเจ็กต์. ตัวอย่างเช่น, ถ้าคุณใช้คำสั่ง CRTDIR และค่าดีฟอลต์ของคำสั่ง, ไดเร็กทอรีใหม่จะรับการถ่ายทอดคุณลักษณะของสิทธิทั้งหมดของ ไดเร็กทอรีแม่, ซึ่งรวมถึงสิทธิไพรเวต, สิทธิของกลุ่มหลัก, และความสัมพันธ์ของ authorization list. ในส่วนถัดไปจะอธิบายถึงวิธีการกำหนดสิทธิสำหรับอินเตอร์เฟสแต่ละประเภท.

สิทธิมาจากไดเร็กทอรีแม่โดยตรง, ไม่ได้มาจากไดเร็กทอรีที่อยู่สูงขึ้นไปใน tree. ดังนั้น, ในฐานะผู้บริหารความปลอดภัย, คุณจำเป็นต้องดูสิทธิที่คุณกำหนดให้ไดเร็กทอรีในลำดับชั้นจากสองมุมมอง:

- สิทธิมีผลกระทบต่อการเข้าถึงอ็อบเจ็กต์ใน tree อย่างไร (คล้ายกับสิทธิไลบรารี).
- สิทธิมีผลกระทบต่อการสร้างอ็อบเจ็กต์ใหม่อย่างไร (คล้ายกับค่า CRTAUT สำหรับไลบรารี).

คำแนะนำ: คุณอาจต้องการให้ผู้ใช้ที่ทำงานในระบบไฟล์รวมมีไดเร็กทอรีหลัก (home directory) (ตัวอย่างเช่น, /home/usrxxx), จากนั้นกำหนดความปลอดภัยที่เหมาะสม (เช่น PUBLIC *EXCLUDE). ไดเร็กทอรีใดๆ ที่ผู้ใช้สร้างขึ้น ภายใต้ไดเร็กทอรี home จะรับการถ่ายทอดสิทธิเหล่านั้นมาด้วย.

ส่วนถัดไปเป็นคำอธิบายเกี่ยวกับการสืบทอดสิทธิสำหรับอินเตอร์เฟสที่ต่างกัน:

การใช้คำสั่ง Create Directory

เมื่อคุณสร้างไดเร็กทอรีใหม่โดยใช้คำสั่ง CRTDIR, คุณมีสองทางเลือกในการกำหนดสิทธิ:

- คุณสามารถกำหนดสิทธิพับลิก(สิทธิในการใช้ข้อมูล, สิทธิอ็อบเจ็กต์, หรือทั้งคู่).
- คุณสามารถกำหนดค่า *INDIR สำหรับสิทธิในการใช้ข้อมูล, สิทธิอ็อบเจ็กต์, หรือทั้งคู่. เมื่อคุณกำหนดค่า *INDIR ให้กับสิทธิในการใช้ข้อมูลและสิทธิอ็อบเจ็กต์, ระบบจะทำการก็อปปี้ข้อมูลเกี่ยวกับสิทธิทั้งหมดจากไดเร็กทอรีแม่ไปยังอ็อบเจ็กต์ใหม่, รวมถึง authorization list, กลุ่มหลัก (primary group), สิทธิพับลิก, และสิทธิไพรเวต. (ระบบไม่ได้ก็อปปี้สิทธิไพรเวตที่โปรไฟล์ QSYS หรือโปรไฟล์ QSECOFR มีไปยังอ็อบเจ็กต์.)

การสร้างไดเร็กทอรีด้วย API

เมื่อคุณสร้างไดเร็กทอรีด้วยการใช้ API mkdir(), คุณต้องกำหนดสิทธิในการใช้ข้อมูลให้กับเจ้าของ, กลุ่มหลัก,และพับลิก (โดยใช้การจับคู่สิทธิ (authority map) ของ *R, *W, และ *X). ระบบใช้ข้อมูลในไดเร็กทอรีบรรพบุรุษในการตั้งค่าสิทธิอ็อบเจ็กต์สำหรับเจ้าของ, กลุ่มหลัก, และพับลิก.

เนื่องจากระบบปฏิบัติการแบบยูนิกซ์ไม่มีแนวคิดเกี่ยวกับสิทธิอ็อบเจ็กต์, API mkdir() จึงไม่สนับสนุน การระบุสิทธิอ็อบเจ็กต์. ถ้าคุณต้องการสิทธิอ็อบเจ็กต์ที่ต่างกัน, คุณสามารถใช้คำสั่งของเซิร์ฟเวอร์ iSeries (CHGAUT). อย่างไรก็ตาม, เมื่อคุณลบสิทธิอ็อบเจ็กต์บางตัว, การทำงานของแอ็พพลิเคชันแบบยูนิกซ์อาจไม่เป็นไปตามที่คุณคาดไว้.

การสร้างไฟล์ stream ด้วยAPI แบบ open() หรือ creat()

เมื่อคุณใช้ API creat() ในการสร้างสตรีมไฟล์, คุณสามารถกำหนดสิทธิในการใช้ข้อมูลของเจ้าของ, กลุ่มหลัก, และพับลิก (โดยการใช้สิทธิที่เหมือนกับยูนิกซ์ *R, *W, และ *X). ระบบใช้ข้อมูลในไดเร็กทอรีบรรพบุรุษในการตั้งค่าสิทธิอ็อบเจ็กต์สำหรับเจ้าของ, กลุ่มหลัก, และพับลิก.

คุณยังสามารถกำหนดสิทธิเหล่านี้ได้เมื่อคุณใช้ API แบบ open() ในการสร้างไฟล์สตรีม. ในอีกทางหนึ่ง, เมื่อคุณใช้ API แบบ open() คุณสามารถกำหนดให้อ็อบเจ็กต์นั้นต้องสืบทอดสิทธิทั้งหมดจากไดเร็กทอรีบรรพบุรุษ. ซึ่งจะเรียกว่า `inherit mode`. เมื่อคุณกำหนดโหมด inherit, ระบบจะ

สร้างคู่เหมือนของสิทธิใน ไดเร็กทอรีบรรพบุรุษ, รวมถึง authorization list, กลุ่มหลัก, สิทธิพับลิก และสิทธิไพรเวต. ทางเลือกนี้ทำงานคล้ายกับการกำหนดค่า *INDIR บนคำสั่ง CRTDIR.

การสร้างอ็อบเจ็กต์โดยการใช้อินเตอร์เฟสของพีซี

เมื่อคุณใช้แอ็พพลิเคชันของพีซีสร้างอ็อบเจ็กต์ในระบบไฟล์ราก, ระบบจะสืบทอดสิทธิ ทั้งหมดจากไดเร็กทอรีแม่โดยอัตโนมัติ. รวมถึง authorization list, กลุ่มหลัก, สิทธิพับลิก, และสิทธิไพรเวต. โดยที่แอ็พพลิเคชันของพีซีไม่ต้องมีการกำหนดสิทธิที่เหมือนกันเมื่อคุณสร้างอ็อบเจ็กต์นั้น.

ระบบไฟล์ QFileSvr.400

ด้วยระบบไฟล์ QFileSvr.400, ผู้ใช้ (USERX) บนระบบ iSeries (SYSTEMA) สามารถเข้าถึงข้อมูลในระบบ iSeries อีกระบบที่ต่อกันอยู่ (SYSTEMB). USERX มีอินเตอร์เฟสที่เหมือนกับอินเตอร์เฟส Client Access. เซิร์ฟเวอร์รีโมต iSeries (SYSTEMB) จะปรากฏเป็นไดเร็กทอรีที่มีระบบไฟล์ทั้งหมดของมันเป็นไดเร็กทอรีย่อย.

เมื่อ USERX พยายามเข้าถึง SYSTEMB ด้วยอินเตอร์เฟสนี้, SYSTEMA จะส่งโปรไฟล์ผู้ใช้ของ USERX และ รหัสผ่านที่ได้เข้ารหัสไว้ไปยัง SYSTEMB. จะต้องมีโปรไฟล์ผู้ใช้และรหัสผ่านเดียวกันอยู่บน SYSTEMB, มิฉะนั้น SYSTEMB อาจปฏิเสธการร้องขอนั้น.

ถ้า SYSTEMB ยอมรับการร้องขอ, USERX จะปรากฏต่อ SYSTEMB เหมือนกับผู้ใช้ Client Access. กฎในการตรวจสอบสิทธิทุกอย่างจะถูกใช้กับ การกระทำทุกอย่างของ USERX.

ในฐานะผู้บริหารความปลอดภัย, คุณจำเป็นต้องตระหนักว่าระบบไฟล์ QFileSrv.400 เป็นเหมือนอีกประตูหนึ่งที่เข้าสู่ระบบของคุณ. คุณไม่สามารถถือเอาว่าคุณได้จำกัดผู้ใช้รีโมตของคุณกับการ sign on แบบโต้ตอบด้วยการส่งผ่าน display station. ถ้าคุณมีระบบย่อย QSERVER ทำงานอยู่และระบบของคุณต่อเข้ากับระบบ iSeries อื่น, ผู้ใช้แบบรีโมตจะสามารถเข้าถึงระบบของคุณเหมือนกับว่าทำงานอยู่บนพีซีโลคัลที่รัน Client Access. ยิ่งไปกว่านั้น, ระบบของคุณจะมีการเชื่อมต่อที่ต้องการมีระบบย่อย QSERVER ทำงานอยู่. นี่คืออีกเหตุผลหนึ่งที่ทำให้ทราบว่า ทำไมโครงร่างของสิทธิอ็อบเจ็กต์ (object authority scheme) จึงมีความสำคัญมาก.

ระบบไฟล์ของระบบเครือข่าย

Network File System (NFS) จะให้การเข้าถึงไปยังและจากระบบที่มีการใช้ NFS เช่นกัน. NFS เป็นวิธีการที่เป็นมาตรฐานอตุสาหกรรมในการใช้ข้อมูลร่วมกันระหว่างผู้ใช้บนระบบเครือข่าย. ระบบปฏิบัติการที่สำคัญส่วนใหญ่ (รวมทั้งระบบปฏิบัติการพีซี) จะมี NFS. สำหรับระบบ UNIX, NFS เป็นวิธีการหลักในการเข้าถึงข้อมูล. เซิร์ฟเวอร์ iSeries สามารถแสดงตัวเป็นได้ทั้งไคลเอ็นต์ของ NFS และเซิร์ฟเวอร์ของ NFS.

เมื่อคุณเป็นผู้บริหารความปลอดภัยของระบบ iSeries ที่ทำหน้าที่เป็นเซิร์ฟเวอร์ NFS, คุณจำเป็นต้องทำความเข้าใจและจัดการกับหลักเกณฑ์ความปลอดภัยของ NFS. คำแนะนำและข้อควรพิจารณามีดังต่อไปนี้:

- คุณต้องเรียกใช้ฟังก์ชันของเซิร์ฟเวอร์ NFS โดยใช้คำสั่ง STRNFSSVR. ต้องควบคุมว่าใครที่จะมีสิทธิในการใช้คำสั่งนี้.
- คุณสร้างไดเร็กทอรีหรืออ็อบเจ็กต์ที่มีสำหรับไคลเอ็นต์ของ NFS โดยการ export. เพราะฉะนั้น, คุณสามารถมีการควบคุมเฉพาะสำหรับส่วนของระบบของคุณที่คุณต้องการให้มีสำหรับไคลเอ็นต์ของ NFS ในเครือข่ายของคุณ.
- เมื่อคุณ export, คุณสามารถกำหนดให้ไคลเอ็นต์ใดมีสิทธิเข้าถึงอ็อบเจ็กต์. คุณระบุไคลเอ็นต์โดยใช้ชื่อของระบบหรือ IP แอดเดรส. ไคลเอ็นต์สามารถเป็นพีซีส่วนบุคคล, เซิร์ฟเวอร์ iSeries ทั้งหมด หรือระบบ UNIX . ในคำศัพท์เฉพาะของ NFS, จะเรียกไคลเอ็นต์ (IP แอดเดรส) ว่า machine.
- เมื่อคุณทำการ export, คุณสามารถกำหนดการเข้าถึงแบบอ่านอย่างเดียว (read-only) หรืออ่าน/เขียน (read/write) สำหรับแต่ละเครื่องที่เข้าถึงไดเร็กทอรีหรืออ็อบเจ็กต์ที่ถูก export มา. โดยส่วนใหญ่, คุณมักจะต้องการให้เข้าถึงแบบ read-only.
- NFS ไม่มีการปกป้องรหัสผ่าน. เนื่องจากถูกออกแบบมาโดยมีจุดประสงค์สำหรับการแบ่งใช้ข้อมูลภายในระบบของกลุ่ม ที่เชื่อถือกันได้. เมื่อผู้ใช้ร้องขอที่จะเข้าถึง, เซิร์ฟเวอร์จะได้รับ uid ของผู้ใช้. ต่อไปนี้เป็นข้อควรพิจารณา บางอย่างสำหรับ uid :
  - เซิร์ฟเวอร์ iSeries พยายามที่จะระบุตำแหน่งของโปรไฟล์ผู้ใช้ด้วย uid เดียวกัน. ถ้ามีการพบ uid ที่ตรงกัน, ก็จะมีการใช้credential ของโปรไฟล์ผู้ใช้. Credential เป็นคำของ NFS ที่อธิบายการใช้สิทธิของผู้ใช้. ซึ่งจะคล้ายคลึงกันกับการสลับค่าโปรไฟลู่ในเซิร์ฟเวอร์แอ็พพลิเคชัน iSeries อื่นๆ.
  - เมื่อคุณ export ไดเร็กทอรีหรืออ็อบเจ็กต์, คุณสามารถกำหนดว่าคุณจะยอมให้เข้าถึงโดยโปรไฟล์ที่มีสิทธิในรากหรือไม่. เซิร์ฟเวอร์ NFS บนเซิร์ฟเวอร์ iSeries มีค่าสิทธิในการใช้งานของ root เป็นสิทธิในการใช้งานพิเศษ *ALLOBJ . ถ้าคุณกำหนดว่าคุณไม่ยอมให้มีสิทธิของ root, ผู้ใช้ NFS ที่มี uid ซึ่งแม็พไปยังโปรไฟล์ผู้ใช้ที่มีสิทธิพิเศษ *ALLOBJ จะไม่สามารถเข้าถึงอ็อบเจ็กต์ภายใต้โปรไฟล์นั้น. และถ้ายอมให้มีการเข้าถึงแบบไม่ต้องระบุผู้ใช้ (anonymous access), ผู้ร้องขอจะถูกแม็พไปยังโปรไฟล์ anonymous.
  - เมื่อคุณทำการ export ไดเร็กทอรีหรืออ็อบเจ็กต์, คุณสามารถระบุว่าคุณจะยอมให้มีการร้องขอแบบไม่ระบุชื่อ (anonymous request) หรือไม่. การร้องขอแบบไม่ระบุชื่อคือการร้องขอด้วย uid ที่ไม่ตรงกับ uid ใดๆ ในระบบของคุณ. ถ้าคุณเลือกที่จะยอมให้มีการร้องขอแบบไม่ระบุชื่อ, ระบบจะแม็พผู้ใช้ที่ไม่ต้องระบุชื่อไปยังโปรไฟล์ผู้ใช้ QNFSANON ที่ IBM กำหนดให้. โปรไฟล์ผู้ใช้นี้จะไม่มีสิทธิพิเศษใดๆ หรือสิทธิใดๆ ที่ชัดแจ้ง. (ในการ export, คุณสามารถกำหนดโปรไฟล์ผู้ใช้ที่แตกต่างไปสำหรับการร้องขอที่ไม่ต้องระบุชื่อได้ หากคุณต้องการ.)
- เมื่อเซิร์ฟเวอร์ iSeries เข้าร่วมในเครือข่าย NFS (หรือเครือข่ายใดๆ ที่มีระบบ UNIX ที่ขึ้นอยู่กับ uid), คุณอาจจะต้องการจัดการ uid ของคุณเองแทนที่จะปล่อยให้ระบบทำการกำหนดค่าให้โดยอัตโนมัติ. คุณจำเป็นต้องประสานเรื่อง uid ให้กับระบบอื่นๆ ในเครือข่ายของคุณ.

  คุณอาจพบว่าคุณจำเป็นต้องเปลี่ยน uid (แม้แต่กับโปรไฟล์ผู้ใช้ที่ IBM กำหนดให้) เพื่อที่จะเข้ากันได้กับระบบอื่นในเครือข่ายของคุณ. โปรแกรมจะมีไว้เพื่อทำให้การเปลี่ยน uid สำหรับโปรไฟล์ผู้ใช้ง่ายขึ้น. (เมื่อคุณเปลี่ยน uid สำหรับโปรไฟล์ผู้ใช้, คุณยังจำเป็นต้องเปลี่ยน uid สำหรับทุกอ็อบเจ็กต์ที่โปรไฟล์เป็นเจ้าของ ทั้งในไดเร็กทอรีรากหรือในไดเร็กทอรี QOpenSrv.)

โปรแกรม QSYCHGID เปลี่ยน `uid` โดยอัตโนมัติทั้งในโปรไฟล์ผู้ใช้และทุกอ็อบเจ็กต์ที่โปรไฟล์เป็นเจ้าของ. สำหรับข้อมูลเพิ่มเติมเกี่ยวกับการใช้โปรแกรมนี้, โปรดดูในหนังสือคู่มือ *iSeries System API Reference* book.

บทที่ 12. การรักษาความปลอดภัยให้กับการสื่อสารแบบ APPC

เมื่อระบบของคุณเข้าร่วมกับระบบอื่นในเครือข่าย, จะทำให้มีช่องทางใหม่ๆ ในการเข้าสู่ระบบของคุณ. ในฐานะของผู้บริหารความปลอดภัย, คุณต้องตระหนักถึงทางเลือกที่คุณสามารถใช้เพื่อควบคุมทางเข้าไปยัง ระบบของคุณในสภาวะแวดล้อมแบบ APPC.

การสื่อสารแบบก้าวหน้าระหว่างโปรแกรมไปยังโปรแกรม (Advanced program-to-program communication หรือ APPC) เป็นวิธีที่คอมพิวเตอร์, รวมไปถึงคอมพิวเตอร์ส่วนบุคคล, สื่อสารระหว่างกัน. จอภาพ pass-through, การจัดการข้อมูลแบบกระจาย, และ iSeries Access for Windows สามารถใช้การสื่อสารแบบ APPC ได้ทั้งสิ้น.

หัวข้อต่อไปจะให้ข้อมูลพื้นฐานเกี่ยวกับว่า การสื่อสาร APPC ทำงานอย่างไร และคุณจะสามารถจัดเตรียมความปลอดภัยที่เหมาะสมอย่างไร. หัวข้อเหล่านี้จะเน้นเรื่อง ส่วนประกอบที่เกี่ยวข้องกับความปลอดภัยของ configuration ของ APPC เป็นหลัก. เพื่อที่จะดัดแปลงตัวอย่างนี้ให้เข้ากับสถานการณ์ของคุณ, คุณจำเป็นต้องทำงาน ร่วมกับผู้ที่บริหารเครือข่ายการสื่อสารของคุณ และบางทีต้องทำงานกับผู้ที่จัดทำแอ็พพลิเคชันด้วย. ใช้ข้อมูลเหล่านี้เป็นพื้นฐานเพื่อช่วยเหลือให้คุณเข้าใจเกี่ยวกับประเด็นเกี่ยวกับการรักษาความปลอดภัย และตัวเลือกที่มีสำหรับ APPC.

ความปลอดภัยไม่เคยได้มา “ฟรีๆ ”. ข้อแนะนำบางอย่างสำหรับการทำให้การรักษาความปลอดภัยของเครือข่ายเป็นเรื่องที่ง่ายขึ้น อาจทำให้การบริหารเครือข่ายยากยิ่งขึ้น. ตัวอย่างเช่น, ข้อมูลนี้ไม่ได้เจาะจงในส่วนของ APPN® (Advanced Peer-to-Peer Networking®), เนื่องจากการรักษาความปลอดภัยเป็นเรื่องที่เข้าใจได้ง่ายขึ้นและสามารถจัดการได้โดยไม่ต้องอาศัยAPPN. อย่างไรก็ตาม, ถ้าไม่มี APPN, ผู้บริหารเครือข่ายจะต้องสร้างข้อมูล configuration ด้วยตนเอง ไม่สามารถให้ APPN สร้างให้โดยอัตโนมัติ.

เครื่องพีซีก็ใช้การสื่อสารด้วย

หลายๆ วิธีสำหรับการเชื่อมต่อพีซีหลายๆ ตัวเข้ากับเซิร์ฟเวอร์iSeries ขึ้นอยู่กับการสื่อสาร, ดังเช่น APPC หรือ TCP/IP. เมื่อคุณอ่านหัวข้อต่อไปนี้, ต้องมั่นใจว่า ได้พิจารณาเกี่ยวกับประเด็นในการรักษาความปลอดภัยสำหรับการเชื่อมต่อทั้งกับระบบอื่นๆ และกับพีซีอื่นๆ. เมื่อคุณวางแผนป้องกันเครือข่ายของคุณ, ตรวจสอบให้มั่นใจว่าคุณไม่ได้ทำการใดที่ส่งผลกระทบในแง่ลบต่อพีซีที่ต่ออยู่กับระบบของคุณ.

คำศัพท์ที่เกี่ยวกับ APPC

APPC จะให้ความสามารถแก่ผู้ใช้บนระบบหนึ่งในการทำงานบนอีกระบบหนึ่ง. ระบบที่การร้องขอ (request) เริ่มต้นขึ้นจะถูกเรียกโดยใช้ชื่อใดชื่อหนึ่งดังนี้:

- **ระบบต้นทาง (Source system)**
- **ระบบโลคัล (Local system)**

- **ไคลเอ็นต์ (Client)**

ระบบที่รับการร้องขอจะถูกเรียกโดยใช้ชื่อใดชื่อหนึ่งดังนี้:

- **ระบบปลายทาง (Target system)**
- **ระบบรีโมต (Remote system)**
- **เซิร์ฟเวอร์ (Server)**

องค์ประกอบเบื้องต้นของการสื่อสารแบบ APPC

จากมุมมองของผู้บริหารความปลอดภัย, สิ่งเหล่านี้จะต้องเกิดขึ้นก่อนที่ผู้ใช้ระบบหนึ่ง (SYSTEMA) จะสามารถทำงานบนอีกระบบหนึ่ง (SYSTEMB):

- ระบบต้นทาง (SYSTEMA) จะต้องมีพาธ (path) ไปยังระบบปลายทาง (SYSTEMB). พาธนี้จะถูกเรียกว่าเซสชัน APPC **(APPC session)**.
- ระบบปลายทางจะต้องระบุผู้ใช้และสร้างความสัมพันธ์กับผู้ใช้ด้วยโปรไฟล์ผู้ใช้. ระบบปลายทางต้องสนับสนุน อัลกอริธึมการเข้ารหัสของระบบต้นทาง (ดู "ระดับต่างๆ ของรหัสผ่าน" ในหน้า 16สำหรับข้อมูลเพิ่มเติม).
- ระบบปลายทางต้องเริ่มงานสำหรับผู้ใช้ด้วยสภาพแวดล้อมที่เหมาะสม (ค่าการจัดการงาน – work management values).

หัวข้อต่อไปจะอธิบายถึงองค์ประกอบเหล่านี้ และความสัมพันธ์ขององค์ประกอบเหล่านี้ต่อความปลอดภัย. ผู้บริหารระบบความปลอดภัยบนระบบปลายทางมีหน้าที่รับผิดชอบหลักในการทำให้มั่นใจว่าผู้ใช้ APPC ไม่ได้ละเมิดความปลอดภัย. อย่างไรก็ตาม, เมื่อผู้บริหารความปลอดภัยของทั้งสองระบบทำงานร่วมกัน, การจัดการความปลอดภัยของ APPC จะเป็นงานที่ง่ายดายขึ้น.

ตัวอย่าง: เซสชัน APPC เบื้องต้น

ในสภาวะแวดล้อมของ APPC , เมื่อผู้ใช้หรือแอ็พพลิเคชันบนระบบร้องขอการเข้าถึง ไปยังอีกระบบหนึ่ง, ระบบทั้งสองนี้จะทำการเซ็ตอัพเซสชันขึ้น. เพื่อที่จะสร้างเซสชัน, ระบบจะต้องเชื่อมคำอธิบายอุปกรณ์ APPC (APPC device descriptions) ทั้งสองที่ตรงกัน. พารามิเตอร์ remote location name (RMTLOCNAME) ในคำอธิบายอุปกรณ์ของ SYSTEMA จะต้องตรงกับ พารามิเตอร์ local location name (LCLLOCNAME) ในคำอธิบายอุปกรณ์ของ SYSTEMB หรืออาจเป็นไปในทางกลับกัน.

สำหรับสองระบบที่ทำให้เกิดเซสชัน APPC, รหัสผ่านของตำแหน่ง (location password) ในคำอธิบายอุปกรณ์ APPC บน SYSTEMA และ SYSTEMB จะต้องเหมือนกัน. ทั้งสองระบบต้องมีค่าเป็น *NONE หรือทั้งสองระบบต้องกำหนดเป็นค่าเดียวกัน.

ถ้ารหัสผ่านมีค่าที่ไม่ใช่ *NONE, รหัสผ่านจะถูกเก็บและส่งผ่านในรูปแบบที่มีการเข้ารหัส. ถ้ารหัสผ่านตรงกัน, ระบบจะสร้างเซสชัน. ถ้ารหัสผ่านไม่ตรงกัน, การร้องขอของผู้ใช้จะถูกปฏิเสธ. เมื่อระบบระบุรหัสผ่านของตำแหน่งในการสร้างเซสชัน, จะเรียกว่า **การเชื่อมที่ปลอดภัย (secure bind)**.

หมายเหตุ: ไม่ใช่ระบบคอมพิวเตอร์ทุกระบบที่รองรับฟังก์ชันการเชื่อมที่ปลอดภัย (secure bind function).

การจำกัดเซสชัน APPC

ในฐานะของผู้บริหารความปลอดภัยของระบบต้นทาง, คุณสามารถใช้สิทธิอ็อบเจ็กต์เพื่อควบคุมผู้ที่สามารถเข้าถึงระบบอื่นได้. ตั้งค่าสิทธิพับลิกของคำอธิบายอุปกรณ์ APPC เป็น *EXCLUDE และให้สิทธิ *CHANGE แก่ผู้ใช้เฉพาะที่กำหนด. ใช้ค่ากำหนดของระบบ QLMTSECOFR เพื่อป้องกันผู้ใช้ที่มีสิทธิพิเศษ *ALLOBJ จากการใช้ การสื่อสาร APPC.

ในฐานะของผู้บริหารความปลอดภัยของระบบปลายทาง, คุณก็สามารถใช้สิทธิในอุปกรณ์ APPC ป้องกันผู้ใช้จากการเรียกใช้เซสชัน APPC บนระบบของคุณ. อย่างไรก็ตาม, คุณจำเป็นต้องทราบว่า user ID ใดที่พยายามเข้าถึงคำอธิบายอุปกรณ์ APPC. “การเข้าถึงระบบปลายทางของผู้ใช้ APPC” ในหน้า 120 อธิบายถึงวิธีที่เซิร์ฟเวอร์ iSeries ทำการโยงความสัมพันธ์ระหว่าง ID ของผู้ใช้กับการร้องขอเซสชัน APPC.

หมายเหตุ: คุณสามารถใช้คำสั่ง Print Publicly Authorized Objects (PRTPUBAUT *DEVD) และคำสั่ง Print Private Authorities (PRTPVTAUT *DEVD) เพื่อหาว่าผู้ใดที่มีสิทธิในคำอธิบายอุปกรณ์บนระบบของคุณ.

เมื่อระบบของคุณใช้ APPN, จะมีการสร้างอุปกรณ์ APPC ขึ้นใหม่โดยอัตโนมัติ เมื่อไม่มีอุปกรณ์ให้กับเส้นทางที่ระบบเลือก. วิธีการหนึ่งสำหรับควบคุมการเข้าถึงยังอุปกรณ์ APPC บนระบบที่ใช้ APPN ก็คือการสร้าง authorization list. authorization list จะบรรจุรายชื่อของผู้ใช้ที่มีสิทธิในอุปกรณ์ APPC. จากนั้นคุณใช้คำสั่ง Change Command Default (CHGCMDDFT) เพื่อเปลี่ยนคำสั่ง CRTDEVAPPC. สำหรับพารามิเตอร์ authority (AUT) บนคำสั่ง CRTDEVAPPC, ให้กำหนดค่าดีฟอลต์เป็น authorization list ที่คุณสร้างขึ้นเอง.

หมายเหตุ: ถ้าระบบของคุณมีภาษาที่ไม่ใช่ภาษาอังกฤษ, คุณจำเป็นต้องเปลี่ยนค่าดีฟอลต์คำสั่งในไลบรารี่ QSYSxxx สำหรับแต่ละภาษาประจำชาติที่อยู่ในระบบของคุณ.

คุณใช้พารามิเตอร์ location password (LOCPWD) ในคำอธิบายอุปกรณ์ APPC เพื่อตรวจสอบค่าประจำตัวของระบบอื่นที่ร้องขอเซสชันในระบบของคุณ (ในฐานะของผู้ใช้หรือแอ็พพลิเคชัน). location password สามารถช่วยคุณตรวจจับระบบที่ประสงค์ร้ายได้.

เมื่อคุณใช้ location password, คุณต้องร่วมมือกับผู้บริหารความปลอดภัยของระบบอื่นภายในเครือข่าย. คุณยังต้องควบคุมผู้ที่สามารถสร้างหรือเปลี่ยนแปลงคำอธิบายอุปกรณ์ APPC และรายการคอนฟิกูเรชัน (configuration list). ระบบต้องการสิทธิพิเศษ *IOSYSCFG สิทธิพิเศษในการใช้คำสั่งที่ทำงานกับอุปกรณ์ APPC และรายกาย configuration.

หมายเหตุ: เมื่อคุณใช้ APPN, location password จะถูกเก็บอยู่ในรายการคอนฟิกูเรชัน QAPPNRMT แทนที่จะอยู่ในคำอธิบายอุปกรณ์.

การเข้าถึงระบบปลายทางของผู้ใช้ APPC

เมื่อระบบสร้างเซสชัน APPC, ระบบได้สร้างพาธสำหรับผู้ใช้ที่ร้องขอให้มีทางเข้าไปยังระบบปลายทาง. มีองค์ประกอบอื่นๆ อีกหลายอย่างที่ใช้พิจารณาสิ่งที่ผู้ใช้ต้องทำเพื่อให้สามารถเข้าไปยังระบบอื่น.

หัวข้อต่อไปจะอธิบายถึงองค์ประกอบที่พิจารณาว่าผู้ใช้ APPC ได้รับทางเข้าไปยังระบบปลายทางอย่างไร.

วิธีของระบบสำหรับการส่งข้อมูลเกี่ยวกับผู้ใช้

สถาปัตยกรรม APPC มีวิธีการสามวิธี สำหรับการส่งข้อมูลความปลอดภัยเกี่ยวกับผู้ใช้จากระบบต้นทางไปยังระบบปลายทาง. วิธีการเหล่านี้เรียกว่าเป็น **ค่าความปลอดภัยที่มีโครงสร้าง (architected security values)**. ตารางที่ 18แสดงวิธีการเหล่านี้:

หมายเหตุ: หนังสือ *APPC Programming* จะมีข้อมูลเพิ่มเติมเกี่ยวกับค่าความปลอดภัยที่มีโครงสร้าง.

ตารางที่ 18. ค่า องความปลอดภัยในสถาปัตยกรรมแบบ APPC

Architected security value	ID ของผู้ใช้ถูกส่งไปยังระบบเป้าหมาย	รหัสผ่านถูกส่งไปยังระบบเป้าหมาย
ไม่มี	ไม่	ไม่
เหมือนกัน	ใช่[1]	ดูที่หมายเหตุ 2.
โปรแกรม	ใช่	ใช่[3]

หมายเหตุ:

1. ระบบต้นทางส่ง user ID ถ้าระบบปลายทางกำหนด SECURELOC(*YES) หรือ SECURELOC (*VFYENCPWD).
2. ผู้ใช้ไม่ต้องป้อนรหัสผ่านในการร้องขอ เนื่องจากรหัสผ่านได้รับการตรวจสอบโดยระบบต้นทางแล้ว. สำหรับ SECURELOC(*YES) และ SECURELOC(*NO) ระบบต้นทางไม่ต้องส่งรหัสผ่าน. ถ้า SECURELOC(*VFYENCPWD), ระบบต้นทางจะนำเอารหัสผ่านที่เข้ารหัสและจัดเก็บไว้ แล้วทำการส่งไป (ในรูปแบบที่เข้ารหัส).
3. ระบบส่งรหัสผ่านในรูปแบบที่ถูกเข้ารหัสถ้าทั้งระบบต้นทางและปลายทางสนับสนุนการเข้ารหัสให้กับรหัสผ่าน. มิฉะนั้น, รหัสผ่านจะไม่ถูกเข้ารหัส.

แอ็พพลิเคชันที่ผู้ใช้ร้องขอจะพิจารณาค่าความปลอดภัยที่มีโครงสร้าง. ตัวอย่างเช่น, SNADS ใช้ SECURITY(NONE) เสมอ. DDM ใช้ SECURITY(SAME). ด้วยการส่งผ่าน display station, ผู้ใช้ระบุค่าความปลอดภัยโดยใช้พารามิเตอร์บนคำสั่ง STRPASTHR.

ในทุกกรณี, ระบบปลายทางเลือกที่จะรับการร้องของด้วยค่าความปลอดภัยที่ระบุโดยระบบต้นทาง. แต่ในบางสถานการณ์, ระบบปลายทางอาจปฏิเสธการร้องขอทั้งหมด. และในบางสถานการณ์, ระบบปลายทางอาจบังคับใช้ค่าความปลอดภัยอื่น. ตัวอย่างเช่น, เมื่อผู้ใช้กำหนดทั้ง user ID และรหัสผ่านในคำสั่ง STRPASTHR, การร้องขอใช้ SECURITY(PGM). อย่างไรก็ตาม, ถ้าค่าระบบ

QRMTSIGN เป็น *FRCSIGNON ในระบบปลายทาง, ผู้ใช้จะยังคงเห็นหน้าจอ Sign on. ด้วยการกำหนดค่า *FRCSIGNON, ระบบจะใช้ SECURITY(NONE) เสมอ, ซึ่งเท่ากับว่าผู้ใช้ไม่ได้ป้อน user ID และรหัสผ่านในคำสั่ง STRPASTHR.

หมายเหตุ:

1. ระบบต้นทางและปลายทางจัดการแลกค่าความปลอดภัยก่อนที่ข้อมูลจะถูกส่ง. ในสถานการณ์ที่ระบบปลายทางกำหนด SECURELOC(*NO) และการร้องขอคือ SECURITY(SAME), ตัวอย่างเช่น, การที่ระบบปลายทางบอกระบบต้นทางให้ใช้ SECURITY(NONE). ระบบต้นทางไม่ต้องส่ง user ID.
2. ระบบปลายทางปฏิเสธคำร้องขอเซสชันเมื่อรหัสผ่านของผู้ใช้บนระบบปลายทางได้หมดอายุลง. ซึ่งจะใช้เฉพาะกับการร้องขอการติดต่อที่มีการส่งรหัสผ่าน, ซึ่งรวมถึง:
   - เซสชันการร้องขอประเภท SECURITY(PROGRAM).
   - เซสชันการร้องขอประเภท SECURITY(SAME) เมื่อค่า SECURELOC เป็น *VFYENCPWD.

ตัวเลือกในการแบ่งความรับผิดชอบด้านความปลอดภัยในเน็ตเวิร์ก

เมื่อระบบของคุณอยู่ร่วมกันในเครือข่าย, คุณต้องตัดสินใจว่า จะเชื่อระบบอื่นในการ ตรวจสอบคุณสมบัติของผู้ใช้ที่พยายามเข้าสู่ระบบของคุณหรือไม่. คุณจะไว้ใจ SYSTEMA เพื่อให้แน่ใจว่า USERA เป็น USERA จริง (หรือ QSECOFR เป็น QSECOFR จริง)หรือไม่? หรือคุณยังต้องการผู้ใช้ให้ user ID และรหัสผ่านอีก?

พารามิเตอร์ secure location (SECURELOC) ในคำอธิบายอุปกรณ์ APPC บนระบบปลายทางกำหนดว่า ระบบต้นทางเป็นตำแหน่งที่ปลอดภัย (ไว้ใจ) ได้หรือไม่.

เมื่อระบบทั้งสองกำลังรันรีลีสที่สนับสนุน *VFYENCPWD, SECURELOC(*VFYENCPWD) จะมีการปกป้องเพิ่มเติมเมื่อแอ็พพลิเคชันเหล่านั้นใช้ SECURITY(SAME). ถึงแม้ว่าผู้ร้องขอไม่ได้ป้อนรหัสผ่านในการร้องขอ, ระบบต้นทางจะดึงรหัสผ่านของผู้ใช้ออกมาและสั่งไปพร้อมกับการร้องขอ. สำหรับการร้องขอที่ประสบผลสำเร็จ, ผู้ใช้จะต้องมี ID ของผู้ใช้ (user ID) และ รหัสผ่านที่เหมือนกันทั้งสองระบบ.

เมื่อระบบปลายทางกำหนด SECURELOC(*VFYENCPWD) และระบบต้นทางไม่ได้รองรับค่านี้, ระบบปลายทางจะจัดการการร้องขอนี้เป็น SECURITY(NONE).

ตารางที่ 19แสดงวิธีการที่ค่าความปลอดภัยที่มีโครงสร้าง และค่า SECURELOC ทำงานร่วมกัน:

ตารางที่ 19. ค่าความปลอดภัยของ APPC และ ค่าของ SECURELOC ทำงานร่วมกันได้อย่างไร

ระบบต้นทาง	ระบบปลายทาง	
Architected security value	**ค่าของ SECURELOC**	**โปรไฟล์ผู้ใช้สำหรับงาน**
ไม่มี	ค่าใดก็ได้	ผู้ใช้ดีฟอลต์[1]

ตารางที่ 19. ค่าความปลอดภัยของ APPC และ ค่าของ SECURELOC ทำงานร่วมกันได้อย่างไร (ต่อ)

ระบบต้นทาง	ระบบปลายทาง	
Architected security value	**ค่าของ SECURELOC**	**โปรไฟล์ผู้ใช้สำหรับงาน**
Same	*NO	ผู้ใช้ดีฟอลต์[1]
	*YES	ชื่อโปรไฟล์ผู้ใช้เดียวกันกับผู้ร้องขอจากระบบต้นทาง
	*VFYENCPWD	ชื่อโปรไฟล์ผู้ใช้เดียวกันกับผู้ร้องขอจากระบบต้นทาง. ผู้ใช้ต้องมีรหัสผ่านเดียวกันในทั้งสองระบบ.
Program	ค่าใดก็ได้	โปรไฟล์ผู้ใช้ที่ถูกกำหนดในการร้องขอจากระบบต้นทาง.

หมายเหตุ:

1. ผู้ใช้ดีฟอลต์ถูกกำหนดโดย communication entry ในคำอธิบายระบบย่อย. “การกำหนดระบบปลายทางของโปรไฟล์ผู้ใช้สำหรับงานต่างๆ”อธิบายเรื่องนี้.

การกำหนดระบบปลายทางของโปรไฟล์ผู้ใช้สำหรับงานต่างๆ

เมื่อผู้ใช้ร้องของาน APPC บนระบบอื่น, การร้องขอจะมีชื่อโหมด (mode name) ที่สัมพันธ์กับการร้องขอ. ชื่อโหมดอาจมาจากการร้องขอของผู้ใช้,หรืออาจเป็นค่าดีฟอลต์จากเน็ตเวิร์กแอ็ตทริบิวต์ของระบบต้นทาง.

ระบบปลายทางใช้ชื่อโหมดและชื่ออุปกรณ์ APPC ในการพิจารณาว่าจะให้งานทำงานอย่างไร. ระบบปลายทางค้นหาระบบย่อยที่ทำงานอยู่สำหรับ communication entry ที่ตรงกับชื่ออุปกรณ์ APPC และชื่อโหมดมากที่สุด.

communication entry จะกำหนดว่าโปรไฟล์ผู้ใช้ใดที่ระบบจะใช้ในคำร้องขอ SECURITY(NONE). ต่อไปนี้เป็นตัวอย่างของ communication entry ในคำอธิบายระบบย่อย:

```
                    Display Communications Entries

Subsystem description:   QCMN          Status:   ACTIVE

                          Job                        Default        Max
Device       Mode         Description    Library     User         Active
*ALL         *ANY         *USRPRF                    *SYS         *NOMAX
*ALL         QPCSUPP      *USRPRF                    *NONE        *NOMAX
```

ตารางที่ 20 ในหน้า 123 แสดงค่าที่เป็นไปได้สำหรับพารามิเตอร์ผู้ใช้ดีฟอลต์ใน communication entry:

ตารางที่ 20. ค่าที่เป็นไปได้สำหรับพารามิเตอร์ผู้ใช้ดีฟอลต์

ค่า	ผลลัพธ์
***NONE**	ไม่มีผู้ใช้ดีฟอลต์. ถ้าระบบต้นทางไม่ได้ส่ง user ID มากับการร้องขอ, จะไม่มีการรันงานนั้น.
***SYS**	มีเพียงโปรแกรมที่ IBM จัดหาให้ (งานของระบบ) จะทำงาน. ไม่มีแอ็พพลิเคชันของผู้ใช้ทำงาน.
user-name	ถ้าระบบต้นทางไม่ได้ส่ง user ID, งานจะรันภายใต้โปรไฟล์ผู้ใช้นี้.

คุณสามารถใช้คำสั่ง Print Subsystem Description (PRTSBSDAUT) เพื่อพิมพ์รายการระบบย่อยทั้งหมดที่ มี communication entry กับโปรไฟล์ผู้ใช้ดีฟอลต์.

ตัวเลือก การส่งผ่านจอภาพ

การส่งผ่านจอภาพนี้เป็นตัวอย่างหนึ่งของแอ็พพลิเคชันที่ใช้การสื่อสารแบบ APPC. คุณสามารถใช้การส่งผ่านจอภาพ ในการ sign on ไปยังระบบอื่นที่ต่อกับระบบของคุณผ่านทางเครือข่าย.

ตารางที่ 21แสดงตัวอย่างของการร้องขอการส่งผ่าน (passthrough request) ของคำสั่ง STRPASTHR และวิธีที่ระบบปลายทางจัดการกับการร้องขอนั้น. สำหรับการส่งผ่านจอภาพ, ระบบจะใช้องค์ประกอบพื้นฐานของการสื่อสาร APPC และค่า remote sign-on (QRMTSIGN) ของระบบ.

หมายเหตุ: การร้องขอการส่งผ่านจอภาพ ไม่ได้ผ่านเส้นทางของระบบย่อย QCMN และ QBASE อีกต่อไป. เริ่มต้นใน V4R1, จะมีเส้นทางผ่านระบบย่อย QSYSWRK. ก่อน V4R1 คุณอาจเข้าใจได้ว่าไม่มีการทำงานของระบบย่อย QCMD และ QBASE, การส่งผ่านจอภาพจึงไม่ทำงาน. แต่ไม่เป็นเช่นนั้นอีกต่อไป. คุณสามารถบังคับ Display Station Passthrough ให้วิ่งผ่าน QCMN (หรือ QBASE ถ้าทำงานอยู่) โดยการเปลี่ยนค่าระบบ QPASTHRSVR เป็น 0.

ตารางที่ 21. ตัวอย่างของการร้องขอ sign-on แบบ pass-through

ค่าที่อยู่ในคำสั่ง TRPASTHR		ระบบปลายทาง		
User ID	**รหัสผ่าน**	**ค่าของ SECURELOC**	**ค่าของ QRMTSIGN**	**ผลลัพธ์**
*NONE	*NONE	ค่าใดก็ได้	ค่าใดก็ได้	ผู้ใช้ต้อง sign on ในระบบปลายทาง.
ชื่อโปรไฟล์ผู้ใช้	ไม่ได้ถูกป้อน	ค่าใดก็ได้	ค่าใดก็ได้	การร้องขอล้มเหลว.

ตารางที่ 21. ตัวอย่างของการร้องขอ sign-on แบบ pass-through (ต่อ)

ค่าที่อยู่ในคำสั่ง TRPASTHR		ระบบปลายทาง		
User ID	**รหัสผ่าน**	**ค่าของ SECURELOC**	**ค่าของ QRMTSIGN**	**ผลลัพธ์**
*CURRENT	ไม่ได้ถูกป้อน	*NO	ค่าใดก็ได้	การร้องขอล้มเหลว
		*YES	*SAMEPRF	งานแบบโต้ตอบเริ่มด้วยชื่อของโปรไฟล์ผู้ใช้เดียวกันกับโปรไฟล์ผู้ใช้ที่อยู่บนระบบต้นทาง. ไม่มีการส่งผ่านรหัสผ่านไปยัง ระบบรีโมต. ต้องมีชื่อโปรไฟล์ผู้ใช้อยู่ในระบบปลายทาง.
			*VERIFY	
			*FRCSIGNON	ผู้ใช้ต้อง sign on ในระบบปลายทาง.
		*VFYENCPWD	*SAMEPRF	งานแบบโต้ตอบเริ่มด้วยชื่อของโปรไฟล์ผู้ใช้เดียวกันกับโปรไฟล์ผู้ใช้ที่อยู่บนระบบต้นทาง. ระบบต้นทางจะเรียก รหัสผ่านของผู้ใช้ออกมาและส่งไปยังระบบรีโมต. ต้องมีชื่อโปรไฟล์ผู้ใช้อยู่ในระบบปลายทาง.
			*VERIFY	
			*FRCSIGNON	ผู้ใช้ต้อง sign on ในระบบปลายทาง.
*CURRENT (หรือชื่อโปรไฟล์ผู้ใช้ ปัจจุบันของงาน)	ถูกป้อน	ค่าใดก็ได้	*SAMEPRF	งานแบบโต้ตอบเริ่มด้วยชื่อของโปรไฟล์ผู้ใช้เดียวกันกับโปรไฟล์ผู้ใช้ที่อยู่บนระบบต้นทาง. รหัสผ่าน *ถูก* ส่งไปยังระบบรีโมต. ต้องมีชื่อโปรไฟล์ผู้ใช้อยู่ในระบบปลายทาง.
			*VERIFY	
			*FRCSIGNON	ผู้ใช้ต้อง sign on ในระบบปลายทาง.
ชื่อโปรไฟล์ผู้ใช้ (ชื่อที่แตกต่าง จากโปรไฟล์ผู้ใช้ปัจจุบันของงาน)	ถูกป้อน	ค่าใดก็ได้	*SAMEPRF	การร้องขอล้มเหลว.
			*VERIFY	งานแบบโต้ตอบเริ่มด้วยชื่อของโปรไฟล์ผู้ใช้เดียวกันกับโปรไฟล์ผู้ใช้ที่อยู่บนระบบต้นทาง. รหัสผ่าน *ถูก* ส่งไปยังระบบรีโมต. ต้องมีชื่อโปรไฟล์ผู้ใช้อยู่ในระบบปลายทาง.
			*FRCSIGNON	งานโต้ตอบเริ่มต้นด้วยชื่อโปรไฟล์ผู้ใช้ที่กำหนด . รหัสผ่านถูกส่งไปยังระบบปลายทาง. ชื่อโปรไฟล์ผู้ใช้ต้องมีอยู่บนระบบปลายทาง.

หลีกเลี่ยงการกำหนดค่าอุปกรณ์โดยไม่ได้ตั้งใจ

เมื่อมีความล้มเหลวเกิดขึ้นกับอุปกรณ์ที่ทำงาน, ระบบพยายามที่จะกู้คืน. ในบางสถานการณ์, เมื่อการติดต่อขาดจากกัน ผู้ใช้อื่นสามารถใช้เซสชันที่ล้มเหลวนั้นใหม่ได้โดยไม่ได้ตั้งใจ. ตัวอย่างเช่น, สมมุติว่า USERA ได้ปิดเวิร์กสเตชันโดยไม่ได้ sign off. USERB สามารถเปิดเวิร์กสเตชันและเริ่มต้นใช้เซสชันของ USERA ได้โดยไม่ต้อง sign on.

เพื่อป้องกันเหตุการณ์ที่อาจเป็นไปได้เหล่านี้, ให้กำหนดค่าระบบ Device I/O Error Action (QDEVRCYACN) เป็น *DSCMSG. เมื่ออุปกรณ์ล้มเหลว, ระบบจะทำการจบงานของผู้ใช้.

ควบคุมคำสั่งรีโมตและงานแบ็ตช์ต่างๆ

มีหลายทางเลือกที่ช่วยคุณควบคุมคำสั่งรีโมตและงานที่สามารถทำงานอยู่ในระบบของคุณ, รวมถึงวิธีข้างล่างนี้:

- ถ้าระบบคุณใช้ DDM, คุณสามารถจำกัดการเข้าถึงไฟล์ DDM เพื่อป้องกันผู้ใช้จากการใช้คำสั่ง Submit Remote Command (SBMRMTCMD) จากระบบอื่น. เพื่อใช้คำสั่ง SBMRMTCMD, ผู้ใช้ต้องสามารถเปิดไฟล์ DDM ได้. คุณยังต้องจำกัดความสามารถในการสร้างไฟล์ DDM.
- คุณสามารถกำหนดโปรแกรมทางออก (exit program) สำหรับค่าระบบ DDM request access (DDMACC). ในโปรแกรมทางออก, คุณสามารถประเมิน การร้องขอ DDM ก่อนที่จะอนุญาตการร้องขอนั้น.
- คุณสามารถใช้เน็ตเวิร์กแอ็ตทริบิวต์ network job action (JOBACN) เพื่อป้องกันงานเครือข่ายจากการถูกส่ง หรือป้องกันจากการทำงานโดยอัตโนมัติ.
- คุณสามารถกำหนดอย่างชัดเจนให้การร้องขอของโปรแกรมใดที่สามารถทำงานอยู่ภายในสภาพแวดล้อมการสื่อสารโดยการลบรายการเส้นทาง (routing entry) PGMEVOKE จากคำอธิบายระบบย่อย. รายการเส้นทาง PGMEVOKE อนุญาตให้ผู้ร้องขอกำหนดโปรแกรมที่จะทำงานได้. เมื่อคุณลบค่ารายการเส้นทางนี้จากคำอธิบายระบบย่อย, เช่น คำอธิบายระบบย่อย QCMN, คุณจะต้องเพิ่มคำรายการเส้นทางสำหรับการร้องขอการสื่อสารที่ต้องการให้ทำงานได้สำเร็จ.

  "คำร้องขอ Architected TPN" ในหน้า 98 แสดงชื่อโปรแกรมสำหรับการร้องขอการสื่อสารโดยแอ็พพลิเคชันที่ IBM จัดหาให้. สำหรับแต่ละการร้องขอที่คุณต้องการอนุญาต, คุณสามารถเพิ่มรายการเส้นทางด้วยค่าที่เปรียบเทียบ และชื่อโปรแกรมซึ่งทั้งคู่ต้องเท่ากับชื่อโปรแกรม.

  เมื่อคุณใช้วิธีนี้, คุณต้องเข้าใจสภาพแวดล้อมในการจัดการระบบงาน (work management environment) บนระบบของคุณ และประเภทของการร้องขอการสื่อสารที่เกิดขึ้นบนระบบของคุณ. ถ้าเป็นไปได้, คุณต้องทดสอบการร้องขอการสื่อสารทุกประเภทเพื่อให้มั่นใจว่ามันทำงานได้ถูกต้องหลังจากที่คุณเปลี่ยนรายการเส้นทาง. เมื่อการร้องขอการสื่อสารไม่พบรายการเส้นทาง, คุณจะได้รับข้อความ CPF1269. อีกวิธีการหนึ่ง (ซึ่งมีปัญหาน้อยกว่าแต่อาจมีประสิทธิภาพด้อยกว่าด้วย) คือ การกำหนดสิทธิพับลิกเป็น *EXCLUDE สำหรับโปรแกรมรายการ (transaction program) ที่คุณไม่ต้องการให้รันในระบบของคุณ.

  หมายเหตุ: หนังสือ *Work Management* ให้ข้อมูลเพิ่มเติมเกี่ยวกับรายการเส้นทาง และวิธีที่ระบบจัดการกับการร้องขอเริ่มต้นโปรแกรม (program-start request).

การประเมินผลการตั้งค่า APPC

คุณสามารถใช้คำสั่ง Print Communication Security (PRTCMNSEC) หรืออ็อพชันของเมนูเพื่อพิมพ์คำที่เกี่ยวข้องกับความปลอดภัยใน APPC คอนฟิกูเรชันของคุณ. หัวข้อต่อไปนี้ จะอธิบายถึงข้อมูลที่อยู่บนรายงาน.

พารามิเตอร์ที่เกี่ยวข้องสำหรับอุปกรณ์ APPC

รูปที่ 9แสดงตัวอย่างของ Communications Information Report สำหรับคำอธิบายอุปกรณ์. รูปที่ 10แสดงตัวอย่างของรายงานแสดงรายการคอนฟิกูเรชัน. ต่อจากรายงานคือ คำอธิบายของฟิลด์บนรายงาน.

```
                          Communications Information (Full Report)
                                                                                SYSTEM4
Object type  . . . . . . . . . :   *DEVD
                                                                                                  Pre           SNUF
Object         Object        Device         Secure     Location     APPN      Single     Establish     Program
Name           Type          Category       Location   Password     Capable   Session     Session      Start

CDMDEV1        *DEVD         *APPC           *NO         *NO        *NO        *YES        *NO
CDMDEV2        *DEVD         *APPC           *NO         *NO        *NO        *YES        *NO
```

รูปที่ 9. ตัวอย่างของรายงาน APPC Device Description

```
                  Display Configuration List                        Page     1
                            SYSTEM4  12/17/95  07:24:36
Configuration list . . . . . . . . :   QAPPNRMT
Configuration list type  . . . . . :   *APPNRMT
Text . . . . . . . . . . . . . . . :
-----------------APPN Remote Locations------------------
          Remote              Remote    Control
Remote    Network   Local     Control   Point     Secure
Location  ID        Location  Point     Net ID     Loc
SYSTEM36  APPN      SYSTEM4   SYSTEM36  APPN       *NO
SYSTEM32  APPN      SYSTEM4   SYSTEM32  APPN       *NO
SYSTEMU   APPN      SYSTEM4   SYSTEM33  APPN       *YES
SYSTEMJ   APPN      SYSTEM4   SYSTEMJ   APPN       *NO
SYSTEMR2  APPN      SYSTEM4   SYSTEM1   APPN       *NO
-------------------------APPN Remote Locations--------------------------
          Remote                                        Local      Pre-
Remote    Network   Local     Single     Number of    Control  established
Location  ID        Location  Session  Conversations   Point     Session
SYSTEM36  APPN      SYSTEM4    *NO            10       *NO        *NO
SYSTEM32  APPN      SYSTEM4    *NO            10       *NO        *NO
```

รูปที่ 10. ตัวอย่างของรายงาน Configuration List

การรักษาความปลอดภัยให้กับฟิลด์ที่ระบุตำแหน่ง

ฟิลด์ตำแหน่งปลอดภัย (SECURELOC) เป็นตัวกำหนดว่าระบบโลคอลไว้ใจระบบรีโมตในการทำการตรวจสอบรหัสผ่านแทนระบบโลคอลหรือไม่. ฟิลด์ SECURELOC จะใช้เฉพาะกับแอ็พพลิเคชันที่ใช้ค่า SECURITY(SAME), เช่น DDM และแอ็พพลิเคชันที่ใช้ CPI-Communication API.

ค่า SECURELOC(*YES) ทำให้ระบบโลคอลไม่ปลอดภัยต่อจุดอ่อนที่อาจเกิดขึ้นกับระบบรีโมต. ผู้ใช้ใดๆ ที่อยู่บนระบบทั้งสองสามารถเรียกใช้โปรแกรมบนระบบโลคอล. ซึ่งเป็นอันตรายอย่างยิ่ง เนื่องจากโปรไฟล์ QSECOFR (เจ้าหน้าที่ความปลอดภัย) มีอยู่บนทุกระบบ iSeries และมีสิทธิพิเศษ *ALLOBJ. ถ้ามีระบบหนึ่งบนเครือข่ายไม่ได้ทำหน้าที่ที่ดีในการปกป้องรหัสผ่านของ QSECOFR, ระบบอื่นๆ ที่คิดว่าระบบนั้นเป็นตำแหน่งที่ปลอดภัยจะอยู่ในความเสี่ยง.

เมื่อคุณใช้ SECURELOC(*VFYENCPWD), ระบบของคุณมีความเสี่ยงน้อยกว่า ในกรณีที่ระบบอื่นที่ไม่ได้ปกป้องรหัสผ่านอย่างพอเพียง. ผู้ใช้ที่ร้องขอแอ็พพลิเคชันที่ใช้ SECURITY(SAME) จะต้องมี user ID และ รหัสผ่านเดียวกันบนทั้งสองระบบ. SECURELOC(*VFYENCPWD) ต้องการนโยบายการบริหารรหัสผ่านระหว่างเครือข่ายของคุณ เพื่อที่ผู้ใช้จะได้มีรหัสผ่านเดียวกันทุกระบบ.

หมายเหตุ: SECURELOC(*VFYENCPWD) ได้รับการสนับสนุนระหว่างระบบที่เป็น V3R2, V3R7, หรือ V4R1 เท่านั้น. ถ้าระบบปลายทางกำหนด SECURELOC (*VFYENCPWD) และระบบต้นทางไม่ได้สนับสนุนฟังก์ชันนี้, การร้องขอจะถูกจัดการเช่นเดียวกับ SECURITY(NONE).

ถ้าระบบกำหนด SECURELOC(*NO), แอ็พพลิเคชันที่ใช้ SECURITY(SAME) จะต้องการผู้ใช้ดีฟอลต์เพื่อรันโปรแกรม. ผู้ใช้ดีฟอลต์ขึ้นกับทั้งคำอธิบายอุปกรณ์และโหมด (mode) ที่สัมพันธ์กับการร้องขอนั้น. (อ่าน "การกำหนดระบบปลายทางของโปรไฟล์ผู้ใช้สำหรับงานต่างๆ" ในหน้า 122.)

ฟิลด์รหัสผ่านของตำแหน่ง

ฟิลด์รหัสผ่านของตำแหน่งใช้พิจารณาว่าสองระบบจะแลกเปลี่ยนรหัสผ่าน เพื่อตรวจสอบว่าระบบที่ทำการร้องขอไม่ใช่ระบบที่ประสงค์ร้าย. "ตัวอย่าง: เซสชัน APPC เบื้องต้น" ในหน้า 118 มีข้อมูลเพิ่มเติมเกี่ยวกับรหัสผ่านของตำแหน่ง.

APPN Capable field

ฟิลด์ APPN-capable (APPN) ระบุว่าระบบรีโมตสามารถสนับสนุนฟังก์ชันเน็ตเวิร์กระดับสูง หรือจะถูกจำกัดไว้ที่การเชื่อมต่อแบบ single-hop. APPN(*YES) มีความหมายดังนี้:

- ถ้าระบบรีโมตเป็นโหนดของเครือข่าย, ระบบรีโมตอาจจะสามารถต่อระบบโลคัลกับระบบอื่น. ซึ่งจะเรียกว่า **เส้นทางโหนดระหว่างกลาง (intermediate node routing)**. ซึ่งหมายความว่าผู้ใช้บนระบบของคุณอาจสามารถใช้ระบบรีโมตเป็นเส้นทางไปยังเครือข่ายขนาดใหญ่ขึ้น.
- ถ้าระบบโลคัลเป็นโหนดของเครือข่าย, ระบบรีโมตสามารถใช้ระบบโลคัลเพื่อติดต่อกับระบบอื่น. ผู้ใช้ระบบรีโมตอาจสามารถใช้ระบบคุณเป็นเส้นทางไปยังเครือข่ายขนาดใหญ่ขึ้น.

  หมายเหตุ: คุณสามารถใช้คำสั่ง DSPNETA เพื่อพิจารณาว่าระบบเป็นโหนดของเครือข่ายหรือโหนดสิ้นสุด (end-node).

ฟิลด์ของเซสชันเดี่ยว

ฟิลด์ single session (SNGSSN) กำหนดว่าระบบรีโมตสามารถวิ่งได้มากกว่าหนึ่งเซสชันในเวลาหนึ่ง โดยใช้คำอธิบายอุปกรณ์ APPC เดียวกัน. SNGSSN(*NO) ถูกใช้เป็นปกติเนื่องจากจะช่วยลดความต้องการทีจะสร้างคำอธิบายอุปกรณ์หลายๆ อัน สำหรับหนึ่งระบบรีโมต. ตัวอย่างเช่น, ผู้ใช้พีซีมักจะต้องการเซสชันของ 5250-emulation มากกว่าหนึ่งเซสชัน และเซสชันสำหรับฟังก์ชันไฟล์เซิร์ฟเวอร์และพรินต์เซิร์ฟเวอร์. ด้วยค่า SNGSSN(*NO), คุณสามารถทำโดยใช้หนึ่งคำอธิบายระบบอุปกรณ์สำหรับพีซีบนระบบ iSeries.

SNGSSN(*NO) หมายความว่าคุณต้องขึ้นกับสำนึกด้านความปลอดภัยในการปฏิบัติงานของผู้ใช้พีซีและผู้ใช้ APPC คนอื่นๆ . ระบบของคุณอาจมีอันตรายจากบางคนในระบบรีโมตที่เริ่มเซสชันที่ไม่ถูกต้อง ที่ใช้คำอธิบายอุปกรณ์เดียวกันเป็นเซสชันเดียวกัน. (การปฏิบัติเช่นนี้บางทีถูกเรียกว่าเป็น **piggy-backing**.)

ฟิลด์ของเซสชัน Pre-establish

ฟิลด์ pre-establish session (PREESTSSN) สำหรับอุปกรณ์แบบเซสชันเดียว (single-session) ควบคุมว่าระบบโลคัลเริ่มต้นเซสชันด้วยระบบรีโมต เมื่อระบบรีโมตทำการติดต่อครั้งแรกกับระบบโลคัล. PREESTSSN(*NO) หมายความว่า ระบบโลคัลจะรอเริ่มต้นเซสชันจนกว่าแอ็พพลิเคชันร้องขอเซสชันกับระบบ. PREESTSSN(*YES) มีประโยชน์ในการลดระยะเวลาที่ใช้ในการการเชื่อมต่อของแอ็พพลิเคชัน.

PREESTSSN(*YES) ป้องกันระบบจากการตัดการติดต่อกับสาย (dial-up) ที่ไม่ได้ใช้อีกต่อไป. แอ็พพลิเคชันหรือผู้ใช้ต้อง vary off สายนั้น. PREESTSSN(*YES) อาจทำให้เวลาที่ระบบโลคัลไม่ปลอดภัยต่อการ piggy-backing บนเซสชันยาวนานขึ้น.

ฟิลด์ SNUF Program start

ฟิลด์ SNUF program start กำหนดว่ามีการยอมให้ระบบรีโมตเริ่มโปรแกรมบนระบบโลคัลได้หรือไม่. *YES หมายถึงว่า โครงร่างของสิทธิอ็อบเจ็กต์บนระบบโลคัลจะต้องพอเพียงต่อการป้องกันอ็อบเจ็กต์ เมื่อผู้ใช้บนระบบรีโมตเริ่มงานและเรียกใช้โปรแกรมบนระบบโลคัล.

พารามิเตอร์สำหรับตัวควบคุม APPC

รูปที่ 11แสดงตัวอย่างของรายงานข้อมูลการสื่อสาร (Communications Information Report) สำหรับคำอธิบายตัวควบคุม. ต่อจากรายงาน, คุณจะพบคำอธิบายของแต่ละฟิลด์ในรายงาน.

```
                    Communications Information (Full Report)
                                                                    SYSTEM4
Object type  . . . . . . . . . :   *CTLD

Object    Object    Controller    Auto     Switched      Call       APPN       CP      Disconnect   Delete    Device
Name      Type      Category      Create   Controller    Direction  Capable    Sessions    Timer      Seconds   Name
CTL01     *CTLD     *APPC         *YES       *YES        *DIAL      *YES       *YES          0        1440    AARON
CTL02     *CTLD     *APPC         *YES       *YES        *DIAL      *YES       *YES          0        1440    BASIC
CTL03     *CTLD     *APPC         *YES       *YES        *DIAL      *YES       *YES          0        1440    *NONE
```

รูปที่ 11. ตัวอย่างของรายงาน APPC Controller Description

ฟิลด์ Auto-create

บน line description, ฟิลด์ auto-create (AUTOCRTCTL) กำหนดว่าระบบโลคัลทำการสร้างคำอธิบายตัวควบคุม (controller description) โดยอัตโนมัติ เมื่อมีการร้องขอที่ไม่สามารถพบคำอธิบายตัวควบคุมที่ตรงกัน. บนคำอธิบายตัวควบคุม, ฟิลด์ auto-create กำหนดว่าระบบโลคัลทำการสร้างคำอธิบายอุปกรณ์โดยอัตโนมัติ เมื่อมีการร้องขอที่ไม่สามารถพบคำอธิบายอุปกรณ์ที่ตรงกัน.

สำหรับตัวควบคุมที่เป็น APPN-capable, ฟิลด์ auto-create จะไม่มีผล. ระบบทำการสร้างคำอธิบายอุปกรณ์โดยอัตโนมัติเมื่อจำเป็น, โดยไม่สนใจว่าคุณได้กำหนดฟิลด์ auto-create ไว้อย่างไร.

เมื่อคุณกำหนด *YES สำหรับ line description, ทุกคนที่เข้าถึงสายสามารถติดต่อกับระบบของคุณ. ซึ่งรวมถึงไซต์ที่ติดต่อโดยใช้บริดจ์ (bridges) หรือเราเตอร์ (routers).

ฟิลด์ Control point sessions

สำหรับตัวควบคุมที่สามารถทำ APPN, ฟิลด์ control point session (CPSSN) จะควบคุมว่าระบบสร้างการเชื่อมต่อ APPC กับระบบรีโมตโดยอัตโนมัติหรือไม่. ระบบใช้เซสชัน CP เพื่อแลกเปลี่ยนข้อมูลและสถานะเครือข่ายกับระบบรีโมต. การแลกเปลี่ยนข้อมูลที่ทันสมัยระหว่างโหนดเครือข่าย APPN เฉพาะเรื่องที่สำคัญมาก เพื่อที่เครือข่ายของคุณจะสามารถทำงานได้อย่างราบรื่น.

เมื่อคุณกำหนด *YES, สายที่อยู่ในสภาพว่าง (idle) จะไม่ถูกตัดการติดต่อโดยอัตโนมัติ. ซึ่งทำให้ระบบของคุณมีความเสี่ยงต่อเซสชัน piggy-back มากขึ้น.

ฟิลด์ Disconnect timer

สำหรับตัวควบคุม APPC, ฟิลด์ disconnect timer จะระบุระยะเวลาที่ตัวควบคุมจะต้องไม่ถูกใช้ (ไม่มีเซสชันที่แอ็คทีฟ) ก่อนที่ระบบตัดการติดต่อของสายที่ไปยังระบบรีโมต. ฟิลด์นี้มีสองค่า. ค่าแรก กำหนดระยะเวลาที่ตัวควบคุม ยังคงแอ็คทีฟอยู่จากเวลาที่เริ่มการติดต่อ. ค่าที่สอง กำหนดระยะเวลาที่ระบบรอหลังจากที่เซสชันสุดท้าย ได้จบลงบนตัวควบคุม ก่อนที่ระบบจะตัดสายนั้น.

ระบบใช้ disconnect timer เฉพาะเมื่อ ฟิลด์ switched disconnect (SWTDSC) เป็น *YES เท่านั้น.

ถ้าคุณกำหนดค่าเหล่านี้มากเกินไป, ระบบของคุณจะเสี่ยงต่อเซสชั่น piggy-back มากขึ้น.

พารามิเตอร์สำหรับ line description

รูปที่ 12 ในหน้า 130 แสดงตัวอย่างของรายงานข้อมูลการสื่อสารสำหรับ line description. ต่อจากรายงาน, คุณจะพบคำอธิบายของแต่ละฟิลด์ในรายงาน.

```
                          Communications Information (Full Report)

Object type  . . . . . . . . . :   *LIND
Auto
Object         Object         Line           Auto      Delete       Auto      Auto
Name           Type           Category       Create    Seconds      Answer    Dial
LINE01          *LIND          *SDLC           *NO            0       *NO       *NO
LINE02          *LIND          *SDLC           *NO            0       *YES      *NO
LINE03          *LIND          *SDLC           *NO            0       *NO       *NO
LINE04          *LIND          *SDLC           *NO            0       *YES      *NO
```

รูปที่ 12. ตัวอย่างของรายงาน APPC Line Description

ฟิลด์ Auto answer

ฟิลด์ auto answer (AUTOANS) กำหนดว่าสายแบบสวิตซ์จะตอบรับการเรียกเข้ามา โดยไม่ต้องมีการแทรกแซงของผู้ควบคุมเครื่องหรือไม่.

เมื่อคุณกำหนดเป็น *YES, ระบบของคุณมีความปลอดภัยน้อยลง เพราะว่าระบบสามารถถูกเข้าถึงได้ง่ายยิ่งขึ้น. เพื่อที่จะลดจุดอ่อนด้านความปลอดภัยเมื่อคุณกำหนดเป็น *YES, คุณต้อง vary off สายของคุณเมื่อไม่ต้องการใช้งาน.

ฟิลด์ Auto dial

ฟิลด์ auto dial (AUTODIAL) กำหนดว่า สายแบบสวิตซ์สามารถทำการเรียกออกภายนอก โดยไม่ต้องมีการแทรกแซงจากผู้ควบคุมเครื่องหรือไม่.เมื่อคุณกำหนดเป็น *YES, คุณอนุญาตให้ผู้ใช้โลคัลซึ่งไม่มีการเข้าถึงโดยตรงไปยังสายการสื่อสาร และโมเด็มสามารถติดต่อกับระบบอื่นได้.

บทที่ 13. การรักษาความปลอดภัยในการสื่อสารด้วย TCP/IP

TCP/IP (Transmission Control Protocol/Internet Protocol) เป็นวิธีปกติที่คอมพิวเตอร์ทุกประเภทติดต่อซึ่งกันและกัน. แอ็พพลิเคชันของ TCP/IP เป็นที่รู้จักและใช้กันอย่างแพร่หลายใน “ทางด่วนข้อมูล”.

ในบทนี้จะมีคำแนะนำเกี่ยวกับเรื่องเหล่านี้:

- การป้องกันไม่ให้แอ็พพลิเคชัน TCP/IP ทำงานบนระบบของคุณ.
- การปกป้องรีซอร์สของระบบเมื่อคุณอนุญาตให้แอ็พพลิเคชัน TCP/IP ทำงานบนระบบของคุณ.

เว็บไซต์ของ iSeries Information Center—>Networking—>TCP/IP เป็นแหล่งข้อมูลที่สมบูรณ์สำหรับข้อมูลเกี่ยวกับแอ็พพลิเคชัน TCP/IP ทั้งหมด. *SecureWay®: iSeries and the Internet* (iSeries Information Center—>Security—>SecureWay อธิบายถึงข้อควรพิจารณาในการรักษาความปลอดภัยเมื่อคุณเชื่อมต่อเซิร์ฟเวอร์ iSeries ของคุณเข้ากับอินเตอร์เน็ต (เน็ตเวิร์ก TCP/IP ที่ใหญ่มาก) หรืออินทราเน็ต. โปรดดูที่ “สิ่งที่ต้องรู้ก่อนและข้อมูลที่เกี่ยวข้อง” ในหน้า xiii สำหรับรายละเอียดเพิ่มเติมในการเข้าถึง Information Center ของ iSeries .

จำไว้ว่าเซิร์ฟเวอร์ iSeries ทั้งหลายสนับสนุนหลากหลายแอ็พพลิเคชัน TCP/IP ที่เป็นไปได้. เมื่อคุณตัดสินใจอนุญาตให้ แอ็พพลิเคชัน TCP/IP หนึ่งทำงานบนระบบของคุณ, คุณอาจต้องทำให้แอ็พพลิเคชัน TCP/IP อื่นๆ ทำงานด้วย. ในฐานะของผู้บริหารความปลอดภัย, คุณจำเป็นต้องทราบถึงขอบเขตของแอ็พพลิเคชัน TCP/IP และผลกระทบต่อความปลอดภัยของแอ็พพลิเคชันเหล่านั้น.

ป้องกันการประมวลผลของ TCP/IP

งานของเซิร์ฟเวอร์ TCP/IP จะรันอยู่ในระบบย่อย QSYSWRK. คุณใช้คำสั่ง Start TCP/IP (STRTCP) เพื่อเริ่ม TCP/IP บนระบบของคุณ. ถ้าคุณไม่ต้องการการประมวลผลใดๆ ของ TCP/IP หรือไม่ให้ แอ็พพลิเคชัน TCP/IP ทำงาน, ห้ามใช้คำสั่ง STRTCP. ระบบของคุณจะส่งมาพร้อมกับสิทธิพับลิก สำหรับคำสั่ง STRTCP ที่กำหนดเป็น *EXCLUDE.

ถ้าคุณสงสัยว่ามีบางคนที่เข้าถึงคำสั่งเริ่ม TCP/IP (เช่น ในช่วงเวลาเลิกงาน), คุณสามารถจัดเตรียมการตรวจสอบอ็อบเจ็กต์บนคำสั่ง STRTCP. ระบบ จะทำการเขียนบันทึกการตรวจสอบ (audit journal entry) เมื่อมีผู้เรียกใช้คำสั่งนี้.

องค์ประกอบความปลอดภัยของ TCP/IP

คุณสามารถอาศัยข้อได้เปรียบขององค์ประกอบความปลอดภัยของ TCP/IP ทั้งหลายที่เพิ่มประสิทธิภาพความปลอดภัยของเน็ตเวิร์กของคุณและเพิ่มความยืดหยุ่นให้กับเน็ตเวิร์ก. แม้ว่าบางส่วนของเทคโนโลยีเหล่านี้ถูกพบในผลิตภัณฑ์ไฟร์วอลล์, แต่องค์ประกอบความปลอดภัยของ TCP/IP สำหรับOS/400 เหล่านี้ไม่ได้มีไว้เพื่อใช้เป็นไฟร์วอลล์ . อย่างไรก็ตาม, คุณอาจใช้บาง

อย่างในคุณสมบัติเหล่านี้ในบางรูปแบบ, เพื่อขจัดความต้องการสำหรับผลิตภัณฑ์ไฟร์วอลล์ที่แยกออกไป. คุณอาจใช้คุณสมบัติ TCP/IP เหล่านี้เสริมความปลอดภัยในสภาพแวดล้อมที่คุณใช้ไฟร์วอลล์อยู่แล้วได้.

องค์ประกอบต่อไปนี้ช่วยให้ความปลอดภัย TCP/IP มีประสิทธิภาพมากขึ้น:

- Packet Rules
- HTTP Proxy Server
- VPN (virtual private networking)
- SSL (secure sockets layer)

การใช้กฎของแพ็กเก็ตในการรักษาความปลอดภัยให้กับการจราจร TCP/IP

กฎของแพ็กเก็ต, ซึ่งเป็นการรวมกันของการกรอง IP และ network address translation (NAT) จะทำงานเสมือนเป็นไฟร์วอลล์เพื่อปกป้องเน็ตเวิร์กภายในของคุณจากผู้บุกรุกทั้งหลาย. การกรอง IP ปล่อยให้คุณควบคุมว่าการจราจรของ IP ใดที่จะอนุญาตให้เข้าและออกเน็ตเวิร์กของคุณ. ในเบื้องต้น, มันจะปกป้องเน็ตเวิร์กโดยการกรองแพ็กเก็ตตามกฎที่คุณกำหนดขึ้น. NAT, ในทางกลับกัน, อนุญาตให้คุณซ่อน IP address ของคุณที่ไม่ได้จดทะเบียนไว้เบื้องหลังของชุด IP address ที่ได้รับการจดทะเบียนแล้ว. ?ทั้งนี้จะเป็นการช่วยปกป้องเน็ตเวิร์กภายในของคุณจากเน็ตเวิร์กต่างๆ ข้างนอก. NAT ก็จะช่วยในการแบ่งเบาปัญหาการหมดไปของ IP address, เนื่องจากแอดเดรสไพรเวทต่างๆ สามารถ ถูกแสดงแทนโดยใช้ชุดแอดเดรสเล็กๆ ซึ่งได้รับการจดทะเบียนแล้วได้. โปรดดูที่ iSeries Information Center สำหรับรายละเอียดเพิ่มเติม .

HTTP พร็อกซีเซิร์ฟเวอร์

HTTP พร็อกซีเซิร์ฟเวอร์มากับ IBM HTTP เซิร์ฟเวอร์สำหรับเซิร์ฟเวอร์ iSeries. HTTP เซิร์ฟเวอร์เป็นส่วนหนึ่งของ OS/400. พร็อกซีเซิร์ฟเวอร์ได้รับคำร้องขอ HTTP จากเว็บบราวเซอร์และส่งคำร้องขอเหล่านั้น ไปยังเว็บเซิร์ฟเวอร์. เว็บเซิร์ฟเวอร์ที่ได้รับคำร้องขอจะทราบเพียง IP แอดเดรสของพร็อกซีเซิร์ฟเวอร์และไม่สามารถทราบชื่อหรือแอดเดรสของพีซีที่เป็นที่มาของคำร้องขอเหล่านั้น. พร็อกซีเซิร์ฟเวอร์สามารถจัดการกับคำร้องขอ URL สำหรับ HTTP, FTP, Gopher และ WAIS.

พร็อกซีเซิร์ฟเวอร์เก็บเว็บเพจที่กลับคืนมาจากคำร้องขอที่ทำโดยผู้ใช้พร็อกซีเซิร์ฟเวอร์ทุกคน. ผลที่ตามมาคือ, เมื่อผู้ใช้ร้องขอเพจ, พร็อกซีเซิร์ฟเวอร์จะตรวจดูว่า มีเพจนั้นอยู่ในแคชหรือไม่. ถ้ามี, พร็อกซีเซิร์ฟเวอร์ก็จะส่งเพจที่เก็บไว้คืนมา. โดยการใช้เพจที่เก็บไว้ในแคช, พร็อกซีเซิร์ฟเวอร์สามารถที่จะให้บริการเว็บเพจได้เร็วขึ้น, ซึ่งช่วยลดระยะเวลาในการร้องขอไปยังเว็บเซิร์ฟเวอร์.

พร็อกซีเซิร์ฟเวอร์ยังสามารถบันทึกการร้องขอ URL ทั้งหมดสำหรับใช้ในการติดตาม. คุณสามารถทบทวนบันทึกเหล่านี้เพื่อเฝ้าสังเกตการใช้รีซอร์สของเครือข่าย อย่างถูกต้องและไม่ถูกต้อง.

คุณสามารถใช้การสนับสนุน HTTP proxy ใน IBM HTTP Server เพื่อรวบรวมการเข้าถึงเว็บเข้าด้วยกัน. มีการปิดบังแอดเดรสของไคลเอ็นต์พีซีจากเว็บเซิร์ฟเวอร์ที่พีซีเหล่านั้นเข้าถึง; จะทราบเพียง IP แอดเดรสของพร็อกซีเซิร์ฟเวอร์เท่านั้น. การเก็บเว็บเพจไว้ในแคชยังช่วยลดความต้องการด้าน

แบนด์วิธของการสื่อสาร และลดเวิร์กโหลดของไฟร์วอลล์. โปรดดูที่ HTTP เซิร์ฟเวอร์ IBM สำหรับ iSeries โฮมเพจสำหรับข้อมูลเพิ่มเติม: http://www-1.ibm.com/servers/eserver/iseries/software/http/index.html

Virtual Private Networking (VPN)

virtual private network (VPN) อนุญาตให้บริษัทของคุณขยายอินทราเน็ตไพรเวทไปบนกรอบงานที่มีอยู่ของเน็ตเวิร์กที่เป็นพับลิก, อาทิเช่น อินเตอร์เน็ต ได้อย่างปลอดภัย. ด้วย VPN, บริษัทของคุณสามารถควบคุมการจราจรของเน็ตเวิร์กได้เมื่อมีการเตรียมคุณลักษณะพิเศษในการรักษาความปลอดภัยที่สำคัญ อาทิเช่น การพิสูจน์ตัวจริง และความเป็นส่วนตัวของข้อมูล.

OS/400 VPN เป็นคอมโพเนนท์ที่สามารถเลือกติดตั้งได้ของ iSeries Navigator, graphical user interface (GUI) สำหรับ OS/400. ซึ่งจะอนุญาตให้คุณสร้างพาธแบบ end-to-end ที่ปลอดภัยระหว่างการรวมกันใดๆ ของโฮสต์ และเกตเวย์. OS/400 VPN ใช้วิธี authentication, อัลกอริธึม encryption, และข้อควรระวังอื่นๆ เพื่อให้แน่ใจว่าข้อมูลที่ส่งระหว่างจุดปลายทางทั้งสองของการเชื่อมต่อนั้น ยังคงปลอดภัยอยู่.

VPN รันบนเลเยอร์เน็ตเวิร์กของแบบจำลองแบบสแต็กของการสื่อสารที่แบ่งไว้เป็นเลเยอร์ของ TCP/IP1. โดยเฉพาะอย่างยิ่ง, VPN ใช้กรอบงาน แบบเปิดที่มีสถาปัตยกรรมแบบ IP Security (IPSec) . IPSec จะมีฟังก์ชันความปลอดภัยพื้นฐานสำหรับอินเตอร์เน็ต, รวมไปถึงการให้ตัวประกอบพื้นฐานนี้ยืดหยุ่นได้ซึ่งจะทำให้คุณสามารถสร้าง virtual private network ที่เสถียร, และปลอดภัย.

VPN ยังสนับสนุนโซลูชันของ Layer 2 Tunnel Protocol (L2TP) VPN อีกด้วย. การเชื่อมต่อ L2TP, ซึ่งถูกเรียกอีกอย่างหนึ่งว่า virtual line, จะมีการเข้าถึงที่มีประสิทธิภาพสำหรับผู้ใช้รีโมตโดยอนุญาตให้เซิร์ฟเวอร์ของเน็ตเวิร์กของกลุ่มควบคุมการกำหนดค่า IP address ให้กับผู้ใช้รีโมตของมันเองได้. นอกจากนั้น, การเชื่อมต่อแบบ L2TP ยังทำให้เกิดการเข้าถึงระบบหรือเน็ตเวิร์กอย่างปลอดภัยเมื่อปกป้องระบบหรือเน็ตเวิร์กของคุณด้วย IPSec.

นับเป็นสิ่งสำคัญอย่างยิ่ง ที่คุณต้องเข้าใจผลกระทบจาก VPN ที่จะมีต่อเน็ตเวิร์กทั้งหมดของคุณได้. การวางแผนและการนำไปปฏิบัติอย่างถูกต้องเป็นหัวใจสำคัญในการประสบความสำเร็จของคุณ. คุณสมควรที่จะทบทวนหัวข้อ VPN ใน iSeries Information Center เพื่อให้แน่ใจว่าคุณทราบว่า VPN ทำงานอย่างไร และคุณจะใช้มันได้อย่างไร. สำหรับข้อมูลเพิ่มเติม, โปรดดูที่ iSeries Information Center—>Security—>Virtual Private Networking. สำหรับข้อมูลเกี่ยวกับการเข้าถึง “สิ่งที่ต้องรู้ก่อนและข้อมูลที่เกี่ยวข้อง” ในหน้า xiiiiSeries Information Center.

Secure Sockets Layer (SSL)

Secure Sockets Layer (SSL) ได้กลายมาเป็นมาตรฐานอุตสาหกรรมสำหรับการทำให้แอ็พพลิเคชันมีเซสชันการสื่อสารที่ปลอดภัยใช้งานได้บนระบบที่ไม่ได้ป้องกันเอาไว้, อาทิเช่น อินเตอร์เน็ต. โปรโตคอล SSL ทำให้เกิดการเชื่อมต่อที่ปลอดภัยระหว่างไคลเอ็นต์และเซิร์ฟเวอร์แอ็พพลิเคชันที่มีการพิสูจน์ตัวจริงของจุดปลายทางจุดใดจุดหนึ่งหรือทั้งสองจุดของเซสชันการสื่อสาร. SSL ยังมีความเป็นส่วนตัวและความสมบูรณ์ของข้อมูลที่ไคลเอ็นต์และเซิร์ฟเวอร์แอ็พพลิเคชันแลกเปลี่ยน

กัน. สำหรับข้อมูลเพิ่มเติม, โปรดดูที่ iSeries Information Center−>Security—>Secure Sockets Layer (SSL). ดูที่ “สิ่งที่ต้องรู้ก่อนและข้อมูลที่เกี่ยวข้อง” ในหน้า xiii สำหรับข้อมูลในการเข้าถึง iSeries Information Center.

การรักษาความปลอดภัยให้กับสภาวะแวดล้อมของ TCP/IP ของคุณ

ในหัวข้อนี้จะให้คำแนะนำทั่วๆ ไปสำหรับขั้นตอนที่คุณสามารถใช้เพื่อลดจุดอ่อนด้านความปลอดภัยในสภาพแวดล้อม TCP/IP บนระบบของคุณ. คำแนะนำนี้ใช้กับสภาพแวดล้อมทั้งหมดของ TCP/IP มากกว่าแอพพลิเคชั่นเฉพาะซึ่งจะถูกกล่าวถึงในหัวข้อต่อไป.

- เมื่อคุณเขียนแอ็พพลิเคชันสำหรับพอร์ตของ TCP/IP, ต้องแน่ใจว่าแอ็พพลิเคชันนั้นมีความปลอดภัยอย่างเหมาะสม. คุณอาจสมมุติว่ามีบุคคลภายนอกที่พยายามเข้าถึงแอ็พพลิเคชันนั้นผ่านทางพอร์ตนั้น. บุคคลภายนอกที่เก่งอาจพยายาม TELNET ไปยังแอ็พพลิเคชันนั้น.
- เฝ้าสังเกตการใช้พอร์ตของ TCP/IP บนระบบของคุณ. แอ็พพลิเคชันของผู้ใช้ที่มีส่วนเกี่ยวข้องกับพอร์ตของ TCP/IP อาจมี “ช่องทางลับ” เข้าสู่ระบบของคุณโดยไม่ต้องใช้ user ID และรหัสผ่าน. บางคนที่มีสิทธิที่พอเพียงบนระบบของคุณสามารถสร้างความสัมพันธ์ระหว่างแอ็พพลิเคชันกับพอร์ต TCP หรือ UDP ได้.
- ในฐานะของผู้บริหารความปลอดภัย, คุณควรจะต้องรู้เทคนิคที่เรียกว่า *IP spoofing* (การปลอมแปลง IP) ที่ใช้โดยนักเจาะระบบ. ทุกๆ ระบบในเครือข่าย TCP/IP มี IP แอดเดรส. บางคนที่ใช้การปลอมแปลง IP สร้างระบบ (มักจะเป็นพีซี) ที่ปลอมแปลงเป็น IP แอดเดรสที่มีอยู่ หรือ IP แอดเดรสที่เชื่อถือได้. ดังนั้น, ผู้ประสงค์ร้ายสามารถสร้างการติดต่อกับระบบของคุณ โดยการปลอมเป็นระบบที่คุณติดต่อด้วยตามปกติ.

  ถ้าคุณมี TCP/IP ทำงานอยู่บนระบบของคุณและระบบของคุณอยู่ในเครือข่ายที่ไม่มีการป้องกันทางกายภาพ (ใช้สายต่อตรง และจุดเชื่อมที่กำหนดไว้ล่วงหน้า), คุณกำลังเสี่ยงอยู่กับการถูกปลอมแปลง IP (IP spoofing). เพื่อป้องกันระบบของคุณจากความเสียหายโดย “ผู้ปลอมแปลง”, (spoofer) เริ่มต้นด้วยคำแนะนำในบทนี้ เช่น การป้องกันการ sign-on และความปลอดภัยของอ็อบเจ็กต์. คุณอาจต้องทำให้แน่ใจว่าระบบของคุณมีการตั้งค่าจำกัดหน่วยความจำสำรอง (auxiliary storage) ที่เหมาะสม. ซึ่งจะป้องกันผู้ปลอมแปลงจากการทำให้ระบบของคุณเต็มโดยใช้เมล์ (จดหมาย) หรือไฟล์ที่ถูก spool ไปถึงจุดที่ระบบของคุณไม่สามารถทำงานต่อได้.

  นอกเหนือจากนี้, คุณควรเฝ้าสังเกตกิจกรรม TCP/IP บนระบบของคุณอย่างสม่ำเสมอ. ถ้าคุณตรวจพบการปลอมแปลง IP คุณจะสามารถค้นพบจุดอ่อนในการตั้ง TCP/IP ของคุณและทำการปรับแต่งให้เหมาะสม.
- สำหรับอินทราเน็ตของคุณ (เครือข่ายหรือระบบที่ไม่จำเป็นต้องติดต่อโดยตรงกับภายนอก), ใช้ IP แอดเดรสที่สามารถใช้ซ้ำได้ (reusable). แอดเดรสที่ใช้ซ้ำได้มีไว้สำหรับใช้ภายในเครือข่ายส่วนตัว. อินเตอร์เน็ตแบ็กโบน (internet backbone) ไม่เปลี่ยนเส้นทางแพ็กเก็ตที่มีแอดเดรสที่สามารถใช้ซ้ำได้. ดังนั้น, แอดเดรสที่ใช้ซ้ำได้เป็นการเพิ่มชั้นของการป้องกันภายในไฟร์วอลล์ของคุณ.

  TCP/IP เว็บไซต์ของ iSeries Information Center—>Networking—> จะมีข้อมูลที่เกี่ยวกับวิธีการกำหนดค่า IP addresses และเกี่ยวกับช่วงของ IP addresses, รวมทั้งข้อมูลของความปลอดภัยที่เกี่ยวกับ TCP/IP.

- ถ้าคุณพิจารณาการเชื่อมต่อระบบของคุณเข้ากับอินเตอร์เน็ตหรืออินทราเน็ต, ให้ทบทวนข้อมูลของความปลอดภัยที่*SecureWay: iSeries and the Internet* (iSeries Information Center—>Security—>SecureWay). โปรดดูที่ "สิ่งที่ต้องรู้ก่อนและข้อมูลที่เกี่ยวข้อง" ในหน้า xiii สำหรับข้อมูลในการเข้าถึง iSeries Information Center.

การควบคุมที่เซิร์ฟเวอร์ TCP/IP เริ่มการทำงานโดยอัตโนมัติ

ในฐานะผู้บริหารความปลอดภัย, คุณต้องควบคุมว่าจะให้แอ็พพลิเคชัน TCP/IP ใดเริ่มต้นโดยอัตโนมัติ เมื่อคุณเริ่มต้น TCP/IP. มีสองคำสั่งที่ใช้ในการเริ่มต้น TCP/IP. สำหรับแต่ละคำสั่ง, ระบบจะใช้วิธีการที่ต่างกันในการพิจารณาว่าจะให้แอ็พพลิเคชัน (เซิร์ฟเวอร์) ใดเริ่มต้น.

ตารางที่ 22แสดงสองคำสั่งและคำแนะนำด้านความปลอดภัยของทั้งสองคำสั่ง. ตารางที่ 23 ในหน้า 136 แสดงค่า autostart ดีฟอลต์สำหรับเซิร์ฟเวอร์. ในการเปลี่ยนแปลงค่า autostart สำหรับเซิร์ฟเวอร์, ให้ใช้คำสั่ง CHGxxxA (Change xxx Attributes) สำหรับเซิร์ฟเวอร์. ตัวอย่างเช่น, คำสั่งสำหรับ TELNET คือ CHGTELNA.

ตารางที่ 22. วิธีการของคำสั่ง TCP/IP ในการตัดสินว่าเซิร์ฟเวอร์ใดจะเริ่มทำงาน

คำสั่ง	เซิร์ฟเวอร์ใดเริ่มทำงาน	คำแนะนำเกี่ยวกับความปลอดภัย
การเริ่มการทำงานของ TCP/IP (STRTCP)	ระบบจะเริ่มต้นทุกๆ เซิร์ฟเวอร์ที่กำหนด AUTOSTART(*YES). ตารางที่ 23 ในหน้า 136 แสดงค่าที่มาพร้อมกับเครื่องสำหรับแต่ละเซิร์ฟเวอร์ TCP/IP.	• กำหนดสิทธิพิเศษ *IOSYSCFG อย่างระมัดระวังเพื่อควบคุมผู้ที่สามารถเปลี่ยนแปลงค่า autostart. • ระมัดระวังในการควบคุมผู้ที่มีสิทธิที่จะใช้คำสั่ง STRTCP. ค่าดีฟอลต์ของสิทธิพับลิกสำหรับคำสั่งนี้คือ *EXCLUDE. • จัดเตรียมการตรวจสอบอ็อบเจ็กต์สำหรับคำสั่ง Change*server-name* Attributes (เช่น CHGTELNA) เพื่อเฝ้าสังเกตผู้ใช้ที่พยายามเปลี่ยนแปลงค่า AUTOSTART สำหรับเซิร์ฟเวอร์.
Start TCP/IP Server (STRTCPSVR)	คุณใช้พารามิเตอร์ในการกำหนดว่าจะให้เซิร์ฟเวอร์ใดเริ่มต้น. ค่าดีฟอลต์ของคำสั่งนี้ที่มาพร้อมเครื่องมือจะเริ่มต้นทุกเซิร์ฟเวอร์.	• ใช้คำสั่ง Change Command Default (CHGCMDDFT) เพื่อจัดเตรียมคำสั่ง STRTCPSVR ให้เริ่มต้นเฉพาะเซิร์ฟเวอร์ที่กำหนดเท่านั้น. ซึ่งไม่ได้ป้องกันผู้ใช้จากการเริ่มต้นเซิร์ฟเวอร์อื่นๆ . อย่างไรก็ตาม, การเปลี่ยนแปลงค่าดีฟอลต์ของคำสั่งจะทำให้โอกาสที่ผู้ใช้จะเริ่มต้นทุกเซิร์ฟเวอร์โดยไม่ตั้งใจน้อยลง. ตัวอย่างเช่น, ใช้คำสั่งนี้ในการกำหนดให้เริ่มต้นเฉพาะเซิร์ฟเวอร์ TELNET:`CHGCMDDFT CMD(STRTCPSVR) NEWDFT('SERVER(*TELNET)')` **หมายเหตุ:** เมื่อคุณเปลี่ยนแปลงค่าดีฟอลต์, คุณสามารถกำหนดได้เพียงเซิร์ฟเวอร์เดียว. ให้เลือกเฉพาะเซิร์ฟเวอร์ที่คุณใช้เป็นประจำหรือเซิร์ฟเวอร์ที่มีปัญหาด้านความปลอดภัยน้อย (เช่น TFTP). • ระมัดระวังในการควบคุมผู้ที่มีสิทธิที่จะใช้คำสั่ง STRTCPSVR. ค่าดีฟอลต์ของสิทธิพับลิกสำหรับคำสั่งนี้คือ *EXCLUDE.

ตารางต่อไปนี้มีค่าเริ่มต้นอัตโนมัติสำหรับเซิร์ฟเวอร์ TCP/IP. สำหรับข้อมูลเพิ่มเติมเกี่ยวกับเซิร์ฟเวอร์แต่ละตัวนี้, โปรดดูที่ iSeries Information Center (**Networking—>TCP/IP**). โปรดดูที่ "สิ่งที่ต้องรู้ก่อนและข้อมูลที่เกี่ยวข้อง" ในหน้า xiii สำหรับรายละเอียดในการเข้าถึง iSeries Information Center.

ตารางที่ 23. ค่าเริ่มต้นอัตโนมัติสำหรับเซิร์ฟเวอร์ TCP/IP

เซิร์ฟเวอร์	ค่าดีฟอล์ต	ค่าของคุณ
TELNET	AUTOSTART(*YES)	
FTP (file transfer protocol)	AUTOSTART(*YES)	
BOOTP (Bootstrap Protocol)	AUTOSTART(*NO)	
TFTP (trivial file transfer protocol)	AUTOSTART(*NO)	
REXEC (Remote EXECution server)	AUTOSTART(*NO)	
RouteD (Route Daemon)	AUTOSTART(*NO)	
SMTP (simple mail transfer protocol)	AUTOSTART(*YES)	
POP (Post Office Protocol)	AUTOSTART(*NO)	
HTTP (Hypertext Transfer Protocol) [1]	AUTOSTART(*NO)	
ICS (Internet Connection Server)[1]	AUTOSTART(*NO)	
LPD (line printer daemon)	AUTOSTART(*YES)	
SNMP (Simple Network Management Protocol (SNMP))	AUTOSTART(*YES)	
DNS (domain name system)	AUTOSTART(*NO)	
DDM	AUTOSTART(*NO)	
DHCP (dynamic host configuration protocol)	AUTOSTART(*NO)	
NSMI	AUTOSTART(*NO)	
INETD	AUTOSTART(*NO)	

หมายเหตุ:

1. ด้วยเซิร์ฟเวอร์ HTTP ของ IBM สำหรับเซิร์ฟเวอร์iSeries, คุณสามารถใช้คำสั่ง CHGHTTPA ในการตั้งค่า AUTOSTART .

ข้อควรพิจารณาเกี่ยวกับความปลอดภัยสำหรับการใช้ SLIP

การสนับสนุน TCP/IP บนเซิร์ฟเวอร์ iSeries จะรวม Serial Interface Line Protocol (SLIP) เอาไว้ด้วย. SLIP ทำให้มีการติดต่อระหว่าง point-to-point ที่มีต้นทุนต่ำ. ผู้ใช้ SLIP สามารถติดต่อไปยัง LAN หรือ WAN โดยการสร้างการติดต่อ point-to-point กับระบบที่เป็นส่วนหนึ่งของ LAN หรือ WAN.

SLIP วิ่งอยู่บนการเชื่อมต่อแบบอะซิงโครนัส (asynchronous). คุณสามารถใช้ SLIP สำหรับการเชื่อมต่อแบบ dial-up ไปยัง และ เรียกจากเซิร์ฟเวอร์ iSeries. ตัวอย่างเช่น, คุณอาจใช้ SLIP เพื่อต่อเลขหมายจากเครื่องพีซีของคุณไปยังระบบ iSeries. หลังจากที่สร้างการติดต่อแล้ว, คุณสามารถ

ใช้แอ็พพลิเคชัน TELNET บนเครื่องพีซีของคุณเพื่อติดต่อไปยังเซิร์ฟเวอร์ TELNET ของ iSeries. หรือคุณสามารถใช้แอ็พพลิเคชัน FTP เพื่อส่งไฟล์ระหว่างสองระบบ.

ไม่มี SLIP configuration อยู่ในระบบของคุณเมื่อเครื่องถูกจัดส่งมา. ดังนั้น, ถ้าคุณไม่ต้องการให้ SLIP (และ dial-up TCP/IP) ทำงานในระบบของคุณ, ไม่ต้องตั้งค่าคอนฟิกูเรชันโปรไฟล์ใดๆ สำหรับ SLIP. คุณใช้คำสั่ง Work with TCP/IP Point-to-Point (WRKTCPPTP) เพื่อสร้างคอนฟิกูเรชันของ SLIP. คุณจะต้องมีสิทธิพิเศษ *IOSYSCFG เพื่อใช้คำสั่ง WRKTCPPTP.

ถ้าคุณต้องการให้ SLIP ทำงานในระบบของคุณ, คุณต้องสร้างคอนฟิกูเรชันโปรไฟล์ของ SLIP (point-to-point) หนึ่งโปรไฟล์หรือมากกว่านั้น. คุณสามารถสร้างคอนฟิกูเรชันโปรไฟล์ด้วยโหมดการทำงานดังนี้:

- Dial in (*ANS)
- Dial out (*DIAL)

หัวข้อต่อไปอธิบายว่า คุณสามารถจัดเตรียมความปลอดภัยสำหรับคอนฟิกูเรชันโปรไฟล์ของ SLIP ได้อย่างไร.

หมายเหตุ: **โปรไฟล์ผู้ใช้** เป็นอ็อบเจ็กต์ของเซิร์ฟเวอร์ iSeries ที่อนุญาตให้ทำการ sign-on ได้. เซิร์ฟเวอร์ iSeries ทุกตัวจะต้องมีโปรไฟล์ผู้ใช้ที่จะรัน. **คอนฟิกูเรชันโปรไฟล์ (configuration profile)** เก็บข้อมูลที่ใช้ในการเริ่มต้นการติดต่อแบบ SLIP กับระบบ iSeries. เมื่อคุณเริ่มการทำงานของการเชื่อมต่อแบบ SLIP ไปยังเซิร์ฟเวอร์ iSeries , คุณจะต้องทำการสร้างลิงก์ขึ้นมาเสมอ. คุณยังไม่ได้ sign on และเริ่มการทำงานของเซิร์ฟเวอร์ iSeries . ดังนั้น, คุณไม่จำเป็นที่จะต้องใช้โปรไฟล์ผู้ใช้ในการเริ่มการเชื่อมต่อแบบ SLIP ไปยังเซิร์ฟเวอร์ iSeries . อย่างไรก็ตาม, ดังที่คุณจะได้เห็นในการพิจารณาต่อไปนี้, โปรไฟล์ของ configuration ของ SLIP อาจจำเป็นที่จะต้องใช้โปรไฟล์ผู้ใช้ในการตัดสินใจว่าจะให้มีการเชื่อมต่อเกิดขึ้นหรือไม่.

การควบคุมการเชื่อมต่อแบบ dial-in SLIP

ก่อนหน้าที่บางคนจะสามารถเริ่มต้นการติดต่อแบบ dial-in ไปยังระบบของคุณด้วย SLIP, คุณต้องให้คอนฟิกูเรชันโปรไฟล์ *ANS ของ SLIP เริ่มทำงาน. เพื่อสร้างหรือเปลี่ยนแปลงคอนฟิกูเรชันโปรไฟล์ของ SLIP, ให้คุณใช้คำสั่ง Work with TCP/IP Point-to-Point (WRKTCPPTP). เพื่อเริ่มต้นคอนฟิกูเรชันโปรไฟล์, คุณสามารถใช้ทั้งคำสั่ง Start TCP/IP Point-to-Point (STRTCPPTP) หรืออ็อพชันจากหน้าจอ WRKTCPPTP. เมื่อระบบของคุณถูกจัดส่งมา, สิทธิพับลิกสำหรับคำสั่ง STRTCPPTP และ ENDTCPPTP คือ *EXCLUDE. อ็อพชันสำหรับ เพิ่ม, เปลี่ยนแปลง, และลบ คอนฟิกูเรชันโปรไฟล์ของ SLIP จะใช้ได้ก็ต่อเมื่อคุณมีสิทธิพิเศษ *IOSYSCFG. ในฐานะผู้บริหารความปลอดภัย, คุณสามารถใช้ทั้งสิทธิในคำสั่งและสิทธิพิเศษ พิจารณาผู้ที่สามารถจัดเตรียมระบบของคุณเพื่ออนุญาตให้มีการติดต่อแบบ dial-in.

การรักษาความปลอดภัยให้กับการเชื่อมต่อแบบ dial-in SLIP

ถ้าคุณต้องการตรวจสอบระบบที่ dial in เข้ามายังระบบของคุณ, คุณจะต้องให้ระบบที่ร้องขอส่ง user ID และรหัสผ่านมาให้. ระบบของคุณจึงจะสามารถตรวจสอบ user ID และรหัสผ่าน. ถ้า user ID และรหัสผ่านไม่ถูกต้อง, ระบบของคุณสามารถปฏิเสธการร้องขอเซสชัน.

เพื่อจัดเตรียมการตรวจสอบ dial-in, ให้ทำดังนี้:

__ ขั้นตอนที่ 1. สร้างโปรไฟล์ผู้ใช้ที่ระบบที่ร้องขอ (request) สามารถใช้สร้างการติดต่อ. User ID และรหัสผ่านที่ผู้ร้องขอส่งต้องตรงกับชื่อโปรไฟล์ผู้ใช้และรหัสผ่านนี้.

หมายเหตุ: สำหรับระบบที่ทำการตรวจสอบรหัสผ่าน, ค่าระบบ QSECURITY จะต้องถูกกำหนดเป็น 20 หรือสูงกว่า.

สำหรับการป้องกันเพิ่มเติม, คุณอาจต้องสร้างโปรไฟล์ผู้ใช้เฉพาะสำหรับเริ่มต้นการติดต่อแบบ SLIP. โปรไฟล์ผู้ใช้ควรจะมีสิทธิในระบบที่จำกัด. ถ้าคุณไม่ได้วางแผนที่จะใช้โปรไฟล์สำหรับการทำงานอื่นนอกจากสร้างการติดต่อแบบ SLIP, คุณสามารถกำหนดค่าข้างล่างนี้ในโปรไฟล์ผู้ใช้:

- initial menu (INLMNU) เป็น *SIGNOFF
- initial program (INLPGM) เป็น *NONE.
- Limit capabilities (LMTCPB) เป็น *YES

ค่าเหล่านี้ป้องกันบุคคลใดก็ตามจากการ sign on แบบโต้ตอบด้วยโปรไฟล์ผู้ใช้.

__ ขั้นตอนที่ 2. สร้าง authorization list สำหรับระบบเพื่อตรวจสอบ เมื่อผู้ร้องขอพยายามเริ่มการติดต่อแบบ SLIP.

หมายเหตุ: คุณกำหนด authorization list นี้ในฟิลด์ *System access authorization list* เมื่อคุณสร้างหรือเปลี่ยนแปลงโปรไฟล์ของ SLIP. (ดูขั้นตอนที่ 4.)

__ ขั้นตอนที่ 3. ใช้คำสั่ง Add Authorization Entry (ADDAUTLE) เพื่อเพิ่มโปรไฟล์ผู้ใช้ที่คุณสร้างในขั้นตอนที่ 1 ให้กับ authorization list. คุณสามารถสร้าง authorization list เฉพาะสำหรับแต่ละคอนฟิกูเรชันโปรไฟล์แบบ point-to-point, หรือคุณสามารถสร้าง authorization list ที่หลายคอนฟิกูเรชันโปรไฟล์ใช้ร่วมกัน.

__ ขั้นตอนที่ 4. ใช้คำสั่ง WRKTCPPTP เพื่อจัดเตรียมโปรไฟล์ *ANS แบบ TCP/IP point-to-point ที่มีคุณลักษณะดังนี้:

- คอนฟิกูเรชันโปรไฟล์ต้องใช้สคริปต์ไดอะล็อกการติดต่อ (connection dialog script) ที่มีฟังก์ชันในการตรวจสอบผู้ใช้. การตรวจสอบผู้ใช้เป็นการรับ user ID และรหัสผ่าน จากผู้ร้องขอและตรวจสอบความถูกต้องของค่าเหล่านั้น. ระบบมาพร้อมกับสคริปต์ไดอะล็อกหลายตัวอย่างที่มีฟังก์ชันนี้.
- คอนฟิกูเรชันโปรไฟล์ต้องระบุชื่อของ authorization list ที่คุณสร้างในขั้นที่ 2. User ID ที่สคริปต์ไดอะล็อกการติดต่อได้รับ ต้องอยู่ใน authorization list.

จำไว้เสมอว่าค่าของการจัดเตรียมความปลอดภัยแบบ dial-in ได้รับผลจากวิธีการปฏิบัติด้านความปลอดภัย และความสามารถของระบบที่คุณ dial in. ถ้าคุณต้องการ user ID และรหัสผ่าน, สคริปต์ไดอะล็อกการติดต่อบนระบบที่ร้องขอต้องส่ง user ID และรหัสผ่านนั้น. บางระบบ, อาทิเช่น เซิร์ฟเวอร์ iSeries , มีวิธีการรักษาความปลอดภัยสำหรับการบันทึก user ID และ รหัสผ่าน. (“ความปลอดภัย และเซสชันการ dial-out” ในหน้า 139 อธิบายถึงวิธีการนั้น.) ระบบอื่นๆ เก็บ user ID และรหัสผ่านในสคริปต์ที่อาจถูกเข้าถึงโดยบุคคลที่ทราบว่าจะพบสคริปต์ได้ในที่ใดบนระบบ.

เนื่องจากความแตกต่างด้านวิธีการดำเนินการด้านความปลอดภัยและความสามารถของผู้ที่ติดต่อสื่อสารกับคุณ, คุณอาจต้องการสร้างคอนฟิกูเรชันโปรไฟล์ที่แตกต่างกันสำหรับสภาพแวดล้อมในการร้องขอที่แตกต่างกัน. คุณใช้คำสั่ง STRTCPPTP เพื่อจัดเตรียมระบบของคุณให้รับเซสชันสำหรับเฉพาะบางคอนฟิกูเรชันโปรไฟล์. คุณสามารถเริ่มเซสชั่นสำหรับบางคอนฟิกูเรชั่นโปรไฟล์เฉพาะในบางเวลาของแต่ละวัน. ตัวอย่างเช่น, คุณอาจใช้การตรวจสอบความปลอดภัยโดยการบันทึกกิจกรรมสำหรับโปรไฟล์ผู้ใช้ที่เกี่ยวข้อง.

ป้องกันผู้ใช้ที่ dial-in เข้ามาจากการเข้าถึงระบบอื่นๆ

ขึ้นอยู่กับระบบของคุณและคอนฟิกูเรชันของเครือข่าย, ผู้ใช้ที่เริ่มการติดต่อแบบ SLIP อาจสามารถที่จะเข้าถึงระบบอื่นๆ ในเครือข่ายของคุณโดยไม่ต้อง sign on ไปยังระบบของคุณ. ตัวอย่างเช่น, ผู้ใช้สามารถเริ่มต้นการติดต่อแบบ SLIP ไปยังระบบของคุณ. จากนั้นผู้ใช้อาจเริ่มต้นการติดต่อแบบ FTP ไปยังระบบอื่นในเครือข่ายของคุณที่ไม่อนุญาตให้ dial-in.

คุณสามารถป้องกันผู้ใช้ SLIP จากการเข้าไปในระบบอื่นๆ ในเครือข่ายของคุณโดยการกำหนด N (No) สำหรับฟิลด์ *Allow IP datagram forwarding* ในคอนฟิกูเรชันโปรไฟล์. ซึ่งป้องกันผู้ใช้จากการเข้าถึงเครือข่ายของคุณก่อนที่ผู้ใช้จะล็อกออน (log on) ไปยังระบบของคุณ. อย่างไรก็ตาม, หลังจากที่ผู้ใช้สามารถล็อกออนไปยังระบบของคุณเป็นผลสำเร็จ, ค่า datagram forwarding จะไม่มีผล. ซึ่งจะไม่จำกัดความสามารถของผู้ใช้ในการใช้แอ็พพลิเคชัน TCP/IP บนระบบ iSeries (เช่น FTP หรือ TELNET),เพื่อเริ่มการติดต่อกับระบบอื่นในเครือข่ายของคุณ.

การควบคุมเซสชัน dial-out

ก่อนที่บางคนจะสามารถใช้ SLIP เพื่อสร้างการติดต่อแบบ dial-out จากระบบของคุณ, คุณต้องให้คอนฟิกูเรชันโปรไฟล์ *DIAL ของ SLIP เริ่มทำงาน. เพื่อสร้างหรือเปลี่ยนแปลงคอนฟิกูเรชันโปรไฟล์ของ SLIP, ให้คุณใช้คำสั่งWRKTCPPTP. เพื่อเริ่มต้นคอนฟิกูเรชันโปรไฟล์, คุณสามารถใช้ทั้งคำสั่ง Start TCP/IP Point-to-Point (STRTCPPTP) หรืออ็อพชันจากหน้าจอ WRKTCPPTP. เมื่อระบบของคุณถูกจัดส่งมา, สิทธิพับลิกสำหรับคำสั่ง STRTCPPTP และ ENDTCPPTP คือ *EXCLUDE. อ็อพชันสำหรับ เพิ่ม, เปลี่ยนแปลง, และลบคอนฟิกูเรชันโปรไฟล์ของ SLIP จะใช้ได้ก็ต่อเมื่อคุณมีสิทธิพิเศษ *IOSYSCFG. ในฐานะผู้บริหารความปลอดภัย, คุณสามารถใช้ทั้งสิทธิในคำสั่งและสิทธิพิเศษ พิจารณาผู้ที่สามารถจัดเตรียมระบบของคุณเพื่ออนุญาตให้มีการติดต่อแบบ dial-out.

ความปลอดภัย และเซสชันการ dial-out

ผู้ใช้บนระบบ iSeries ของคุณอาจต้องการเริ่มต้นการติดต่อ dial-out ไปยังระบบที่ต้องการการตรวจสอบผู้ใช้. ไดอะล็อกสคริปต์ของการเชื่อมต่อบนไดอะล็อกของเซิร์ฟเวอร์ iSeries ของคุณจะต้องส่ง user ID และ รหัสผ่าน ไปยังระบบรีโมต. เซิร์ฟเวอร์ iSeries มีวิธีในการรักษาความปลอดภัยสำหรับการบันทึกรหัสผ่านนั้น. รหัสผ่านไม่จำเป็นต้องถูกเก็บไว้ในสคริปต์ไดอะล็อกการติดต่อ.

หมายเหตุ:

1. ถึงแม้ว่าระบบของคุณจัดเก็บรหัสผ่านของการติดต่อในรูปแบบที่ถูกเข้ารหัส, ระบบของคุณจะถอดรหัสผ่าน ก่อนที่จะส่งรหัสผ่านออกไป. รหัสผ่านของ SLIP, เช่นเดียวกับรหัสผ่านของ FTP และ TELNET, ถูกส่งออกไปแบบไม่ได้เข้ารหัส(“ในแบบเดิม”). อย่างไรก็ตาม, ที่ต่างจาก FTP และ TELNET คือ, รหัสผ่านของ SLIP ถูกส่งก่อนที่ระบบจะเริ่มต้นโหมด TCP/IP.

เนื่องจาก SLIP ใช้การติดต่อแบบ point-to-point ในโหมดอะซิงโครนัส, จุดอ่อนด้านความปลอดภัยเมื่อทำการส่งรหัสผ่านที่ไม่ได้เข้ารหัส จะแตกต่างจากจุดอ่อนที่เกิดกับรหัสผ่านของ FTP และ TELNET. รหัสผ่านของ FTP และ TELNET ที่ไม่ได้เข้ารหัสอาจถูกส่งเป็นทราฟฟิกของ IP บนเครือข่าย, และไม่ปลอดภัยต่อการถูกดูดข้อมูลทางอิเล็กทรอนิกส์. การส่งรหัสผ่านของ SLIP ของคุณมีความปลอดภัยเหมือนกับการติดต่อผ่านโทรศัพท์ระหว่างสองระบบ.

2. ดีฟอลต์ไฟล์สำหรับจัดเก็บสคริปต์ไดอะล็อกการติดต่อของ SLIP คือ QUSRSYS/QATOCPPSCR. สิทธิพับลิกสำหรับไฟล์นี้คือ *USE, ซึ่งป้องกันผู้ใช้พับลิกจากการเปลี่ยนแปลงสคริปต์ไดอะล็อกการติดต่อดีฟอลต์.

เมื่อคุณสร้างโปรไฟล์การติดต่อสำหรับรีโมตเซสชันที่ต้องการการตรวจสอบ, ให้ทำดังนี้:

__ ขั้นตอนที่ 1. ต้องแน่ใจว่าค่ากำหนดของระบบ Retain Server Security Data (QRETSVRSEC) เป็น 1 (Yes). ค่ากำหนดของระบบนี้พิจารณาว่าคุณจะอนุญาตให้รหัสผ่านที่สามารถถูกถอดรหัสได้นั้นเก็บอยู่ในพื้นที่ป้องกัน (protected area) บนระบบของคุณหรือไม่.

__ ขั้นตอนที่ 2. ใช้คำสั่ง WRKTCPPTP เพื่อสร้างคอนฟิกูเรชันโปรไฟล์ ที่มีลักษณะดังนี้:

- สำหรับโหมดของคอนฟิกูเรชันโปรไฟล์, ระบุค่า *DIAL.
- สำหรับ *Remote service access name*, ระบุ user ID ที่ระบบรีโมตต้องการ. ตัวอย่างเช่น, ถ้าคุณกำลังเชื่อมต่ออยู่กับเซิร์ฟเวอร์ iSeries อีกเซิร์ฟเวอร์หนึ่ง, ให้ระบุชื่อของโปรไฟล์ผู้ใช้บนเซิร์ฟเวอร์ iSeries นั้น.
- สำหรับ *Remote service access password*, ระบุรหัสผ่านที่ระบบรีโมตต้องการสำหรับ user ID นี้. บนเซิร์ฟเวอร์ iSeries ของคุณ, รหัสผ่านนี้จะถูกบันทึกในเนื้อที่ที่ได้รับการปกป้องในรูปแบบที่สามารถถอดรหัสได้. ชื่อและรหัสผ่านที่คุณกำหนดสำหรับคอนฟิกูเรชันโปรไฟล์มีความสัมพันธ์กับโปรไฟล์ผู้ใช้ QTCP. ชื่อและรหัสผ่านไม่สามารถเข้าถึงโดยคำสั่งผู้ใช้หรืออินเตอร์เฟสใดๆ. มีเพียงโปรแกรมระบบที่ลงทะเบียนไว้เท่านั้น ที่จะสามารถเข้าถึงข้อมูลรหัสผ่านนี้.

  หมายเหตุ: จำไว้เสมอว่ารหัสผ่านสำหรับโปรไฟล์การติดต่อของคุณไม่ถูกจัดเก็บ เมื่อคุณจัดเก็บไฟล์คอนฟิกูเรชันของ TCP/IP. เพื่อจัดเก็บรหัสผ่านของ SLIP, คุณต้องใช้คำสั่ง Save Security Data (SAVSECDTA) เพื่อจัดเก็บโปรไฟล์ผู้ใช้ QTCP.
- สำหรับสคริปต์ไดอะล็อกการติดต่อ, ระบุสคริปต์ที่ส่ง user ID และรหัสผ่าน. ระบบมาพร้อมกับสคริปต์ไดอะล็อกหลายตัวอย่างที่มีฟังก์ชันนี้. เมื่อระบบเรียกใช้สคริปต์, ระบบจะทำการดึงรหัสผ่าน, ถอดรหัส, และส่งรหัสผ่านไปยังระบบรีโมต.

ข้อควรพิจารณาเกี่ยวกับความปลอดภัยสำหรับโปรโตคอลแบบ point-to-point

โปรโตคอลแบบ point-to-point (PPP) จะมีอยู่ในรูปของส่วนหนึ่งของ TCP/IP. PPP เป็นมาตรฐานอุตสาหกรรมของการติดต่อแบบ point-to-point ที่มีฟังก์ชันเพิ่มเติมมากกว่าที่มีกับ SLIP.

ด้วย PPP, เซิร์ฟเวอร์ iSeries ของคุณสามารถมีการเชื่อมต่อที่มีความเร็วสูงโดยตรงไปยังผู้ให้บริการอินเตอร์เน็ตหรือ ไปยังระบบอื่นๆ ในอินทราเน็ตหรือเอ็กซ์ทราเน็ต. รีโมต LAN สามารถทำการเชื่อมต่อแบบ dial-in ไปยังเซิร์ฟเวอร์ iSeries ของคุณได้จริง.

จำไว้ว่า PPP, เช่นเดียวกันกับ SLIP, มีการเชื่อมต่อเน็ตเวิร์กไปยังเซิร์ฟเวอร์ iSeries ของคุณ. การติดต่อแบบ PPP ได้พาเอาผู้ร้องขอ (requester) มายังประตูของระบบของคุณ. ผู้ร้องขอยังต้องใช้ user ID และรหัสผ่านเพื่อเข้าสู่ระบบของคุณ และติดต่อไปยังเซิร์ฟเวอร์เช่น TELNET หรือ FTP. ต่อไปนี้คือสิ่งที่ควรพิจารณาเกี่ยวกับความปลอดภัย สำหรับความสามารถในการติดต่อใหม่นี้:

หมายเหตุ: คุณสามารถปรับแต่งค่าของ PPP โดยการใช้ iSeries Navigator ที่อยู่บนเวิร์กสเตชันIBM iSeries Access for Windows.

- PPP ทำให้ความสามารถที่จะมีการติดต่อแบบ dedicated (ที่ผู้ใช้เดียวกันมี IP แอดเดรสเดียวกันเสมอ. ด้วยแอดเดรสแบบ dedicated, คุณมีแนวโน้มที่จะถูกปลอมแปลง IP (ระบบที่ประสงค์ร้ายที่แสร้งทำเป็นระบบที่น่าเชื่อถือโดยค่า IP แอดเดรสที่เป็นที่รู้จัก). อย่างไรก็ตาม, ความสามารถในการพิสูจน์ตัวจริงที่มีประสิทธิภาพที่ PPP มีนั้นจะช่วยป้องกันการปลอมแปลง IP ได้.
- ด้วย PPP, เช่นเดียวกับ SLIP, คุณสร้างโปรไฟล์การติดต่อที่มีชื่อผู้ใช้และรหัสผ่านที่สัมพันธ์กัน. อย่างไรก็ตาม, ไม่เหมือนกับ SLIP, ผู้ใช้ไม่จำเป็นที่จะต้องมีโปรไฟล์ผู้ใช้และรหัสผ่านที่ถูกต้อง. user name และ รหัสผ่าน ไม่ได้เกี่ยวโยงกับโปรไฟล์ผู้ใช้. มีการใช้รายการการตรวจสอบ (validation list) สำหรับการพิสูจน์ตัวจริงของ PPP. นอกจากนี้, PPP ไม่ต้องการสคริปต์การติดต่อ. การพิสูจน์ตัวจริง (การแลกเปลี่ยนชื่อผู้ใช้และรหัสผ่าน) เป็นส่วนหนึ่งของสถาปัตยกรรม PPP และเกิดขึ้นในระดับที่ต่ำกว่า SLIP.
- ด้วย PPP, คุณมีอ็อพชั่นที่จะใช้ CHAP (challenge handshake authentication protocol). คุณไม่จำเป็นต้องกังวลเกี่ยวกับการลักลอบดูรหัสผ่าน (eavesdropper sniffing password) เนื่องจาก CHAP จะเข้ารหัสชื่อผู้ใช้และรหัสผ่าน.

  การติดต่อแบบ PPP ของคุณใช้ CHAP ก็ต่อเมื่อทั้งสองฝั่งมีการรองรับ CHAP. ระหว่างการแลกเปลี่ยนสัญญาณเพื่อจัดเตรียมการสื่อสารระหว่างโมเด็มสองตัว, ทั้งสองระบบจะ negotiate กัน. ตัวอย่างเช่น, ถ้า SYSTEMA รองรับ CHAP และ SYSTEMB ไม่รองรับ, SYSTEMA สามารถปฏิเสธเซสชันหรือตกลงที่จะใช้ชื่อผู้ใช้และรหัสผ่านที่ไม่ได้เข้ารหัส. การตกลงที่จะใช้ชื่อผู้ใช้และรหัสผ่านที่ไม่ได้เข้ารหัส เรียกว่า negotiating down. การตัดสินใจที่จะ negotiate down เป็นทางเลือกในการปรับตั้งค่า. ตัวอย่างเช่น บนอินทราเน็ตของคุณ, เมื่อคุณทราบว่า ระบบของคุณทั้งหมดมีขีดความสามารถ CHAP, คุณควรจะกำหนดโปรไฟล์การติดต่อของคุณเพื่อที่จะไม่ทำ negotiate down. ในการติดต่อแบบพับลิก ที่ระบบของคุณโทรออกภายนอก, คุณอาจจะต้องการ negotiate down.

  โปรไฟล์การติดต่อสำหรับ PPP มีความสามารถในการกำหนด IP แอดเดรสที่ใช้งานได้. ตัวอย่างเช่น, คุณสามารถบ่งชี้ว่าคุณต้องการแอดเดรสที่กำหนดหรือช่วงของแอดเดรสสำหรับผู้ใช้เฉพาะ. ความสามารถนี้รวมกับความสามารถของรหัสผ่านที่ถูกเข้ารหัสลับจะช่วยป้องกันจากการปลอมแปลง IP.

  เพื่อการป้องกันเพิ่มเติมต่อการปลอมแปลง IP หรือการเกาะมากับเซสชันที่ทำงานอยู่, คุณสามารถกำหนดให้ PPP มีการร้องถามใหม่ในช่วงเวลาที่กำหนด. ตัวอย่างเช่น, ในขณะที่เซสชัน PPP แอ็คทีฟ, เซิร์ฟเวอร์ iSeries ของคุณอาจจะถามถึง ผู้ใช้ และรหัสผ่านจากระบบอื่น. โดยจะ

ทำแบบนี้ในทุกๆ 15 นาที เพื่อให้แน่ใจว่าเป็นโปรไฟล์การติดต่อเดียวกัน. (ผู้ใช้ปลายทางจะไม่รับทราบกิจกรรมการร้องถามใหม่นี้. ระบบจะแลกเปลี่ยนชื่อและรหัสผ่านในระดับที่ต่ำกว่าที่ผู้ใช้ปลายทางนั้นมองเห็น.)

ด้วย PPP, เป็นไปได้ที่จะคาดว่ารีโมต LAN อาจมีการสร้างการเชื่อมต่อแบบ dial-in ไปยังระบบ iSeries ของคุณ และไปยังเน็ตเวิร์กที่ขยายออกไปของคุณ. ในสภาพแวดล้อมนี้, การเปิด IP forwarding อาจเป็นสิ่งที่จำเป็น. IP forwarding อาจยอมให้ผู้บุกรุกไปได้ทั่วทั้งเครือข่ายของคุณ. อย่างไรก็ตาม, PPP มีการป้องกันที่ดีกว่า (เช่น การเข้ารหัสของรหัสผ่านและการตรวจสอบ IP แอดเดรส). ซึ่งเป็นการยากที่ผู้บุกรุกจะสามารถเริ่มต้นการติดต่อเครือข่ายได้ตั้งแต่แรก.

สำหรับข้อมูลเพิ่มเติมเกี่ยวกับ PPP, โปรดดูที่ iSeries Information Center..

ข้อควรพิจารณาด้านความปลอดภัยสำหรับการใช้เซิร์ฟเวอร์ Bootstrap Protocol

Bootstrap Protocol (BOOTP) จะให้วิธีการแบบไดนามิกสำหรับการโยงความสัมพันธ์ระหว่างเวิร์กสเตชันกับเซิร์ฟเวอร์ และกำหนด IP แอดเดรสของเวิร์กสเตชันและให้ซอร์สสำหรับการทำ initial program load (IPL).

BOOTP เป็นโปรโตคอล TCP/IP ที่ใช้อนุญาตให้เวิร์กสเตชันที่ไม่มีหน่วยเก็บข้อมูล (ไคลเอ็นต์) ร้องขอไฟล์ที่มีโค้ดเริ่มต้น (initial code) จากเซิร์ฟเวอร์บนเครือข่าย. เซิร์ฟเวอร์ BOOTP จะรอฟังพอร์ตที่เป็นที่รู้จักของเซิร์ฟเวอร์ BOOTP (พอร์ต 67). เมื่อได้รับการร้องขอจากไคลเอ็นต์, เซิร์ฟเวอร์มองหา IP แอดเดรสที่กำหนดสำหรับไคลเอ็นต์ และตอบกลับไปยังไคลเอ็นต์ด้วย IP แอดเดรสของไคลเอ็นต์และชื่อของไฟล์ที่โหลด. จากนั้น ไคลเอ็นต์จะเริ่มต้นการร้องขอ TFTP ไปยังเซิร์ฟเวอร์สำหรับโหลดไฟล์. การจับคู่กันระหว่างฮาร์ดแวร์แอดเดรสของไคลเอ็นต์ และ IP addressจะถูกเก็บไว้ในตาราง BOOTP บนเซิร์ฟเวอร์ iSeries .

การป้องกันการเข้าถึง BOOTP

ถ้าคุณไม่มี thin client ใดๆ ต่ออยู่กับเน็ตเวิร์กของคุณ, คุณไม่จำเป็นที่จะต้องรันเซิร์ฟเวอร์ BOOTP ที่อยู่บนระบบของคุณ. BOOTP สามารถใช้กับอุปกรณ์อื่นๆ , แต่ทางออกที่ดีกว่าสำหรับอุปกรณ์เหล่านั้นคือการใช้ DHCP. เพื่อป้องกันไม่ให้เซิร์ฟเวอร์ BOOTP ทำงาน ให้ทำดังนี้:

__ ขั้นตอนที่ 1. เพื่อป้องกันไม่ให้งานของเซิร์ฟเวอร์ BOOTP เริ่มต้นโดยอัตโนมัติเมื่อคุณเริ่มต้น TCP/IP, ให้พิมพ์ดังนี้:

```
CHGBPA AUTOSTART(*NO)
```

หมายเหตุ:

1. AUTOSTART(*NO) เป็นค่าดีฟอลต์.
2. “การควบคุมที่เซิร์ฟเวอร์ TCP/IP เริ่มการทำงานโดยอัตโนมัติ” ในหน้า 135 มีข้อมูลเพิ่มเติมเกี่ยวกับการควบคุมให้เซิร์ฟเวอร์ TCP/IP เริ่มทำงานโดยอัตโนมัติ.

__ ขั้นตอนที่ 2. เพื่อป้องกันบางคนจากการสัมพันธ์กับแอ็พพลิเคชันผู้ใช้, เช่น ซ็อกเก็ตแอ็พพลิเคชัน, ด้วยพอร์ตที่ระบบโดยปกติ ใช้สำหรับ BOOTP, ให้ทำดังนี้:

หมายเหตุ: เนื่องจาก DHCP และ BOOTP ใช้หมายเลขพอร์ตเดียวกัน, วิธีนี้จะยับยั้งพอร์ตที่ DHCP ใช้ด้วย. ต้องไม่จำกัดพอร์ต ถ้าคุณต้องการใช้ DHCP.

__ ขั้นตอนที่ a. พิมพ์ GO CFGTCP เพื่อแสดงเมนู Configure TCP/IP.

__ ขั้นตอนที่ b. เลือกอ็อพชัน 4 (Work with TCP/IP port restrictions).

__ ขั้นตอนที่ c. บนหน้าจอ Work with TCP/IP Port Restrictions, ให้ระบุอ็อพชัน 1 (Add).

__ ขั้นตอนที่ d. สำหรับ lower port range, ระบุค่า 67.

__ ขั้นตอนที่ e. สำหรับ upper port range, ระบุค่า *ONLY.

หมายเหตุ:

1. ข้อจำกัดของพอร์ตมีผลครั้งต่อไปที่คุณเริ่มต้น TCP/IP. ถ้า TCP/IP ทำงานอยู่ เมื่อคุณกำหนดข้อจำกัดของพอร์ต, คุณควรจะจบ TCP/IP และเริ่มต้นใหม่อีกครั้ง.
2. RFC1700 มีข้อมูลเกี่ยวกับการกำหนดหมายเลขพอร์ต.

__ ขั้นตอนที่ f. สำหรับ protocol, ระบุค่า *UDP.

__ ขั้นตอนที่ g. สำหรับฟิลด์โปรไฟล์ผู้ใช้, ระบุชื่อโปรไฟล์ผู้ใช้ที่มีการป้องกันในระบบของคุณ. (โปรไฟล์ผู้ใช้ที่มีการป้องกันคือ โปรไฟล์ผู้ใช้ที่ไม่เป็นเจ้าของโปรแกรมที่ได้รับสิทธิมา และไม่มีรหัสผ่านที่ผู้ใช้อื่นทราบ.) โดยการจำกัดพอร์ตให้กับผู้ใช้เฉพาะ, คุณสามารถตัดผู้ใช้อื่นออกไปได้โดยอัตโนมัติ.

การรักษาความปลอดภัยให้กับเซิร์ฟเวอร์ BOOTP

เซิร์ฟเวอร์ BOOTP ไม่ได้ให้การแอ็คเซสโดยตรงไปยังระบบ iSeries ของคุณ, และเป็นจุดอ่อนด้านความปลอดภัยที่ถูกจำกัด. ข้อควรพิจารณาอันดับแรกของคุณในฐานะที่เป็นผู้บริหารความปลอดภัย ก็คือ การทำให้แน่ใจว่าข้อมูลที่ถูกต้องถูกเชื่อมโยงเข้ากับ thin client ที่ถูกต้อง. เรียกอีกอย่างหนึ่งว่า, ผู้ประสงค์ร้ายสามารถทำการเปลี่ยนแปลงตาราง BOOTP และทำให้ thin client ของคุณทำงานผิดพลาดหรือไม่ทำงานเลย.

เพื่อจัดการกับเซิร์ฟเวอร์ BOOTP และตาราง BOOTP, คุณต้องมีสิทธิพิเศษ *IOSYSCFG. คุณจำเป็นต้องควบคุมโปรไฟล์ผู้ใช้ที่มีสิทธิพิเศษ *IOSYSCFG ในระบบของคุณ อย่างระมัดระวัง.

ข้อควรพิจารณาด้านความปลอดภัยสำหรับการใช้เซิร์ฟเวอร์ DHCP

Dynamic host configuration protocol (DHCP) จะให้โครงสร้างสำหรับการส่งผ่านข้อมูลคอนฟิกูเรชันไปยังโฮสต์บนเครือข่าย TCP/IP. สำหรับไคลเอ็นต์เวิร์กสเตชันของคุณ, DHCP สามารถให้ฟังก์ชันที่คล้ายคลึงกับการตั้งค่าโดยอัตโนมัติ. โปรแกรมที่สามารถใช้ DHCP ในไคลเอ็นต์เวิร์กสเตชันจะกระจายการร้องขอข้อมูลคอนฟิกูเรชัน. ถ้าเซิร์ฟเวอร์ DHCP กำลังรันบนเซิร์ฟเวอร์ iSeries ของคุณ, เซิร์ฟเวอร์นั้นจะโต้ตอบกับคำร้องขอโดยการส่งข้อมูลที่ไคลเอ็นต์เวิร์กสเตชันต้องการเพื่อที่จะตั้งค่า TCP/IP ได้อย่างถูกต้อง.

คุณสามารถใช้ DHCP ในการทำให้ผู้ใช้สามารถเชื่อมต่อกับเซิร์ฟเวอร์ iSeries ของคุณได้ง่ายขึ้นในครั้งแรก. ทั้งนี้เนื่องจากผู้ใช้ไม่จำเป็นต้องป้อนข้อมูลคอนฟิกูเรชันของ TCP/IP. คุณยังสามารถใช้ DHCP เพื่อลดจำนวนของแอดเดรสภายในของ TCP/IP ที่คุณต้องการในเครือข่ายย่อย (subnetwork). เซิร์ฟเวอร์ DHCP สามารถจัดสรร IP แอดเดรสชั่วคราวให้กับผู้ใช้ที่แอ็คทีฟ (จาก pool ของ IP แอดเดรส).

สำหรับ thin client, คุณสามารถใช้ DHCP แทน BOOTP ได้. DHCP มีฟังก์ชันมากกว่า BOOTP, และมันสามารถสนับสนุน dynamic configuration ของทั้ง thin client และ พีซี.

การป้องกันการเข้าถึง DHCP

หากคุณ *ไม่* ต้องการให้มีผู้ใดใช้เซิร์ฟเวอร์ DHCP ในระบบของคุณ, ให้ทำดังนี้:

1. เพื่อป้องกันไม่ให้งานของเซิร์ฟเวอร์ DHCP เริ่มต้นโดยอัตโนมัติเมื่อคุณเริ่มต้น TCP/IP, ให้พิมพ์ดังนี้:

   ```
   CHGDHCPA AUTOSTART(*NO)
   ```

   หมายเหตุ:

   1. AUTOSTART(*NO) เป็นค่าดีฟอลต์.
   2. “การควบคุมที่เซิร์ฟเวอร์ TCP/IP เริ่มการทำงานโดยอัตโนมัติ” ในหน้า 135 มีข้อมูลเพิ่มเติมเกี่ยวกับการควบคุมให้เซิร์ฟเวอร์ TCP/IP เริ่มทำงานโดยอัตโนมัติ.
2. เพื่อป้องกันบางคนจากการสัมพันธ์กับแอ็พพลิเคชันผู้ใช้, เช่น ซ็อกเก็ตแอ็พพลิเคชัน, ด้วยพอร์ตที่ระบบโดยปกติ ใช้สำหรับ DHCP, ให้ทำดังนี้:
   a. พิมพ์ GO CFGTCP เพื่อแสดงเมนู Configure TCP/IP.
   b. เลือกอ็อพชัน 4 (Work with TCP/IP port restrictions).
   c. บนหน้าจอ Work with TCP/IP Port Restrictions, ให้ระบุอ็อพชัน 1 (Add).
   d. สำหรับ lower port range, ระบุค่า 67.
   e. สำหรับ upper port range, ระบุค่า 68.

      หมายเหตุ:

      1. ข้อจำกัดของพอร์ตมีผลครั้งต่อไปที่คุณเริ่มต้น TCP/IP. ถ้า TCP/IP ทำงานอยู่ เมื่อคุณกำหนดข้อจำกัดของพอร์ต, คุณควรจะจบ TCP/IP และเริ่มต้นใหม่อีกครั้ง.
      2. RFC1700 มีข้อมูลเกี่ยวกับการกำหนดหมายเลขพอร์ต.

   f. สำหรับ protocol, ระบุค่า *UDP.
   g. สำหรับฟิลด์โปรไฟล์ผู้ใช้, ระบุชื่อโปรไฟล์ผู้ใช้ที่มีการป้องกันในระบบของคุณ. (โปรไฟล์ผู้ใช้ที่มีการป้องกันคือ โปรไฟล์ผู้ใช้ที่ไม่เป็นเจ้าของโปรแกรมที่ได้รับสิทธิมา และไม่มีรหัสผ่านที่ผู้ใช้อื่นทราบ.) โดยการจำกัดพอร์ตให้กับผู้ใช้เฉพาะ, คุณสามารถตัดผู้ใช้อื่นออกไปได้โดยอัตโนมัติ.

การรักษาความปลอดภัยให้กับเซิร์ฟเวอร์ป DHCP

ต่อไปนี้ คือสิ่งที่ควรพิจารณาเกี่ยวกับความปลอดภัย เมื่อคุณเลือกที่จะใช้ DHCP ในระบบ iSeries ของคุณ:

- จำกัดจำนวนของผู้ใช้ที่มีสิทธิในการบริหาร DHCP. การบริหาร DHCP ต้องการสิทธิต่อไปนี้:
  - สิทธิพิเศษ *IOSYSCFG
  - สิทธิ *RW ในไฟล์ต่อไปนี้:

    ```
    /QIBM/UserData/OS400/DHCP/dhcpsd.cfg
    /QIBM/UserData/OS400/DHCP/dhcprd.cfg
    ```
- ประเมินดูวิธีการเข้าถึงระบบ LAN ของคุณทางกายภาพ. บุคคลภายนอกสามารถเดินเข้ามาในที่ของคุณพร้อมกับแล็ปทอป และทำการติดต่อไปยังระบบ LAN ของคุณทางกายภาพได้อย่างง่ายดายหรือไม่? ถ้านี่เป็นช่องโหว่, DHCP จะให้ความสามารถในการสร้างรายชื่อของไคลเอ็นต์ (ฮาร์ดแวร์แอดเดรส) ที่เซิร์ฟเวอร์ DHCP จะตั้งค่า. เมื่อคุณใช้คุณสมบัตินี้, คุณได้ลบประโยชน์บางอย่างในแง่ของปริมาณงานที่ DHCP ช่วยทำให้กับผู้บริหารเครือข่ายของคุณ. อย่างไรก็ตาม, คุณได้ป้องกันระบบจากการตั้งค่าเวิร์กสเตชันที่คุณไม่รู้จัก.
- ถ้าเป็นไปได้, ให้ใช้ pool ของ IP แอดเดรสที่สามารถใช้ซ้ำได้ (ไม่ได้ถูกออกแบบสำหรับอินเตอร์เน็ต). ซึ่งช่วยป้องกันเวิร์กสเตชันที่อยู่ภายนอกเครือข่ายของคุณ จากการได้รับข้อมูลคอนฟิกูเรชันที่มีประโยชน์จากเซิร์ฟเวอร์.
- ใช้จุดทางออกของ DHCP ถ้าคุณต้องการการป้องกันความปลอดภัยเพิ่มเติม . ต่อไปนี้คือ ภาพรวมของจุดทางออกและขีดความสามารถ. หนังสือ *iSeries System API Reference* อธิบายถึงวิธีใช้จุดทางออกเหล่าน้.

  Port entry

  ระบบจะเรียกโปรแกรมทางออกของคุณ เมื่อระบบได้อ่านแพ็กเก็ตข้อมูล (data packet) จากพอร์ต 67 (พอร์ต DHCP). โปรแกรมทางออกของคุณได้รับแพ็กเก็ตข้อมูลเต็ม . โปรแกรมทางออกสามารถตัดสินใจว่า ระบบควรจะประมวลผลหรือปฏิเสธแพ็กเก็ต. คุณสามารถใช้จุดทางออกนี้ เมื่อคุณสมบัติการกรอง DHCP ที่มีอยู่ไม่เพียงพอต่อความต้องการของคุณ.

  Address assignment

  ระบบจะเรียกโปรแกรมทางออกของคุณเมื่อ DHCP มีการกำหนดแอดเดรสตามรูปแบบไปยังไคลเอ็นต์.

  Address release

  ระบบจะเรียกโปรแกรมทางออกของคุณเมื่อ DHCP ปล่อยแอดเดรสตามรูปแบบ และคืนแอดเดรสกับไปยัง address pool.

ข้อควรพิจารณาด้านความปลอดภัยสำหรับการใช้เซิร์ฟเวอร์ TFTP

Trivial file transfer protocol (TFTP) จะให้การโอนถ่ายไฟล์แบบพื้นฐานโดยไม่มีการพิสูจน์ตัวจริงของผู้ใช้. TFTP ทำงานร่วมกับ Bootstrap Protocol (BOOTP) หรือ Dynamic Host Configuration Protocol (DHCP) อย่างใดอย่างหนึ่ง.

ไคลเอนต์เชื่อมต่อในช่วงเริ่มต้นกับเซิร์ฟเวอร์ BOOTP หรือเซิร์ฟเวอร์ DHCP. เซิร์ฟเวอร์ BOOTP หรือเซิร์ฟเวอร์ DHCP จะตอบกลับด้วย IP แอดเดรสและชื่อของโหลดไฟล์. จากนั้น ไคลเอ็นต์จะเริ่มต้นการร้องขอ TFTP ไปยังเซิร์ฟเวอร์สำหรับโหลดไฟล์. เมื่อไคลเอ็นต์เสร็จสิ้นการดาวน์โหลดโหลดไฟล์แล้ว, ก็จะจบเซสชัน TFTP.

การป้องกันการเข้าถึง TFTP

ถ้าคุณไม่มี thin client ใดๆ ต่ออยู่กับเน็ตเวิร์กของคุณ, คุณอาจจะไม่จำเป็นต้องรันเซิร์ฟเวอร์ TFTP บนระบบของคุณ. เพื่อป้องกันไม่ให้เซิร์ฟเวอร์ TFTP ทำงาน ให้ทำดังนี้:

__ ขั้นตอนที่ 1. เพื่อป้องกันไม่ให้งานของเซิร์ฟเวอร์ TFTP เริ่มต้นโดยอัตโนมัติเมื่อคุณเริ่มต้น TCP/IP, ให้พิมพ์ดังนี้:

```
CHGTFTPA AUTOSTART(*NO)
```

หมายเหตุ:

1. AUTOSTART(*NO) เป็นค่าดีฟอลต์.
2. “การควบคุมที่เซิร์ฟเวอร์ TCP/IP เริ่มการทำงานโดยอัตโนมัติ” ในหน้า 135 มีข้อมูลเพิ่มเติมเกี่ยวกับการควบคุมให้เซิร์ฟเวอร์ TCP/IP เริ่มทำงานโดยอัตโนมัติ.

__ ขั้นตอนที่ 2. เพื่อป้องกันบางคนจากการสัมพันธ์กับแอ็พพลิเคชันผู้ใช้, เช่น ซ็อกเก็ตแอ็พพลิเคชัน, ด้วยพอร์ตที่ระบบโดยปกติ ใช้สำหรับ TFTP, ให้ทำดังนี้:

__ ขั้นตอนที่ a. พิมพ์ GO CFGTCP เพื่อแสดงเมนู Configure TCP/IP.

__ ขั้นตอนที่ b. เลือกอ็อพชัน 4 (Work with TCP/IP port restrictions).

__ ขั้นตอนที่ c. บนหน้าจอ Work with TCP/IP Port Restrictions, ให้ระบุอ็อพชัน 1 (Add).

__ ขั้นตอนที่ d. สำหรับ lower port range, ระบุค่า 69.

__ ขั้นตอนที่ e. สำหรับ upper port range, ระบุค่า *ONLY.

หมายเหตุ:

1. ข้อจำกัดของพอร์ตมีผลครั้งต่อไปที่คุณเริ่มต้น TCP/IP. ถ้า TCP/IP ทำงานอยู่ เมื่อคุณกำหนดข้อจำกัดของพอร์ต, คุณควรจะจบ TCP/IP และเริ่มต้นใหม่อีกครั้ง.
2. RFC1700 มีข้อมูลเกี่ยวกับการกำหนดหมายเลขพอร์ต.

__ ขั้นตอนที่ f. สำหรับ protocol, ระบุค่า *UDP.

__ ขั้นตอนที่ g. สำหรับฟิลด์โปรไฟล์ผู้ใช้, ระบุชื่อโปรไฟล์ผู้ใช้ที่มีการป้องกันในระบบของคุณ. (โปรไฟล์ผู้ใช้ที่มีการป้องกันคือ โปรไฟล์ผู้ใช้ที่ไม่เป็นเจ้าของโปรแกรมที่ได้รับสิทธิมา และไม่มีรหัสผ่านที่ผู้ใช้อื่นทราบ.) โดยการจำกัดพอร์ตให้กับผู้ใช้เฉพาะ, คุณสามารถตัดผู้ใช้อื่นออกไปได้โดยอัตโนมัติ.

การรักษาความปลอดภัยให้กับเซิร์ฟเวอร์ TFTP

โดยดีฟอลต์, เซิร์ฟเวอร์ TFTP จะให้การเข้าถึงที่จำกัดมากไปยังระบบ iSeries ของคุณ. มันจะถูกปรับแต่งค่าเป็นพิเศษเพื่อกำหนดโค้ดเริ่มต้นสำหรับ thin client. ในฐานะของผู้บริหารความปลอดภัย, คุณควรจะต้องตระหนักถึงคุณลักษณะของเซิร์ฟเวอร์ TFTP ต่อไปนี้:

- เซิร์ฟเวอร์ TFTP ไม่ต้องการการพิสูจน์ตัวจริง (user ID และรหัสผ่าน). งาน TFTP ทั้งหมดทำงานภายใต้โปรไฟล์ผู้ใช้ QTFTP. โปรไฟล์ผู้ใช้ QTFTP ไม่มีรหัสผ่าน. ดังนั้น, จึงไม่มีการ sign-

on แบบโต้ตอบ. โปรไฟล์ผู้ใช้ QTFTP ไม่มีสิทธิพิเศษใดๆ , และไม่มีสิทธิที่ชัดแจ้งในรีซอร์สของระบบ. มันใช้สิทธิพับลิกในการเข้าถึงรีซอร์สที่มันต้องการสำหรับ thin client.

- เมื่อเซิร์ฟเวอร์ TFTP มาถึง, มีการปรับแต่งค่าให้เข้าถึงไดเร็กทอรีที่มีข้อมูลของ thin client อยู่. คุณต้องมีสิทธิ *PUBLIC หรือ QTFTP เพื่ออ่านหรือเขียนในไดเร็กทอรีนั้น. เพื่อจะเขียนในไดเร็กทอรี คุณต้องมีค่า *CREATE ระบุในพารามิเตอร์ "Allow file writes" ของคำสั่ง CHGTFTPA. เพื่อที่จะเขียนในไฟล์ที่มีอยู่แล้ว คุณต้องมีค่า *REPLACE ระบุในพารามิเตอร์ "Allow file writes" ของ CHGTFTPA. *CREATE ยอมให้คุณแทนที่ไฟล์เดิมหรือสร้างไฟล์ใหม่. แต่ *REPLACE ยอมให้คุณแทนที่ไฟล์เดิมเท่านั้น.

  ไคลเอ็นต์ TFTP ไม่สามารถเข้าถึงไดเร็กทอรีใด นอกจากคุณจะกำหนดไดเร็กทอรีไว้อย่างชัดเจนด้วยคำสั่ง Change TFTP Attributes (CHGTFTPA). ดังนั้น, ถ้าผู้ใช้โลคัลหรือผู้ใช้รีโมตพยายามที่จะเริ่มต้นเซสชัน TFTP ไปยังระบบของคุณ, , ความสามารถของผู้ใช้ในการเข้าถึงข้อมูลหรือทำให้เสียหายจะถูกจำกัดเป็นอย่างมาก.
- ถ้าคุณเลือกที่จะปรับแต่งค่าของเซิร์ฟเวอร์ TFTP เพื่อให้มีปริการอื่นๆ เพิ่มเติมเพื่อจัดการกับ thin client, คุณสามารถกำหนดโปรแกรมทางออกในการประเมินผล และให้สิทธิแก่ทุกๆ คำร้องขอของ TFTP. เซิร์ฟเวอร์ TFTP ให้ทางออกของการตรวจสอบการร้องขอที่เหมือนกับทางออกที่มีอยู่ในเซิร์ฟเวอร์ FTP. สำหรับข้อมูลเพิ่มเติม, ดูที่ iSeries Information Center—>Networking—>TCP/IP—>TFTP. ดูที่ "สิ่งที่ต้องรู้ก่อนและข้อมูลที่เกี่ยวข้อง" ในหน้า xiii สำหรับข้อมูลที่เกี่ยวกับการเข้าถึง iSeries Information Center.

ข้อควรพิจารณาด้านความปลอดภัยสำหรับการใช้เซิร์ฟเวอร์ REXEC

Remote EXECution server (REXEC) ได้รับและรันคำสั่งจากไคลเอ็นต์ REXEC. ไคลเอ็นต์ REXEC คือเครื่องพีซีธรรมดาหรือแอ็พพลิเคชัน ยูนิกซ์ ที่สนับสนุนการส่งคำสั่ง REXEC. การสนับสนุนที่เซิร์ฟเวอร์นี้มีคล้ายคลึงกับความสามารถที่มีให้เมื่อคุณใช้คำสั่งย่อย RCMD (Remote Command) สำหรับเซิร์ฟเวอร์ FTP.

การป้องกันการเข้าถึง REXEC

ถ้าคุณไม่ต้องการให้เซิร์ฟเวอร์ iSeries ของคุณยอมรับคำสั่งจากไคลเอ็นต์ของ REXEC, ให้ทำดังต่อไปนี้เพื่อป้องกันเซิร์ฟเวอร์ REXEC จากการรัน:

__ ขั้นตอนที่ 1. เพื่อป้องกันไม่ให้งานของเซิร์ฟเวอร์ REXEC เริ่มต้นโดยอัตโนมัติเมื่อคุณเริ่มต้น TCP/IP, ให้พิมพ์ดังนี้:

```
CHGRXCA AUTOSTART(*NO)
```

หมายเหตุ:

1. AUTOSTART(*NO) เป็นค่าดีฟอลต์.
2. "การควบคุมที่เซิร์ฟเวอร์ TCP/IP เริ่มการทำงานโดยอัตโนมัติ" ในหน้า 135 มีข้อมูลเพิ่มเติมเกี่ยวกับการควบคุมให้เซิร์ฟเวอร์ TCP/IP เริ่มทำงานโดยอัตโนมัติ.

__ ขั้นตอนที่ 2. เพื่อป้องกันบางคนจากการสัมพันธ์กับแอ็พพลิเคชันผู้ใช้, เช่น ซ็อกเก็ตแอ็พพลิเคชัน, ด้วยพอร์ตที่ระบบโดยปกติ ใช้สำหรับ REXEC, ให้ทำดังนี้:

__ ขั้นตอนที่ a. พิมพ์ GO CFGTCP เพื่อแสดงเมนู Configure TCP/IP.

__ ขั้นตอนที่ b. เลือกอ็อพชัน 4 (Work with TCP/IP port restrictions).

__ ขั้นตอนที่ c. บนหน้าจอ Work with TCP/IP Port Restrictions, ให้ระบุอ็อพชัน 1 (Add).

__ ขั้นตอนที่ d. สำหรับ lower port range, ระบุค่า 512.

__ ขั้นตอนที่ e. สำหรับ upper port range, ระบุค่า *ONLY.

__ ขั้นตอนที่ f. สำหรับ protocol, ระบุค่า *TCP.

__ ขั้นตอนที่ g. สำหรับฟิลด์โปรไฟล์ผู้ใช้, ระบุชื่อโปรไฟล์ผู้ใช้ที่มีการป้องกันในระบบของคุณ. (โปรไฟล์ผู้ใช้ที่มีการป้องกันคือ โปรไฟล์ผู้ใช้ที่ไม่เป็นเจ้าของโปรแกรมที่ได้รับสิทธิมา และไม่มีรหัสผ่านที่ผู้ใช้อื่นทราบ.) โดยการจำกัดพอร์ตให้กับผู้ใช้เฉพาะ, คุณสามารถตัดผู้ใช้อื่นออกไปได้โดยอัตโนมัติ.

หมายเหตุ:

1. ข้อจำกัดของพอร์ตมีผลครั้งต่อไปที่คุณเริ่มต้น TCP/IP. ถ้า TCP/IP ทำงานอยู่ เมื่อคุณกำหนดข้อจำกัดของพอร์ต, คุณควรจะจบ TCP/IP และเริ่มต้นใหม่อีกครั้ง.
2. RFC1700 มีข้อมูลเกี่ยวกับการกำหนดหมายเลขพอร์ต.

การรักษาความปลอดภัยให้กับเซิร์ฟเวอร์ REXEC

ต่อไปนี้ คือคำสั่งที่ควรพิจารณาเกี่ยวกับความปลอดภัยเมื่อคุณเลือกที่จะรัน Remote EXECution server ในระบบของคุณ:

- คำร้องขอ REXCD ประกอบด้วย user ID, รหัสผ่าน, และคำสั่งเพื่อทำงาน. การพิสูจน์ตัวจริงและการตรวจสอบสิทธิของเซิร์ฟเวอร์ iSeries โดยปกติใช้ได้กับ:
  - ทั้งโปรไฟล์ผู้ใช้และรหัสผ่านต้องถูกต้อง.
  - ระบบบังคับใช้ค่า *Limit capabilities* (LMTCPB) สำหรับโปรไฟล์ผู้ใช้.
  - ผู้ใช้ต้องได้รับอนุญาตในคำสั่งและในรีซอร์สทั้งหมดที่คำสั่งใช้.
- เซิร์ฟเวอร์ REXEC มีจุดทางออกที่คล้ายกับจุดทางออกที่มีไว้สำหรับเซิร์ฟเวอร์ FTP. คุณสามารถใช้จุดทางออก Validation เพื่อประเมินคำสั่งและตัดสินใจว่าจะอนุญาตให้ใช้คำสั่งหรือไม่. สำหรับข้อมูลเพิ่มเติม, โปรดดูที่ iSeries Information Center—>Networking—>TCP/IP—>REXEC. โปรดดูที่ “สิ่งที่ต้องรู้ก่อนและข้อมูลที่เกี่ยวข้อง” ในหน้า xiii สำหรับข้อมูลในการเข้าถึง iSeries Information Center.
- เมื่อคุณเลือกที่จะรันเซิร์ฟเวอร์ REXEC, คุณกำลังทำงานอยู่ภายนอกเมนูแอ็คเซสคอนโทรลใดๆ ที่คุณมีในระบบ. คุณต้องแน่ใจว่าโครงร่างสิทธิอ็อบเจ็กต์ของคุณเพียงพอที่จะป้องกันรีซอร์สของคุณ.

ข้อควรพิจารณาด้านความปลอดภัยสำหรับการใช้ RouteD

เซิร์ฟเวอร์ Route Daemon (RouteD) ให้การสนับสนุนสำหรับ Routing Information Protocol (RIP) บนเซิร์ฟเวอร์ iSeries. RIP routing protocol ที่มีการใช้กันแพร่หลายที่สุด. โดยเป็น Interior Gateway Protocol ที่ช่วย TCP/IP ในการจัดเส้นทางของแพ็กเก็ต IP ภายในระบบที่เป็นอิสระ.

RouteD มีจุดมุ่งหมายในการเพิ่มประสิทธิภาพของ network traffic โดยยอมให้ระบบภายในเครือข่ายที่ไว้ใจได้ปรับปรุงข้อมูลเส้นทางปัจจุบันให้แก่กันและกัน. เมื่อคุณรัน RouteD, ระบบของคุณสามารถได้รับการปรับปรุงจากระบบอื่นที่อยู่ร่วมกัน เกี่ยวกับว่าการส่งผ่าน (แพ็กเก็ต)ควรจะมีเส้นทางอย่างไร. ดังนั้น, ถ้ามีการเข้าถึงเซิร์ฟเวอร์ RouteD ของคุณโดยนักเจาะระบบ, นักเจาะระบบอาจใช้เซิร์ฟเวอร์นั้นเปลี่ยนเส้นทางแพ็กเก็ตของคุณ ผ่านทางระบบที่สามารถดูดข้อมูลหรือดัดแปลงแพ็กเก็ตเหล่านั้น. ต่อไปนี้คือ คำแนะนำสำหรับความปลอดภัยของ RouteD:

- เซิร์ฟเวอร์iSeries ใช้ RIPv1, ที่ไม่มีวิธีการพิสูจน์ค่าจริงของ router. และใช้สำหรับภายในเครือข่ายที่ไว้ใจได้. ถ้าระบบของคุณอยู่ในเครือข่าย ที่มีระบบอื่นที่คุณไม่ ″ไว้ใจ″, คุณจะต้องไม่รันเซิร์ฟเวอร์ RouteD. เพื่อให้แน่ใจว่าเซิร์ฟเวอร์ RouteD จะไม่เริ่มทำงานอย่างอัตโนมัติ, ให้พิมพ์ดังนี้:

  ```
  CHGRTDA AUTOSTART(*NO)
  ```

  หมายเหตุ:

  1. AUTOSTART(*NO) เป็นค่าดีฟอลต์.
  2. “การควบคุมที่เซิร์ฟเวอร์ TCP/IP เริ่มการทำงานโดยอัตโนมัติ” ในหน้า 135 มีข้อมูลเพิ่มเติมเกี่ยวกับการควบคุมให้เซิร์ฟเวอร์ TCP/IP เริ่มทำงานโดยอัตโนมัติ.
- ทำให้แน่ใจว่าคุณควบคุมผู้ที่จะสามารถเปลี่ยนแปลงคอนฟิกูเรชันของ RouteD ได้, ซึ่งต้องการสิทธิพิเศษ *IOSYSCFG.
- ถ้าระบบของคุณมีส่วนร่วมอยู่ในหลายเครือข่าย (ตัวอย่างเช่น, อินทราเน็ตและอินเตอร์เน็ต), คุณสามารถตั้งค่าเซิร์ฟเวอร์ RouteD เพื่อส่งและรับค่าปรับปรุงจากเครือข่ายที่ปลอดภัยเท่านั้น.

ข้อควรพิจารณาด้านความปลอดภัยสำหรับเซิร์ฟเวอร์ DNS

เซิร์ฟเวอร์ Domain Name System (DNS) มีความสามารถในการแปลงชื่อโฮสต์ไปเป็น IP แอดเดรส และในทางกลับกัน. บนเซิร์ฟเวอร์ iSeries นี้, เซิร์ฟเวอร์ DNS มีไว้เพื่อทำการแปลแอดเดรสสำหรับเน็ตเวิร์กที่ปลอดภัย (อินทราเน็ต) ภายใน.

การป้องกันการเข้าถึง DNS

หากคุณ *ไม่* ต้องการให้มีผู้ใดใช้เซิร์ฟเวอร์ DNS ในระบบของคุณ, ให้ทำดังนี้:

1. เพื่อป้องกันไม่ให้งานของเซิร์ฟเวอร์ DNS เริ่มต้นโดยอัตโนมัติเมื่อคุณเริ่มต้น TCP/IP, ให้พิมพ์ดังนี้:

   ```
   CHGDNSA AUTOSTART(*NO)
   ```

   หมายเหตุ:

   1. AUTOSTART(*NO) เป็นค่าดีฟอลต์.

2. “การควบคุมที่เซิร์ฟเวอร์ TCP/IP เริ่มการทำงานโดยอัตโนมัติ” ในหน้า 135 มีข้อมูลเพิ่มเติมเกี่ยวกับการควบคุมให้เซิร์ฟเวอร์ TCP/IP เริ่มทำงานโดยอัตโนมัติ.

2. เพื่อป้องกันบางคนจากการสัมพันธ์กับแอ็พพลิเคชันผู้ใช้, เช่น ซ็อกเก็ตแอ็พพลิเคชัน, ด้วยพอร์ตที่ระบบโดยปกติ ใช้สำหรับ DNS, ให้ทำดังนี้:
   a. พิมพ์ GO CFGTCP เพื่อแสดงเมนู Configure TCP/IP.
   b. เลือกอ็อพชัน 4 (Work with TCP/IP port restrictions).
   c. บนหน้าจอ Work with TCP/IP Port Restrictions, ให้ระบุอ็อพชัน 1 (Add).
   d. สำหรับ lower port range, ระบุค่า 53.
   e. สำหรับ upper port range, ระบุค่า *ONLY.

      หมายเหตุ:

      1. ข้อจำกัดของพอร์ตมีผลครั้งต่อไปที่คุณเริ่มต้น TCP/IP. ถ้า TCP/IP ทำงานอยู่ เมื่อคุณกำหนดข้อจำกัดของพอร์ต, คุณควรจะจบ TCP/IP และเริ่มต้นใหม่อีกครั้ง.
      2. RFC1700 มีข้อมูลเกี่ยวกับการกำหนดหมายเลขพอร์ต.

   f. สำหรับ protocol, ระบุค่า *TCP.
   g. สำหรับฟิลด์โปรไฟล์ผู้ใช้, ระบุชื่อโปรไฟล์ผู้ใช้ที่มีการป้องกันในระบบของคุณ. (โปรไฟล์ผู้ใช้ที่มีการป้องกันคือ โปรไฟล์ผู้ใช้ที่ไม่เป็นเจ้าของโปรแกรมที่ได้รับสิทธิมา และไม่มีรหัสผ่านที่ผู้ใช้อื่นทราบ.) โดยการจำกัดพอร์ตให้กับผู้ใช้เฉพาะ, คุณสามารถตัดผู้ใช้อื่นออกไปได้โดยอัตโนมัติ.
   h. ทำซ้ำในขั้นตอน 2c ถึงขั้นตอน 2g สำหรับโปรโตคอล *UDP (User datagram).

การรักษาความปลอดภัยให้กับเซิร์ฟเวอร์ DNS

ต่อไปนี้ คือสิ่งที่ควรพิจารณาเกี่ยวกับความปลอดภัย เมื่อคุณเลือกที่จะรัน DNS ในระบบ iSeries ของคุณ:

- ฟังก์ชันที่เซิร์ฟเวอร์ DNS ทำคือ การแปลง IP แอดเดรสและการแปลงชื่อ. โดยไม่มีการเข้าถึงอ็อบเจ็กต์ใดๆ ในระบบ iSeries ของคุณ. ความเสี่ยงของคุณเมื่อมีบุคคลภายนอกเข้าถึงเซิร์ฟเวอร์ DNS คือ เซิร์ฟเวอร์จะทำให้เห็นรูปแบบ (topology) ของเครือข่ายของคุณได้โดยง่าย . DNS ของคุณอาจช่วยนักเจาะระบบในการพิจารณาแอดเดรสของเป้าหมายที่เป็นไปได้. อย่างไรก็ตาม, DNS ของคุณไม่ได้ให้ข้อมูลที่จะช่วยให้เข้าไปยังระบบเป้าหมายเหล่านั้น.
- โดยทั่วไป, คุณใช้เซิร์ฟเวอร์ DNS ของ iSeries สำหรับอินทราเน็ตของคุณ. ดังนั้น, คุณอาจไม่จำเป็นต้องจำกัดความสามารถในการสอบถาม DNS. อย่างไรก็ตาม, คุณอาจมีหลายเครือข่ายย่อยภายในอินทราเน็ตของคุณ. คุณอาจจะไม่ต้องการให้ผู้ใช้จากเน็ตเวิร์กย่อยที่ต่างกันสามารถที่จะทำเคียวรี่ DNS บนเซิร์ฟเวอร์ iSeries . อ็อพชันความปลอดภัยของ DNS ให้คุณจำกัดการเข้าถึงไปยังโดเมนหลัก. ใช้ iSeries Navigator ในการระบุ IP address ที่เซิร์ฟเวอร์ DNS server สมควรจะตอบสนอง.

  อ็อพชันความปลอดภัยอื่นให้คุณระบุเซิร์ฟเวอร์รอง (secondary server) ที่สามารถก็อปปีข้อมูลจากเซิร์ฟเวอร์ DNS หลัก (primary DNS server) ของคุณ. เมื่อคุณใช้อ็อพชันนี้, เซิร์ฟเวอร์ของคุณจะรับ zone transfer request (การร้องขอที่จะก็อปปีข้อมูล) จากเซิร์ฟเวอร์รองที่คุณกำหนดรายชื่อไว้เท่านั้น.

- ต้องแน่ใจว่าได้จำกัดความสามารถในการเปลี่ยนแปลงไฟล์คอนฟิกูเรชันสำหรับเซิร์ฟเวอร์ DNS ของคุณอย่างระมัดระวัง. บางคนที่ประสงค์ร้ายอาจทำบางอย่าง, เช่น, เปลี่ยนแปลงไฟล์ DNS ของคุณให้ชี้ไปยัง IP แอดเดรสภายนอกเครือข่ายของคุณ. พวกเขาอาจจำลองเป็นเซิร์ฟเวอร์ในเครือข่ายของคุณ, และบางที, อาจได้เข้าถึงข้อมูลที่เป็นความลับจากผู้ใช้ที่ไปเซิร์ฟเวอร์นั้น.

ข้อควรพิจารณาเกี่ยวกับความปลอดภัยสำหรับการใช้เซิร์ฟเวอร์ HTTP สำหรับ iSeries

เซิร์ฟเวอร์ HTTP ช่วยให้ไคลเอ็นต์ของ World Wide Web browser สามารถเข้าถึงมัลติมีเดียอ็อบเจ็กต์ของเซิร์ฟเวอร์ iSeries , อาทิเช่น เอกสาร HTML (Hypertext Markup Language) . และยังสนับสนุนข้อกำหนดของ *Common Gateway Interface (CGI)*. ทำให้แอ็พพลิเคชันโปรแกรมเมอร์สามารถเขียนโปรแกรม CGI เพื่อขยายการทำงานของเซิร์ฟเวอร์ได้.

administrator สามารถใช้เซิร์ฟเวอร์ Internet Connection Server หรือ HTTP IBM สำหรับ iSeries ในการรันหลายๆ เซิร์ฟเวอร์พร้อมๆ กันบนเซิร์ฟเวอร์ iSeries เดียวกัน. แต่ละเซิร์ฟเวอร์ที่กำลังรันอยู่นั้น เรียกว่า **server instance**. แต่ละ server instance มีชื่อที่ไม่ซ้ำกัน. ผู้บริหารระบบจะควบคุมว่า instance ใดจะเริ่มทำงานและสิ่งใดที่แต่ละ instance จะสามารถทำได้.

หมายเหตุ: คุณต้องมี instance *ADMIN ของเซิร์ฟเวอร์ HTTP รันอยู่ในขณะที่คุณใช้เว็บบราวเซอร์ในการตั้งค่าหรือจัดการสิ่งต่างๆ ต่อไปนี้:

- ไฟร์วอลล์สำหรับ iSeries
- Internet Connection Server
- Internet Connection Secure Server
- IBM HTTP Server for iSeries

ผู้ใช้ (ผู้เยี่ยมชมเว็บไซต์) จะมองไม่เห็นหน้าจอ Sign On ของเซิร์ฟเวอร์ iSeries . อย่างไรก็ตาม, ผู้บริหารเซิร์ฟเวอร์ iSeries ต้องทำการให้สิทธิแก่เอกสาร HTML และโปรแกรม CGI ทั้งหมดอย่างชัดเจนโดยการกำหนดไว้ใน HTTP directives. นอกจากนี้, ผู้บริหารระบบสามารถจัดเตรียมทั้งความปลอดภัยของรีซอร์ส และการพิสูจน์ตัวจริงผู้ใช้ (user ID และรหัสผ่าน) สำหรับการร้องขอบางส่วนหรือทั้งหมดได้.

การโจมตีโดยนักเจาะระบบอาจส่งผลให้เกิดการปฏิเสธการให้บริการ(denial of service) กับเว็บเซิร์ฟเวอร์ของคุณ. เซิร์ฟเวอร์ของคุณสามารถตรวจจับการโจมตีแบบ denial-of-service โดยการวัดเวลา time-out ของการร้องขอของบางไคลเอ็นต์. ถ้าเซิร์ฟเวอร์ไม่รับการร้องขอจากไคลเอ็นต์, เซิร์ฟเวอร์ของคุณอาจพิจารณาได้ว่าการโจมตีแบบ denial-of-service กำลังดำเนินอยู่. ซึ่งเกิดขึ้นหลังจากทำการติดต่อเริ่มต้นของไคลเอ็นต์ไปยังเซิร์ฟเวอร์ของคุณ. โดยปกติเซิร์ฟเวอร์จะทำการตรวจจับการโจมตีและทำการลงโทษ.

การป้องกันการเข้าถึง HTTP

หากคุณ *ไม่* ต้องการให้ทุกคนใช้โปรแกรมเพื่อเข้าถึงระบบของคุณ, คุณควรจะป้องกันไม่ให้เซิร์ฟเวอร์ HTTP ทำงาน. โดยทำดังนี้:

__ ขั้นตอนที่ 1. เพื่อป้องกันไม่ให้งานของเซิร์ฟเวอร์ HTTP เริ่มต้นโดยอัตโนมัติเมื่อคุณเริ่มต้น TCP/IP, ให้พิมพ์ดังนี้:

```
CHGHTTPA AUTOSTART(*NO)
```

หมายเหตุ:

1. AUTOSTART(*NO) เป็นค่าดีฟอลต์.
2. "การควบคุมที่เซิร์ฟเวอร์ TCP/IP เริ่มการทำงานโดยอัตโนมัติ" ในหน้า 135 มีข้อมูลเพิ่มเติมเกี่ยวกับการควบคุมให้เซิร์ฟเวอร์ TCP/IP เริ่มทำงานโดยอัตโนมัติ.

__ ขั้นตอนที่ 2. โดยดีฟอลต์, งานของเซิร์ฟเวอร์ HTTP จะใช้โปรไฟล์ผู้ใช้ QTMHHTTP. เพื่อป้องกันไม่ให้เซิร์ฟเวอร์ HTTP เริ่มทำงาน, ให้กำหนดค่าสถานะของโปรไฟล์ผู้ใช้ QTMHHTTP เป็น *DISABLED.

การควบคุมการเข้าถึงเซิร์ฟเวอร์ HTTP

จุดประสงค์หลักของการใช้งานเซิร์ฟเวอร์ HTTP คือการให้การเข้าถึงสำหรับผู้เข้าเยี่ยมชมไปยังเว็บไซต์บนระบบ iSeries ของคุณ. คุณอาจคิดถึงคนที่เข้าเยี่ยมชมเว็บไซต์ของคุณ ว่าเหมือนกับคนที่ดูโฆษณาในวารสารทางการค้า. ผู้เข้าเยี่ยมชมไม่ทราบถึงฮาร์ดแวร์และซอฟต์แวร์ที่ทำงานอยู่บนเว็บไซต์ของคุณ, เช่น ประเภทของเซิร์ฟเวอร์ที่คุณกำลังใช้, และตำแหน่งทางกายภาพที่เซิร์ฟเวอร์ของคุณอยู่. โดยปกติ, คุณไม่ต้องการวางเครื่องขวางกั้นใดๆ (เช่น จอภาพ Sign On) ระหว่างผู้เข้าเยี่ยมชมกับเว็บไซต์ของคุณ. อย่างไรก็ตาม, คุณอาจต้องการจำกัดการเข้าถึง ไปยังบางเอกสารหรือโปรแกรม CGI ที่เว็บไซต์ของคุณมี.

คุณอาจต้องการมีระบบ iSeries เดียวที่มีลอจิคัลเว็บไซต์หลายเว็บไซต์. ตัวอย่างเช่น, ระบบ iSeries ของคุณอาจ สนับสนุนหลายๆ สาขาของธุรกิจของคุณที่มีลูกค้าที่ต่างประเภทกัน. สำหรับแต่ละสาขาของธุรกิจเหล่านี้, คุณต้องการเว็บไซต์ที่ต่างกันที่เป็นอิสระต่อกัน เมื่อปรากฏกับผู้เข้ามาเยี่ยมชมเว็บไซต์. มากไปกว่านั้น, คุณอาจต้องการมีเว็บไซต์ภายใน (อินทราเน็ต) ที่มีข้อมูลที่เป็นความลับของธุรกิจของคุณ.

ในฐานะของผู้บริหารความปลอดภัย, คุณจำเป็นต้องป้องกันเนื้อหาของเว็บไซต์ของคุณ, ในขณะเดียวกัน, คุณก็จำเป็นที่จะต้องแน่ใจว่าวิธีปฏิบัติด้านความปลอดภัยของคุณ ไม่มีผลในทางลบกับเว็บไซต์ของคุณ. นอกเหนือจากนี้, คุณจำเป็นต้องแน่ใจว่ากิจกรรมของ HTTP ไม่เป็นอันตรายต่อความมั่นคงของระบบของคุณหรือเครือข่ายของคุณ. หัวข้อต่อไปจะให้ข้อเสนอแนะด้านความปลอดภัยเมื่อคุณใช้โปรแกรม.

ข้อควรพิจารณาในการบริหารระบบ

สิ่งที่ควรพิจารณาบางประการเกี่ยวกับความปลอดภัยสำหรับการบริหารอินเตอร์เน็ตเซิร์ฟเวอร์ของคุณ มีดังนี้.

- คุณทำการจัดเตรียมและการตั้งค่า โดยการใช้เว็บบราวเซอร์และ *ADMIN instance. สำหรับบางฟังก์ชัน, เช่น การสร้าง instance เพิ่มเติมบนเซิร์ฟเวอร์, คุณต้องใช้เซิร์ฟเวอร์ *ADMIN.
- URL ดีฟอลต์สำหรับการบริหารโฮมเพจ (โฮมเพจสำหรับเซิร์ฟเวอร์ *ADMIN) ถูกจัดพิมพ์อยู่ในคู่มือ สำหรับผลิตภัณฑ์ที่ให้ฟังก์ชันการบริหารทางบราวเซอร์. ดังนั้น, นักเจาะระบบอาจจะทราบค่าดีฟอลต์ของ URL และเผยแพร่ในฟอรัมของนักเจาะระบบ, เช่นเดียวกับค่าดีฟอลต์รหัสผ่าน สำหรับโปรไฟล์ผู้ใช้ที่ IBM จัดหาให้ ที่เป็นที่รู้จักและมีการตีพิมพ์. คุณสามารถป้องกันตัวคุณเองจากจุดอ่อนนี้ในหลายๆ ทาง:
  - ให้ *ADMIN instance ของเซิร์ฟเวอร์ HTTP ทำงานเฉพาะเมื่อคุณต้องการทำฟังก์ชันการบริหาร. อย่าให้ *ADMIN instance ทำงานอยู่ตลอดเวลา.
  - เรียกใช้ SSL ให้สนับสนุน *ADMIN instance (โดยการใช้ Digital Certificate Manager). *ADMIN instance ใช้ HTTP protection directive เพื่อร้องขอ user ID และรหัสผ่าน. เมื่อคุณใช้ SSL, user ID และรหัสผ่านของคุณจะถูกเข้ารหัส (พร้อมๆ กับข้อมูลอื่น ที่เกี่ยวกับคอนฟิกูเรชันของคุณที่ปรากฏอยู่บนฟอร์มการบริหาร).
  - ใช้ไฟร์วอลล์เพื่อป้องกันการเข้าถึงเซิร์ฟเวอร์ *ADMIN จากอินเตอร์เน็ต และเพื่อปิดบังชื่อระบบและชื่อโดเมนของคุณ, ซึ่งเป็นส่วนหนึ่งของ URL.
- เมื่อคุณทำฟังก์ชันการบริหาร, คุณต้อง sign on ด้วยโปรไฟล์ผู้ใช้ที่มีสิทธิพิเศษ *IOSYSCFG. คุณอาจต้องการสิทธิในบางอ็อบเจ็กต์ในระบบด้วย, ได้แก่:
  - ไลบรารีหรือไดเร็กทอรีที่มีเอกสาร HTML และโปรแกรม CGI ของคุณ.
  - โปรไฟล์ผู้ใช้ใดๆ ที่คุณวางแผนที่จะสลับกันภายในไดเร็กทีฟสำหรับเซิร์ฟเวอร์.
  - Access Control Lists (ACLs) สำหรับไดเร็กทอรีใดๆ ที่ไดเร็กทีฟของคุณใช้งาน.
  - อ็อบเจ็กต์รายการการตรวจสอบสำหรับการสร้างและดูแล user ID และรหัสผ่าน.

  ด้วยเซิร์ฟเวอร์ *ADMIN และ TELNET, คุณมีความสามารถที่จะทำฟังก์ชันการบริหารจากระยะไกล, หรืออาจผ่านการติดต่อแบบอินเตอร์เน็ต. ให้ระวังว่าถ้าคุณทำการบริหารอยู่บนการเชื่อมโยงแบบสาธารณะ (อินเตอร์เน็ต), คุณอาจเปิดเผย user ID และรหัสผ่านที่สำคัญจากการถูกดูดข้อมูล. "ผู้ดูดข้อมูล (sniffer)" สามารถใช้ user ID และรหัสผ่านนี้ในการพยายามเข้าถึงระบบของคุณโดยใช้ TELNET หรือ FTP.

  หมายเหตุ:

  1. ใน TELNET, หน้าจอ Sign On จะถูกปฏิบัติเหมือนกับจอภาพอื่นๆ . แม้ว่าจะไม่มีการแสดงรหัสผ่านในขณะที่คุณพิมพ์, แต่ระบบจะส่งรหัสผ่านนั้นโดยไม่มีการเข้ารหัส (encryption) หรือแปลงรหัส (encoding).
  2. ในเซิร์ฟเวอร์ *ADMIN, มีการแปลงรหัสแต่ไม่ได้เข้ารหัส. โครงร่างในการแปลงรหัสเป็นมาตรฐานอุตสาหกรรม, และเป็นที่รู้จักกันทั่วไปในหมู่นักเจาะระบบ. ถึงแม้ว่าการแปลงรหัสจะไม่ได้เข้าใจได้ง่ายโดย "ผู้ดูดข้อมูล" ทั่วไป, แต่ผู้ดูดข้อมูลที่ฉลาดอาจมีเครื่องมือที่จะแปลงรหัสผ่าน.

ข้อแนะนำด้านความปลอดภัย

ถ้าคุณวางแผนที่จะทำการบริหารจากระยะไกลผ่านทางอินเตอร์เน็ต, คุณควรจะใช้ *ADMIN instance กับ SSL, เพื่อที่การส่งผ่านข้อมูลของคุณจะถูกเข้ารหัส. ไม่ควรใช้แอ็พพลิเคชันที่ไม่มีการทำให้ปลอดภัย, เช่น TELNET ก่อนเวอร์ชัน V4R4 (TELNET ที่สนับสนุน SSL เริ่มต้นใน V4R4). ถ้าคุณใช้เซิร์ฟเวอร์ *ADMIN ผ่านอินทราเน็ตของผู้ใช้ที่ *เชื่อถือได้*, คุณสามารถใช้เซิร์ฟเวอร์ *ADMIN เพื่อทำการบริหารได้อย่างปลอดภัย.

- HTTP directive เป็นรากฐานสำหรับทุกกิจกรรมบนเซิร์ฟเวอร์ของคุณ. คอนฟิกูเรชันที่มาพร้อมกับเครื่องมีความสามารถในการให้บริการดีฟอลต์ Welcome page. ไคลเอ็นต์ไม่สามารถดูเอกสารใดๆ นอกจาก Welcome page จนกว่าผู้บริหารเซิร์ฟเวอร์กำหนดไดเร็กทีฟสำหรับเซิร์ฟเวอร์. ในการกำหนดไดเร็กทีฟ, ให้ใช้เว็บบราวเซอร์และเซิร์ฟเวอร์ *ADMIN หรือคำสั่ง Work with HTTP Configuration (WRKHTTPCFG). ทั้งสองวิธีต้องการสิทธิพิเศษ *IOSYSCFG. เมื่อคุณเชื่อมต่อเซิร์ฟเวอร์ iSeries ของคุณเข้ากับอินเตอร์เน็ต, จะเป็นสิ่งที่ต้องใช้ความระมัดระวังมากขึ้นในการประเมินผลและควบคุมจำนวนของผู้ใช้ในองค์กรของคุณที่มีสิทธิพิเศษ *IOSYSCFG.

การปกป้องรีซอร์ส

เซิร์ฟเวอร์ HTTP IBM สำหรับ iSeries จะรวมเอา HTTP directive ที่สามารถให้การควบคุมที่ลงลึกในส่วนของข้อมูลทรัพย์สินที่เซิร์ฟเวอร์ใช้. คุณสามารถใช้ directive ในการควบคุมจากไดเร็กทอรีที่เว็บเซิร์ฟเวอร์ให้บริการ URL สำหรับทั้งไฟล์ HTML และโปรแกรม CGI, ในการสลับไปยังโปรไฟล์ผู้ใช้อื่นๆ , และในการร้องขอการพิสูจน์ตัวจริงจากบางรีซอร์ส.

หมายเหตุ: เอกสารคู่มือในหัวข้อ "Web serving" ที่อยู่ใน Information Center มีรายละเอียดที่สมบูรณ์ของ HTTP directive ที่มีอยู่และวิธีการใช้. ต่อไปนี้เป็นข้อเสนอแนะและข้อควรพิจารณาบางประการ ในการใช้การสนับสนุนนี้:

- เซิร์ฟเวอร์ HTTP เริ่มต้นจากพื้นฐานของ "สิทธิโดยชัดแจ้ง (explicit authority)". เซิร์ฟเวอร์จะไม่รับการร้องขอจนกว่า การร้องขอถูกกำหนดโดยชัดแจ้งในไดเร็กทีฟ. หรืออีกนัยหนึ่ง, เซิร์ฟเวอร์จะปฏิเสธการร้องขอ URL โดยทันทีถ้า URL นั้นไม่ได้ถูกกำหนดในไดเร็กทีฟ (ทั้งโดยชื่อหรือแบบทั่วๆไป).
- คุณสามารถใช้ protection directive เพื่อขอ user ID และรหัสผ่าน ก่อนจะรับการร้องขอรีซอร์สของคุณบางส่วนหรือทั้งหมด.
  - เมื่อผู้ใช้ (ไคลเอ็นต์) ร้องขอรีซอร์สที่ป้องกันไว้, เซิร์ฟเวอร์จะให้บราวเซอร์ถาม user ID และรหัสผ่าน. บราวเซอร์จะให้ผู้ใช้ป้อน user ID และรหัสผ่าน, จากนั้นจะส่งข้อมูลไปยังเซิร์ฟเวอร์. บางบราวเซอร์จะเก็บ user ID และรหัสผ่าน และส่งข้อมูลเหล่านี้โดยอัตโนมัติเมื่อมีการร้องขอภายหลัง. ซึ่งจะช่วยให้ผู้ใช้ ไม่ต้องป้อน user ID และรหัสผ่านซ้ำๆ กันสำหรับแต่ละการร้องขอ.

เนื่องจากบางบราวเซอร์บันทึก user ID และรหัสผ่าน, คุณมีหน้าที่ให้ความรู้แก่ผู้ใช้เช่นเดียวกับที่มีเมื่อผู้ใช้เข้ามาในระบบผ่านทางหน้าจอ Sign On ของเซิร์ฟเวอร์ iSeries หรือผ่านทาง router. เซสชันบราวเซอร์ที่ไม่มีการดูแล แสดงถึงแนวโน้มที่จะเกิดจุดอ่อนด้านความปลอดภัย.

- คุณมีสามทางเลือกสำหรับวิธีการที่ระบบจัดการกับ user IDs และรหัสผ่าน (กำหนดไว้ใน protection directive):

  1. คุณสามารถใช้โปรไฟล์ผู้ใช้ และ การตรวจสอบรหัสผ่านของเซิร์ฟเวอรี iSeries โดยปกติ. ซึ่งใช้กันเป็นส่วนใหญ่ เพื่อป้องกันรีซอร์สในอินทราเน็ต (เครือข่ายที่ปลอดภัย).
  2. คุณสามารถสร้าง "Internet users": คือผู้ใช้ที่สามารถตรวจสอบได้แต่ไม่มีโปรไฟล์ผู้ใช้อยู่บนเซิร์ฟเวอร์ iSeries . Internet user ถูกนำมาใช้ผ่านทางอ็อบเจ็กต์ของเซิร์ฟเวอร์ iSeries ที่เรียกว่า "validation list" . อ็อบเจ็กต์ validation list มีรายชื่อของผู้ใช้และรหัสผ่าน ที่มีการกำหนดโดยเฉพาะสำหรับใช้กับแอ็พพลิเคชันหนึ่งโดยเฉพาะ.

     คุณตัดสินว่าวิธีใดที่จะได้มาซึ่ง user ID และรหัสผ่านของ Internet users (เช่น โดยแอ็พพลิเคชัน, หรือโดยผู้บริหารที่ตอบสนองการร้องขอทางอีเมล์), เช่นเดียวกับวิธีการจัดการ Internet users. ใช้อินเตอร์เฟสแบบบราวเซอร์กับเซิร์ฟเวอร์ HTTP เพื่อจัดเตรียมสิ่งนี้.

     สำหรับเน็ตเวิร์กที่ไม่มีความปลอดภัย (อินเตอร์เน็ต), การใช้ Internet user ทำให้มีการปกป้องโดยรวมที่ดีกว่าการใช้โปรไฟล์ผู้ใช้และรหัสผ่านโดยปกติ . ชุดที่ไม่ซ้ำกันของ user ID และรหัสผ่านจะสร้างข้อจำกัดภายใน กับสิ่งที่ผู้ใช้สามารถกระทำได้. user ID และรหัสผ่านไม่ได้มีไว้สำหรับการ sign-on ปกติ (เช่น ด้วย TELNET หรือ FTP). นอกจากนี้, คุณจะไม่มีการเปิดเผย user ID และรหัสผ่านปกติให้กับการดูดข้อมูล.
  3. Lightweight directory access protocol (LDAP) คือ ไดเร็กทอรีเซอร์วิสโปรโตคอลที่ให้การเข้าถึงไดเร็กทอรีโดยผ่าน Transmission Control Protocol (TCP). ซึ่งจะให้คุณเก็บข้อมูลไว้ในไดเร็กทอรีเซอร์วิสนั้นและให้คุณสอบถามได้. ปัจจุบัน LDAP ได้รับการสนับสนุนให้เป็นทางเลือกหนึ่งสำหรับการพิสูจน์ผู้ใช้ (user authentication).

  หมายเหตุ:

  1. เมื่อบราวเซอร์ส่ง user ID และรหัสผ่าน (ไม่ว่าจะเป็นสำหรับโปรไฟล์ผู้ใช้หรือ Internet user), พวกมันจะถูกแปลงรหัส, ไม่ใช่เข้ารหัส. โครงร่างในการแปลงรหัสเป็นมาตรฐานอุตสาหกรรม, และเป็นที่รู้จักกันทั่วไปในหมู่นักเจาะระบบ. ถึงแม้ว่าการแปลงรหัสจะไม่ได้เข้าใจได้ง่ายโดย "ผู้ดูดข้อมูล" ทั่วไป, แต่ผู้ดูดข้อมูลที่ฉลาดอาจมีเครื่องมือที่จะแปลงข้อมูลเหล่านั้น.
  2. เซิร์ฟเวอร์ iSeries บันทึกอ็อบเจ็กต์ที่ผ่านการตรวจสอบในพื้นที่ของระบบที่ได้รับการปกป้อง. คุณสามารถเข้าถึงได้ด้วยอินเตอร์เฟสที่ระบบกำหนดให้ (APIs) และสิทธิที่เหมาะสมเท่านั้น.

- คุณสามารถใช้ Digital Certificate Manager (DCM) ในการสร้าง Certificate Authority ในอินทราเน็ตของคุณเอง. Digital Certificate จะเกี่ยวโยงโดยอัตโนมัติกับ certificate ที่มีโปรไฟล์ผู้ใช้ของเจ้าของ. certificate มีการให้สิทธิและการอนุญาต ที่เหมือนกันกับโปรไฟล์ที่สัมพันธ์กัน.

• เมื่อเซิร์ฟเวอร์ยอมรับคำร้องขอ, ความปลอดภัยของรีซอร์สของเซิร์ฟเวอร์ iSeries จะทำหน้าที่แทน. โปรไฟล์ผู้ใช้ที่ร้องขอรีซอร์สต้องมีสิทธิในการใช้งานรีซอร์ส (อาทิ เช่น โฟลเดอร์หรือ ไฟล์

ฯที่เป็นซอร์สที่มีเอกสาร HTML). โดยดีฟอลต์, งานจะรันภายใต้โปรไฟล์ผู้ใช้ QTMHHTTP. คุณสามารถใช้ directive ในการสลับค่าไปยังโปรไฟล์ผู้ใช้ที่ต่างกัน. จากนั้นระบบจะใช้สิทธิของโปรไฟล์ผู้ใช้นั้น ในการเข้าถึงอ็อบเจ็กต์. ต่อไปนี้คือข้อควรพิจารณาบางประการ ในการใช้การสนับสนุนนี้:

- การสลับโปรไฟล์ผู้ใช้มีประโยชน์เป็นพิเศษ เมื่อเซิร์ฟเวอร์ของคุณมีลอจิคัลเว็บไซต์มากกว่าหนึ่งเว็บไซต์. คุณสามารถเชื่อมโยงกับโปรไฟล์ผู้ใช้ที่ต่างกันด้วย directive สำหรับแต่ละเว็บไซต์, และดังนั้นจะใช้ความปลอดภัยของรีซอร์สของเซิร์ฟเวอร์ iSeries โดยปกติในการปกป้องเอกสารสำหรับแต่ละไซต์.
- คุณสามารถใช้ความสามารถในการสลับโปรไฟล์ผู้ใช้ร่วมกันกับการตรวจสอบอ็อบเจ็กต์เซิร์ฟเวอร์ใช้ user ID และรหัสผ่านที่เป็นเอกลักษณ์ (แยกออกจาก user ID และรหัสผ่านปกติของคุณ) ในการประเมินผลคำร้องขอในตอนแรก. หลังจากที่เซิร์ฟเวอร์ได้ทำการพิสูจน์ตัวจริงของผู้ใช้, ระบบจะทำการสลับค่าไปเป็นโปรไฟล์ผู้ใช้ที่ต่างกัน และใช้ความได้เปรียบของความปลอดภัยของรีซอร์ส. ผู้ใช้จะไม่ทราบถึงชื่อโปรไฟล์ผู้ใช้จริงและไม่สามารถที่จะใช้มันในแบบอื่นๆ (เช่น FTP).

- บางการร้องขอของเซิร์ฟเวอร์ HTTP ต้องการที่จะรันโปรแกรมในเซิร์ฟเวอร์ HTTP. ตัวอย่าง เช่น, โปรแกรมที่อาจเข้าถึงข้อมูลในระบบของคุณ. ก่อนที่โปรแกรมจะสามารถทำงานได้, ผู้บริหารเซิร์ฟเวอร์ต้องแม็พการร้องขอ (URL) ไปยังโปรแกรมเฉพาะที่ผู้ใช้กำหนด ซึ่งสอดคล้องกับมาตรฐานส่วนการติดต่อกับผู้ใช้ของ CGI. ต่อไปนี้คือข้อควรพิจารณาบางประการ สำหรับโปรแกรม CGI:
  - คุณสามารถใช้ protection directive สำหรับโปรแกรม CGI เหมือนกับที่คุณทำกับเอกสาร HTML. ดังนั้น, คุณสามารถให้มีการป้อน user ID และรหัสผ่านก่อนที่จะรันโปรแกรม.
  - โดยดีฟอลต์, โปรแกรม CGI ทำงานอยู่ภายใต้โปรไฟล์ผู้ใช้ QTMHHTP1. คุณสามารถสลับค่าไปเป็นโปรไฟล์ผู้ใช้ที่ต่างกันก่อนการรันโปรแกรม. ดังนั้น, คุณสามารถตั้งค่าปกติของความปลอดภัยของรีซอร์สของเซิร์ฟเวอร์ iSeries สำหรับรีซอร์สที่โปรแกรม CGI ของคุณมีการเข้าถึง.
  - ในฐานะผู้บริหารความปลอดภัย, คุณควรจะทำการพิจารณาความปลอดภัย ก่อนที่อนุญาตให้ใช้โปรแกรม CGI ใดๆ ในระบบของคุณ. คุณควรทราบที่มาของโปรแกรม และฟังก์ชันที่โปรแกรม CGI นั้นทำ. คุณควรจะเฝ้าสังเกตความสามารถของโปรไฟล์ผู้ใช้ที่คุณใช้ในการรันโปรแกรม CGI นั้นด้วย. คุณควรจะทำการทดสอบกับโปรแกรม CGI เพื่อพิจารณาในบางเรื่อง, ยกตัวอย่างเช่น, คุณสามารถเข้าถึงบรรทัดรับคำสั่งได้หรือไม่. ปฏิบัติต่อโปรแกรม CGI ด้วยความระมัดระวัง เช่นเดียวกับที่คุณปฏิบัติกับโปรแกรมที่ได้รับสิทธิมา.
  - นอกจากนี้, ให้แน่ใจว่าได้ประเมินจุดอ่อนใดๆ ที่อาจมีเมื่ออ็อบเจ็กต์มีสิทธิพับลิกที่ไม่เหมาะสม. โปรแกรม CGI ที่ออกแบบมาไม่ดี, ในบางกรณี, อาจอนุญาตให้ผู้ใช้ที่มีความรู้, แต่ประสงค์ไม่ดีเข้ามาดูข้อมูลในระบบของคุณ .
  - ใช้ไลบรารีผู้ใช้เฉพาะ, เช่น CGILIB, เพื่อเก็บโปรแกรม CGI ทั้งหมดของคุณ. ใช้สิทธิ์อ็อบเจ็กต์ควบคุมทั้งผู้ที่สามารถใส่อ็อบเจ็กต์ในไลบรารีนี้ และผู้ที่สามารถรันโปรแกรมในไลบรารีนี้. ใช้ไดเร็กทีฟเพื่อจำกัดเซิร์ฟเวอร์ HTTP ให้รันโปรแกรม CGI ที่อยู่ในไลบรารีนี้.

    หมายเหตุ: ถ้าเซิร์ฟเวอร์ของคุณมีหลายลอจิคัลเว็บไซต์, คุณอาจต้องการจัดเตรียมไลบรารีที่แยกจากกัน สำหรับโปรแกรม CGI ของแต่ละไซต์.

ข้อควรพิจารณาด้านความปลอดภัยอื่นๆ

สิ่งที่ควรพิจารณาเพิ่มเติมเกี่ยวกับความปลอดภัย มีดังนี้:

- HTTP ให้การเข้าถึงแบบ read-only ไปยังระบบ iSeries ของคุณ. การร้องขอของเซิร์ฟเวอร์ HTTP ไม่สามารถอัพเดตหรือลบข้อมูลในระบบของคุณได้โดยตรง. อย่างไรก็ตาม, คุณอาจมีโปรแกรม CGI ที่อัพเดตข้อมูล. นอกจากนี้, คุณสามารถทำให้ Net.Data® โปรแกรม CGI ให้เข้าไปใช้ฐานข้อมูลของเซิร์ฟเวอร์ iSeries ของคุณได้. ระบบใช้สคริปต์ (ซึ่งเหมือนกับโปรแกรมทางออก) เพื่อประเมินการร้องขอไปยังโปรแกรม Net.Data. ดังนั้น, ผู้บริหารระบบสามารถควบคุมสิ่งที่โปรแกรม Net.Data สามารถทำได้.
- เซิร์ฟเวอร์ HTTP มีบันทึกการเข้าถึง (access log) ที่คุณสามารถใช้ในการเฝ้าสังเกต ทั้งการเข้าถึงและความพยายามที่จะเข้าถึงเซิร์ฟเวอร์.

ข้อควรพิจารณาด้านความปลอดภัยสำหรับการใช้ SSL กับเซิร์ฟเวอร์ HTTP IBM สำหรับ iSeries

IBM เซิร์ฟเวอร์ HTTP สำหรับ iSeries สามารถให้การเชื่อมต่อกับเว็บที่ปลอดภัยไปยังเซิร์ฟเวอร์ iSeries ของ. **เว็บไซต์ที่ปลอดภัย** หมายถึงการส่งผ่านระหว่างไคลเอ็นต์กับเซิร์ฟเวอร์ (ในทิศทางทั้งสอง) ถูกเข้ารหัส. การส่งข้อมูลที่เข้ารหัสจะปลอดภัยจากการพิจารณาอย่างละเอียดของนักดูดข้อมูล และจากผู้ที่พยายามจะดักจับหรือเปลี่ยนแปลงการส่งข้อมูล.

หมายเหตุ: โปรดจำไว้ว่าเว็บไซต์ที่ปลอดภัย ความปลอดภัยของข้อมูลที่ผ่านไปมาระหว่างไคลเอ็นต์และเซิร์ฟเวอร์. จุดประสงค์นี้ไม่ใช่การลดความไม่ปลอดภัยของเซิร์ฟเวอร์ของคุณต่อนักเจาะระบบ. อย่างไรก็ตาม, จะเป็นการช่วยจำกัดข้อมูลที่นักเจาะระบบสามารถได้ไปโดยง่ายผ่านการดูดข้อมูล.

หัวข้อเกี่ยวกับ SSL และ Webserving (HTTP) ใน information center มีข้อมูลที่สมบูรณ์สำหรับการติดตั้ง, การตั้งค่า, และการจัดการกระบวนการเข้ารหัส. หัวข้อเหล่านี้ให้ทั้งภาพรวมของคุณสมบัติของเซิร์ฟเวอร์ และข้อควรพิจารณาในการใช้เซิร์ฟเวอร์.

Internet Connection Server มีการสนับสนุน HTTP และ HTTPS เมื่อโปรแกรมหนึ่งของไลเซนส์โปรแกรมต่อไปนี้ถูกติดตั้ง:

- 5722-NC1
- 5722-NCE

เมื่อมีการติดตั้งอ็อพชันเหล่านี้, ผลิตภัณฑ์จะถูกเรียกว่า Internet Connection Secure Server.

เซิ์ฟเวอร์ HTTP IBM สำหรับ iSeries (5722-DG1) ให้การสนับสนุนทั้ง http และ https. คุณต้องติดตั้งผลิตภัณฑ์ในการเข้ารหัสข้อมูลผลิตภัณฑ์ใดผลิตภัณฑ์หนึ่งต่อไปนี้ เพื่อให้ SSL ทำงาน:

- 5722-AC2
- 5722-AC3

ความปลอดภัยที่ขึ้นกับการเข้ารหัส มีความต้องการในหลายสิ่ง ได้แก่:

- ทั้งผู้ส่งและผู้รับ (เซิร์ฟเวอร์และไคลเอ็นต์) ต้อง "เข้าใจ" กลไกการเข้ารหัส และสามารถทำการเข้ารหัส (encryption) และการถอดรหัส (decryption) ได้. เซิร์ฟเวอร์ HTTP ต้องการไคลเอ็นต์แบบ SSL-enabled. (เว็บบราวเซอร์ที่เป็นที่นิยมส่วนใหญ่เป็นแบบ SSL-enabled.) ไลเซนส์โปรแกรมการเข้ารหัสของ iSeries สนับสนุนการเข้ารหัสตามมาตรฐานอุตสาหกรรมหลายวิธี. เมื่อไคลเอ็นต์พยายามเริ่มต้นเซสชันที่ปลอดภัย, เซิร์ฟเวอร์และไคลเอ็นต์จะสนทนากัน เพื่อหาวิธีการเข้ารหัสที่ปลอดภัยที่สุดที่ทั้งสองฝ่ายให้การสนับสนุน.
- การส่งข้อมูลต้องไม่สามารถถอดรหัสได้โดยผู้ลอบฟัง. ดังนั้น, วิธีการเข้ารหัส ต้องให้ทั้งสองฝ่ายมี **กุญแจส่วนตัว (private key)** สำหรับการเข้ารหัส/การถอดรหัส ที่เป็นที่ทราบเฉพาะพวกเขา. ถ้าคุณต้องการมีเว็บไซต์*ภายนอก*ที่ปลอดภัย, คุณควรจะใช้ certificate authority (CA) อิสระเพื่อสร้างและออก digital certificate ให้กับผู้ใช้และเซิร์ฟเวอร์. certificate authority เป็นที่รู้จักกันในนาม trusted party.

การเข้ารหัสป้องกันความลับของข้อมูลที่ส่งผ่าน. อย่างไรก็ตาม, สำหรับข้อมูลที่เป็นความลับพิเศษ, เช่น ข้อมูลทางการเงิน, คุณต้องการความมั่นคงและการรับรองเพิ่มเติมให้กับข้อมูลที่เป็นความลับ. หรืออีกนัยหนึ่ง, ไคลเอ็นต์และเซิร์ฟเวอร์ (ตัวเลือก) ต้องเชื่อใจผู้ที่อยู่ในอีกฝั่งหนึ่ง (ผ่านทางการอ้างอิงที่เป็นอิสระ) และพวกเขาต้องแน่ใจว่าการส่งผ่านไม่ได้ถูกเปลี่ยนแปลง. ลายเซ็นดิจิตอล (digital signature) ที่ทำโดย certification authority (CA) เป็นการให้ความมั่นใจในความถูกต้องและสมบูรณ์. โปรโตคอล SSL ให้การพิสูจน์ตัวจริง โดยการตรวจสอบลายเซ็นดิจิตอลใน certificate ของเซิร์ฟเวอร์ (และอาจตรวจสอบใน certificate ของไคลเอ็นต์ด้วย).

การเข้ารหัสและการถอดรหัสต้องการเวลาในการประมวลผล และจะมีผลต่อประสิทธิภาพของการส่งข้อมูลของคุณ. ดังนั้นเซิร์ฟเวอร์, iSeries ที่มีความสามารถในการรันโปรแกรมสำหรับการบริการทั้งที่ปลอดภัย และไม่ปลอดภัยในขณะเดียวกัน. คุณสามารถใช้เซิร์ฟเวอร์ HTTP ที่ไม่ปลอดภัยให้บริการเอกสาร ที่ไม่ต้องการความปลอดภัย, เช่น แค็ตตาล็อกผลิตภัณฑ์ของคุณ. เอกสารเหล่านี้มี URL ที่เริ่มต้นด้วย `http://`. คุณสามารถใช้เซิร์ฟเวอร์ HTTP ที่ปลอดภัยสำหรับข้อมูลที่เป็นความลับ เช่น ฟอร์มที่ลูกค้าป้อนข้อมูลบัตรเครดิต เป็นต้น. โปรแกรมสามารถให้บริการเอกสารที่มี URL เริ่มต้นด้วย `http://` หรือ `https://`.

เตือนความจำ

เป็นธรรมเนียมปฏิบัติทางอินเตอร์เน็ตที่ดีที่จะบอกแก่ลูกค้าของคุณว่า การส่งข้อมูลนั้นปลอดภัยหรือไม่ปลอดภัย, โดยเฉพาะเมื่อเว็บไซต์ของคุณใช้เฉพาะเซิร์ฟเวอร์ ที่ปลอดภัยสำหรับบางเอกสาร.

โปรดจำไว้ว่า การเข้ารหัสต้องการทั้งไคลเอ็นต์ที่ปลอดภัยและเซิร์ฟเวอร์ที่ปลอดภัย. บราวเซอร์ที่ปลอดภัย (ไคลเอ็นต์ HTTP) จะกลายเป็นสิ่งธรรมดา.

ข้อควรพิจารณาเกี่ยวกับการรักษาความปลอดภัยสำหรับ LDAP

คุณลักษณะพิเศษของการรักษาความปลอดภัยให้กับ Lightweight Directory Access Protocol (LDAP) ประกอบด้วย Secure Sockets Layer (SSL), Acess Control Lists, และการเข้ารหัสให้กับรหัสผ่านแบบ CRAM-MD5. ใน V5R1, การตรวจสอบการเชื่อมต่อและการตรวจสอบความปลอดภัยแบบ Kerberos ได้ถูกเพิ่มเข้าไป เพื่อเพิ่มประสิทธิภาพความปลอดภัยของ LDAP.

สำหรับข้อมูลเพิ่มเติมเกี่ยวกับข้อมูลเหล่านี้, โปรดอ้างอิงถึง iSeries Information Center->Networking->TCP/IP->Directory Services (LDAP). โปรดดูที่ "สิ่งที่ต้องรู้ก่อนและข้อมูลที่เกี่ยวข้อง" ในหน้า xiii สำหรับข้อมูลในการเข้าไปใช้งานใน iSeries Information Center.

ข้อควรพิจารณาเกี่ยวกับความปลอดภัยสำหรับ LPD

LPD (line printer daemon) ให้ความสามารถในการกระจาย เอาต์พุตของพรินเตอร์ไปยังระบบของคุณ. ระบบไม่มีกระบวนการ sign-on ใดๆ สำหรับ LPD.

การป้องกันการเข้าถึง LPD

หากคุณ *ไม่* ต้องการให้ทุกคนใช้ LPD เพื่อเข้าถึงระบบของคุณ, คุณควรจะป้องกันไม่ให้เซิร์ฟเวอร์ LPD ทำงาน. โดยทำดังนี้:

__ ขั้นตอนที่ 1. เพื่อป้องกันไม่ให้งานของเซิร์ฟเวอร์ LPD เริ่มต้นโดยอัตโนมัติเมื่อคุณเริ่มต้น TCP/IP, ให้พิมพ์ดังนี้:

```
CHGLPDA AUTOSTART(*NO)
```

หมายเหตุ:

1. AUTOSTART(*YES) เป็นค่าดีฟอลต์.
2. "การควบคุมที่เซิร์ฟเวอร์ TCP/IP เริ่มการทำงานโดยอัตโนมัติ" ในหน้า 135 มีข้อมูลเพิ่มเติมเกี่ยวกับการควบคุมให้เซิร์ฟเวอร์ TCP/IP เริ่มทำงานโดยอัตโนมัติ.

__ ขั้นตอนที่ 2. เพื่อป้องกันบางคนจากการสัมพันธ์กับแอ็พพลิเคชันผู้ใช้, เช่น ซ็อกเก็ตแอ็พพลิเคชัน, ด้วยพอร์ตที่ระบบโดยปกติ ใช้สำหรับ LPD, ให้ทำดังนี้:

- __ ขั้นตอนที่ a. พิมพ์ GO CFGTCP เพื่อแสดงเมนู Configure TCP/IP.
- __ ขั้นตอนที่ b. เลือกอ็อพชัน 4 (Work with TCP/IP port restrictions).
- __ ขั้นตอนที่ c. บนหน้าจอ Work with TCP/IP Port Restrictions, ให้ระบุอ็อพชัน 1 (Add).
- __ ขั้นตอนที่ d. สำหรับ lower port range, ระบุค่า 515.
- __ ขั้นตอนที่ e. สำหรับ upper port range, ระบุค่า *ONLY.

หมายเหตุ:

1. ข้อจำกัดของพอร์ตมีผลครั้งต่อไปที่คุณเริ่มต้น TCP/IP. ถ้า TCP/IP ทำงานอยู่ เมื่อคุณกำหนดข้อจำกัดของพอร์ต, คุณควรจะจบ TCP/IP และเริ่มต้นใหม่อีกครั้ง.
2. RFC1700 มีข้อมูลเกี่ยวกับการกำหนดหมายเลขพอร์ต.

__ ขั้นตอนที่ f. สำหรับ protocol, ระบุค่า *TCP.

__ ขั้นตอนที่ g. สำหรับฟิลด์โปรไฟล์ผู้ใช้, ระบุชื่อโปรไฟล์ผู้ใช้ที่มีการป้องกันในระบบของคุณ. (โปรไฟล์ผู้ใช้ที่มีการป้องกันคือ โปรไฟล์ผู้ใช้ที่ไม่เป็นเจ้าของโปรแกรมที่ได้รับสิทธิมา และไม่มีรหัสผ่านที่ผู้ใช้อื่นทราบ.) โดยการจำกัดพอร์ตให้กับผู้ใช้เฉพาะ, คุณสามารถตัดผู้ใช้อื่นออกไปได้โดยอัตโนมัติ.

__ ขั้นตอนที่ h. ทำซ้ำในขั้นตอน 2c ถึงขั้นตอน 2g สำหรับโปรโตคอล *UDP.

ควบคุมการเข้าถึง LPD

ถ้าคุณต้องการอนุญาตให้ไคลเอ็นต์ของ LPD เข้าถึงระบบของคุณ, ให้ระวังในประเด็นของความปลอดภัยดังนี้:

- เพื่อป้องกันผู้ใช้จากการทำให้ระบบของคุณเต็มด้วยอ็อบเจ็กต์ที่ไม่เป็นที่ต้องการ, ให้แน่ใจว่าคุณได้กำหนดขีดจำกัดที่พอเพียงสำหรับ auxiliary storage pools (ASPs). คุณสามารถแสดงและกำหนดค่า threshold สำหรับ ASPs โดยการใช้ system service tools (SST) หรือ dedicated service tools (DST). หนังสือ *Backup and Recovery* มีข้อมูลเพิ่มเติมเกี่ยวกับ ASP threshold.
- คุณสามารถใช้สิทธิในเอาต์พุตคิวเพื่อควบคุมผู้ที่สามารถส่งไฟล์ที่อยู่ในสพูลไปยังระบบของคุณ. ผู้ใช้งาน LPD ที่ไม่มี user ID จะใช้โปรไฟล์ผู้ใช้ที่เป็น QTMPLPD . คุณสามารถให้โปรไฟล์ผู้ใช้นี้ เข้าถึงเฉพาะบางเอาต์พุตคิว.

ข้อควรพิจารณาเกี่ยวกับความปลอดภัยสำหรับ SNMP

เซิร์ฟเวอร์ iSeries สามารถทำงานเป็น simple network management protocol (SNMP) agent ในเน็ตเวิร์ก. SNMP จะให้วิธีการสำหรับการจัดการเกตเวย์, เราเตอร์, และโฮสต์ ในสภาพแวดล้อมของเครือข่าย. เอเจนต์ของ SNMP จะรวบรวมข้อมูลเกี่ยวกับระบบและทำฟังก์ชันที่ remote SNMP network managers ร้องขอ.

การป้องกันการเข้าถึง SNMP

หากคุณ *ไม่* ต้องการให้ทุกคนใช้ SNMP เพื่อเข้าถึงระบบของคุณ, คุณควรจะป้องกันไม่ให้เซิร์ฟเวอร์ SNMP ทำงาน. โดยทำดังนี้:

__ ขั้นตอนที่ 1. เพื่อป้องกันไม่ให้งานของเซิร์ฟเวอร์ SNMP เริ่มต้นโดยอัตโนมัติเมื่อคุณเริ่มต้น TCP/IP, ให้พิมพ์ดังนี้:

```
CHGSNMPA AUTOSTART(*NO)
```

หมายเหตุ:

1. AUTOSTART(*YES) เป็นค่าดีฟอลต์.

2. "การควบคุมที่เซิร์ฟเวอร์ TCP/IP เริ่มการทำงานโดยอัตโนมัติ" ในหน้า 135 มีข้อมูลเพิ่มเติมเกี่ยวกับการควบคุมให้เซิร์ฟเวอร์ TCP/IP เริ่มทำงานโดยอัตโนมัติ.

__ ขั้นตอนที่ 2. เพื่อป้องกันบางคนจากการสัมพันธ์กับแอ็พพลิเคชันผู้ใช้, เช่น ซ็อกเก็ตแอ็พพลิเคชัน, ด้วยพอร์ตที่ระบบโดยปกติใช้สำหรับ SNMP, ให้ทำดังนี้:

__ ขั้นตอนที่ a. พิมพ์ GO CFGTCP เพื่อแสดงเมนู Configure TCP/IP.

__ ขั้นตอนที่ b. เลือกอ็อพชัน 4 (Work with TCP/IP port restrictions).

__ ขั้นตอนที่ c. บนหน้าจอ Work with TCP/IP Port Restrictions, ให้ระบุอ็อพชัน 1 (Add).

__ ขั้นตอนที่ d. สำหรับ lower port range, ระบุค่า 161.

__ ขั้นตอนที่ e. สำหรับ upper port range, ระบุค่า *ONLY.

หมายเหตุ:

1. ข้อจำกัดของพอร์ตมีผลครั้งต่อไปที่คุณเริ่มต้น TCP/IP. ถ้า TCP/IP ทำงานอยู่ เมื่อคุณกำหนดข้อจำกัดของพอร์ต, คุณควรจะจบ TCP/IP และเริ่มต้นใหม่อีกครั้ง.
2. RFC1700 มีข้อมูลเกี่ยวกับการกำหนดหมายเลขพอร์ต.

__ ขั้นตอนที่ f. สำหรับ protocol, ระบุค่า *TCP.

__ ขั้นตอนที่ g. สำหรับฟิลด์โปรไฟล์ผู้ใช้, ระบุชื่อโปรไฟล์ผู้ใช้ที่มีการป้องกันในระบบของคุณ. (โปรไฟล์ผู้ใช้ที่มีการป้องกันคือ โปรไฟล์ผู้ใช้ที่ไม่เป็นเจ้าของโปรแกรมที่ได้รับสิทธิมา และไม่มีรหัสผ่านที่ผู้ใช้อื่นทราบ.) โดยการจำกัดพอร์ตให้กับผู้ใช้เฉพาะ, คุณสามารถตัดผู้ใช้อื่นออกไปได้โดยอัตโนมัติ.

__ ขั้นตอนที่ h. ทำซ้ำในขั้นตอน 2c ถึงขั้นตอน 2g สำหรับโปรโตคอล *UDP.

การควบคุมการเข้าถึง SNMP

ถ้าคุณต้องการอนุญาตให้ไคลเอ็นต์ของ SNMP เข้าถึงระบบของคุณ, ให้ระวังในประเด็นของความปลอดภัยดังนี้:

- บางคนที่สามารถเข้าถึงเครือข่ายของคุณด้วย SNMP จะสามารถรวบรวมข้อมูล เกี่ยวกับเครือข่ายของคุณ. ข้อมูล ที่คุณปิดบังโดยการใช้ alias และโดเมนเนมเซิร์ฟเวอร์ จะปรากฏแก่ผู้บุกรุกที่ผ่านทาง SNMP. นอกเหนือจากนี้, ผู้บุกรุกอาจใช้ SNMP เปลี่ยนแปลงคอนฟิกูเรชันของเครือข่ายของคุณและรบกวนการสื่อสารของคุณ.
- SNMP ขึ้นอยู่กับชื่อ community สำหรับการเข้าถึง. โดยหลักการ, ชื่อ community คล้ายคลึงกับรหัสผ่าน. ชื่อ community ไม่มีการเข้ารหัส. ดังนั้น, จึงอาจถูกดูดข้อมูลได้. ใช้คำสั่ง Add Community for SNMP (ADDCOMSNMP) เพื่อกำหนดพารามิเตอร์ manager internet address (INTNETADR) ให้เป็น IP แอดเดรสเฉพาะ หนึ่งค่าหรือมากกว่านั้นแทนค่า *ANY. คุณยังสามารถกำหนดพารามิเตอร์ OBJACC ของคำสั่ง ADDCOMSNMP หรือคำสั่ง CHGCOMSNMP ให้เป็น *NONE เพื่อป้องกัน manager ใน community จากการเข้าถึงอ็อบเจ็กต์ MIB ใดๆ . วิธีนี้เป็นการทำเพียงชั่วคราว เพื่อปฏิเสธการเข้าถึง manager ใน community โดยไม่ต้องลบ community.

ข้อควรพิจารณาเกี่ยวกับความปลอดภัยสำหรับเซิร์ฟเวอร์ INETD

ไม่เหมือนกับเซิร์ฟเวอร์ TCP/IP โดยส่วนใหญ่, เซิร์ฟเวอร์ INETD ไม่ได้ให้บริการเพียงบริการเดียวแก่ไคลเอ็นต์. แต่เซิร์ฟเวอร์ INETD ให้บริการหลายประเภท ที่ผู้บริหารสามารถปรับแต่งได้. และด้วยเหตุผลนั้น, ในบางครั้งมีการเรียกเซิร์ฟเวอร์ INETD ว่า "super server". เซิร์ฟเวอร์ INETD มีการบริการที่ติดมาด้วยต่อไปนี้:

- time
- daytime
- echo
- discard
- changed

มีการสนับสนุนบริการเหล่านี้ทั้ง TCP และ UDP. สำหรับ UDP, การบริการ echo, time, daytime, และ changed จะได้รับแพ็กเก็ต UDP, จากนั้นจะส่งแพ็กเก็ตกลับไปยังผู้เริ่มต้น. เซิร์ฟเวอร์ echo สะท้อนกลับแพ็กเก็ตที่ได้รับ, เซิร์ฟเวอร์ time และ daytime สร้างค่าเวลาในรูปแบบเฉพาะและส่งกลับ, และเซิร์ฟเวอร์ changed สร้างแพ็กเก็ตของอักขระ ASCII ที่สามารถพิมพ์ได้และส่งกลับไป.

ธรรมชาติของบริการ UDP เหล่านี้ทำให้ระบบมีความเสี่ยงต่อการถูกโจมตีเพื่อให้ระบบปฏิเสธการให้บริการ (denial of service attack). ตัวอย่างเช่น, สมมติให้คุณมีเซิร์ฟเวอร์ iSeries สองตัว ได้แก่: SYSTEMA และ SYSTEMB. โปรแกรมเมอร์ที่ประสงค์ร้ายสามารถปลอม IP header และ UDP header ด้วยแอดเดรสต้นทางของ SYSTEMA และหมายเลขพอร์ต UDP ของเซิร์ฟเวอร์ time. จากนั้นเขาสามารถส่งแพ็กเก็ตนั้นไปยังเซิร์ฟเวอร์ time บน SYSTEMB, ซึ่งจะส่งค่าเวลาไปยัง SYSTEMA, และจะตอบกลับไปยัง SYSTEMB, และต่อๆ ไป, ซึ่งทำให้เกิดการวนซ้ำที่ต่อเนื่องไม่สิ้นสุด และใช้รีซอร์สของ CPU บนทั้งสองระบบ, เช่นเดียวกับแบนด์วิธของเครือข่าย.

ดังนั้น, คุณควรจะพิจารณาความเสี่ยงของการโจมตีดังกล่าวบนระบบ iSeries ของคุณ, และรันบริการเหล่านี้บนเครือข่ายที่ปลอดภัยเท่านั้น. เซิร์ฟเวอร์ INETD ที่มาพร้อมกับเครื่องจะไม่เริ่มทำงานโดยอัตโนมัติเมื่อคุณเริ่มต้น TCP/IP. คุณสามารถตั้งค่า ให้บริการเหล่านี้เริ่มทำงานหรือไม่เมื่อ INETD เริ่มทำงาน. โดยดีฟอลต์, ทั้งเซิร์ฟเวอร์ time และเซิร์ฟเวอร์ daytime ของ TCP และ UDP เริ่มต้นทำงานเมื่อคุณให้เซิร์ฟเวอร์INETD เริ่มทำงาน.

มีสอง configuration file สำหรับเซิร์ฟเวอร์ INETD:

```
/QIBM/UserData/OS400/inetd/inetd.conf
/QIBM/ProdData/OS400/inetd/inetd.conf
```

ไฟล์เหล่านี้กำหนดว่าโปรแกรมใดจะเริ่มทำงานเมื่อ เริ่มต้นเซิร์ฟเวอร์ INETD. และยังกำหนดว่าโปรไฟล์ผู้ใช้ใดที่โปรแกรมจะทำงานอยู่ภายใต้ เมื่อ INETD เริ่มต้นโปรแกรมเหล่านี้.

หมายเหตุ: configuration file ใน proddata ควรจะไม่มีการแก้ไข. จะมีการแทนที่ทุกครั้งที่ระบบถูกโหลดขึ้นมาใหม่. การเปลี่ยนแปลงคอนฟิกูเรชันของลูกค้าควรจะเก็บอยู่ในไฟล์, ในไดเร็กทอรีทรี userdata, เช่นเดียวกับที่ไฟล์นี้ **ไม่ได้**ถูกอัพเดตในระหว่างการอัพเกรดรีลีส.

ถ้าโปรแกรมเมอร์ที่ประสงค์ร้ายได้เข้าถึงไฟล์เหล่านี้, เขาสามารถตั้งค่าใหม่ให้เริ่มโปรแกรมอื่นๆ เมื่อ INETD เริ่มต้น. ดังนั้น, เป็นสิ่งสำคัญมากที่ต้องป้องกันไฟล์เหล่านี้. โดยดีฟอลต์ จำเป็นที่จะต้องมีสิทธิ QSECOFR ในการทำการเปลี่ยนแปลง. คุณไม่ควรจะลดสิทธิที่ต้องใช้เพื่อเข้าถึงไฟล์เหล่านี้.

หมายเหตุ: ห้ามแก้ไข configuration file ในไดเร็กทอรี ProdData. จะมีการแทนที่ไฟล์นั้นทุกครั้งที่ระบบถูกโหลดขึ้นมาใหม่. การเปลี่ยนแปลงคอนฟิกูเรชันของลูกค้าควรจะเก็บอยู่ในไฟล์, ในไดเร็กทอรีทรี UserData, เช่นเดียวกับที่ไฟล์นี้ไม่ได้ถูกอัพเดตในระหว่างการอัพเกรดรีลีส.

ข้อควรพิจารณาเกี่ยวกับความปลอดภัยสำหรับการจำกัดการใช้ TCP/IP roaming

ถ้าระบบของคุณติดต่อไปยังเครือข่าย, คุณอาจต้องการจำกัดความสามารถของผู้ใช้ของคุณ ที่จะท่องเที่ยวไปในเครือข่ายด้วยแอพพลิเคชัน TCP/IP. วิธีการหนึ่งที่จะทำได้ คือการจำกัดการเข้าถึงไปยังคำสั่งไคลเอ็นต์ TCP/IP ต่อไปนี้:

หมายเหตุ: คำสั่งเหล่านี้อาจอยู่ในหลายๆ ไลบรารีในระบบของคุณ. อย่างน้อยที่สุด, ก็จะอยู่ทั้งในไลบรารี QSYS และไลบรารี QTCP. ให้แน่ใจว่า ได้หาทุกตำแหน่งที่คำสั่งปรากฏอยู่และทำให้ทั้งหมดปลอดภัย.

- STRTCPFTP
- FTP
- STRTCPTELN
- TELNET
- LPR
- SNDTCPSPLF
- RUNRMTCMD (REXEC client)

ปลายทางที่เป็นไปได้ของผู้ใช้ของคุณ กำหนดโดย:

- รายการในตารางโฮสต์ TCP/IP ของคุณ.
- รายการ *DFTROUTE ในตารางเส้นทาง TCP/IP. ซึ่งอนุญาตให้ผู้ใช้เข้าสู่ IP แอดเดรสของระบบใน hop ถัดไปเมื่อปลายทางของพวกเขาเป็นเครือข่ายที่ไม่รู้จัก. ผู้ใช้สามารถไปถึง หรือติดต่อกับเครือข่ายรีโมต (remote network) โดยการใช้เส้นทางดีฟอลต์.
- Remote name server configuration. การสนับสนุนนี้อนุญาตให้เซิร์ฟเวอร์อื่นในเครือข่าย หาตำแหน่งชื่อโฮสต์สำหรับผู้ใช้ของคุณ.
- ตารางระบบรีโมต.

คุณจำเป็นต้องควบคุมผู้ที่สามารถเพิ่มรายการไปยังตารางเหล่านี้ และเปลี่ยนแปลงคอนฟิกูเรชันของคุณ. คุณยังจำเป็นต้องเข้าใจความหมายโดยนัยของรายการในตารางของคุณ และคอนฟิกูเรชันของคุณ.

ให้ระวังผู้ใช้ที่มีความรู้ที่เข้าถึง ILE C compiler จะสามารถสร้างโปรแกรมซ็อกเก็ต ที่สามารถติดไปกับพอร์ต TCP หรือพอร์ต UDP. คุณสามารถทำให้ยากขึ้น โดยการจำกัดการเข้าถึงไปยังไฟล์ ซ็อกเก็ตอินเตอร์เฟสต่อไปนี้ในไลบรารี QSYSINC:

- SYS
- NETINET
- H
- ARPA
- sockets และ SSL

สำหรับเซอร์วิสโปรแกรม, คุณสามารถจำกัดการใช้งานแอ็พพลิเคชันของ socket และ SSL ที่ถูกคอมไพล์แล้วโดยการจำกัดการใช้เซอร์วิสโปรแกรมต่อไปนี้:

- QSOSRV1
- QSOSRV2
- QSOSKIT(SSL)
- QSOSSLSR(SSL)

เซอร์วิสโปรแกรมที่มีพร้อมกับสิทธิพับลิก *USE, แต่สามารถเปลี่ยนไปเป็น *EXCLUDE (หรือค่าอื่นได้ ตามต้องการ).

บทที่ 14. รักษาความปลอดภัยในการเข้าถึงเวิร์กสเตชัน

ผู้ใช้ระบบของคุณหลายๆ คนมีคอมพิวเตอร์ส่วนบุคคล (PCs) อยู่บนโต๊ะทำงาน เสมือนเป็นเวิร์กสเตชันของพวกเขา. พวกเขาใช้ทูลที่รันบนเครื่องพีซีได้, และจะใช้พีซีในการเชื่อมต่อไปยังเซิร์ฟเวอร์ iSeries server.

วิธีส่วนใหญ่ในการเชื่อมต่อพีซีเข้ากับเซิร์ฟเวอร์ iSeries มีฟังก์ชันมากกว่าที่มีอยู่ในการอีมูเลชันเวิร์กสเตชัน พีซีอาจดูเหมือนจอแสดงผลไปยัง iSeries และให้ผู้ใช้มีเซสชันการ sign-on แบบโต้ตอบ. นอกจากนั้น, พีซีอาจจะดูเหมือนคอมพิวเตอร์อื่นสำหรับเซิร์ฟเวอร์ iSeries และจะมีฟังก์ชันอาทิเช่นการถ่ายโอนไฟล์ และการเรียกโพรซีเดอร์แบบรีโมต.

ในฐานะที่เป็นผู้บริหารความปลอดภัยของเซิร์ฟเวอร์ iSeries , คุณต้องทราบเกี่ยวกับสิ่งต่างๆ ต่อไปนี้:

- ฟังก์ชันที่มีไว้สำหรับผู้ใช้พีซีที่ติดต่อกับระบบของคุณ
- รีซอร์สของเซิร์ฟเวอร์ iSeries ที่ผู้ใช้พีซีสามารถเข้าถึงได้.

คุณอาจต้องการที่จะป้องกันฟังก์ชันพีซีระดับสูงต่างๆ (อาทิเช่น การถ่ายโอนไฟล์ และการเรียกโพรซีเดอร์แบบรีโมต) ถ้าแบบแผนในการรักษาความปลอดภัยของเซิร์ฟเวอร์ iSeries ของคุณยังไม่ได้ถูกเตรียมไว้สำหรับฟังก์ชันเหล่านั้น. บางที, วัตถุประสงค์ในระยะยาวของคุณคือการอนุญาตให้ใช้ฟังก์ชันขั้นสูงของพีซี ในขณะที่คุณยังคงป้องกันข้อมูลในระบบของคุณ. ในหัวข้อต่อไป อธิบายประเด็นความปลอดภัยบางประการ ที่เกี่ยวข้องกับการเข้าถึงของพีซี.

การป้องกันไวรัสของเวิร์กสเตชัน

ข้อมูลนี้แนะนำวิธีที่ผู้บริหารความปลอดภัยสามารถป้องกันไวรัสต่างๆ ที่เกิดกับพีซีได้.

การรักษาความปลอดภัยให้กับการเข้าถึงข้อมูล

ซอฟต์แวร์ที่เป็นไคลเอ็นต์ของพีซีบางชนิดใช้โฟลเดอร์ร่วมในการบันทึกข้อมูลบนเซิร์ฟเวอร์. เพื่อเข้าถึงไฟล์ฐานข้อมูลของ iSeries, ผู้ใช้พีซีมีชุดของอินเตอรเฟสที่จำกัด, และถูกกำหนดมาอย่างดี. ด้วยความสามารถในการถ่ายโอนไฟล์ที่เป็นส่วนหนึ่งของซอฟต์แวร์ ไคลเอ็น/เซิร์ฟเวอร์ ส่วนใหญ่, ทำให้ผู้ใช้พีซีสามารถทำสำเนาไฟล์ต่างๆ ระหว่างเซิร์ฟเวอร์ และ พีซีได้. และด้วยความสามารถในการเข้าถึงฐานข้อมูล; อาทิเช่น ไฟล์ DDM, SQL แบบรีโมต, หรือไดร์เวอร์ของ ODBC; ทำให้ผู้ใช้พีซีสามารถเข้าไปใช้ข้อมูลบนเซิร์ฟเวอร์ได้.

ในสภาวะแวดล้อมเช่นนี้, คุณสามารถสร้างโปรแกรมที่ใช้สกัด และประเมินคำร้องขอของผู้ใช้พีซีในการเข้าไปใช้รีซอร์สของเซิร์ฟเวอร์ได้. เมื่อการร้องขอใช้ DDM, ให้คุณระบุโปรแกรมทางออกในเน็ตเวิร์กแอ็ตทริบิวต์ distributed data management access (DDMACC). สำหรับบางวิธีของการโอนถ่ายไฟล์พีซี, ให้คุณระบุโปรแกรมทางออกในเน็ตเวิร์กแอ็ตทริบิวต์ client request access (PCSACC). หรือ, คุณสามารถระบุค่า PCSACC (*REGFAC) เพื่อใช้ฟังก์ชันการจดทะเบียน.

เมื่อการร้องขอใช้ฟังก์ชันอื่นของเซิร์ฟเวอร์อื่นในการเข้าถึงข้อมูล, คุณสามารถใช้คำสั่ง WRKREGINF เพื่อจดทะเบียนโปรแกรมทางออกสำหรับฟังก์ชันของเซิร์ฟเวอร์เหล่านั้น.

อย่างไรก็ตาม, โปรแกรมทางออกอาจยากต่อการออกแบบ, และมีโอกาสที่จะล้มเหลว. โปรแกรมทางออกไม่ได้มาแทนที่สิทธิอ็อบเจ็กต์, ซึ่งออกแบบมาเพื่อป้องกันอ็อบเจ็กต์ของคุณ จากการเข้าถึงที่ไม่ได้รับอนุญาตจากต้นทางใดๆ .

ซอฟต์แวร์บางไคลเอนต์, เช่น IBM iSeries แอคเซสสำหรับ Windows, ใช้ integrated file system ในการเก็บและเข้าถึงข้อมูลบน iSeries เซิร์ฟเวอร์. ด้วย integrated file system, เซิร์ฟเวอร์ทั้งหมดกลับกลายเป็น สามารถให้ผู้ใช้พีซีเข้ามาใช้งานได้ง่ายขึ้น. สิทธิอ็อบเจ็กต์จะมีความสำคัญมากยิ่งขึ้น. ผ่านทาง integrated file system, ผู้ใช้ที่มีสิทธิในการใช้งานสูงพอ สามารถมองเห็นไลบรารีของเซิร์ฟเวอร์ราวกับว่ามันเป็นไดเร็กทอรีหนึ่งของพีซี. คำสั่งเคลื่อนย้ายและทำสำเนาแบบง่ายๆ สามารถทำการเคลื่อนย้ายข้อมูลจากไลบรารีของเซิร์ฟเวอร์ iSeries ไปยังไดเร็กทอรีของ พีซีหรือ ในทางกลับกัน. และระบบจะทำการเปลี่ยนแปลงรูปแบบของข้อมูลให้โดยอัตโนมัติ.

หมายเหตุ:

1. คุณสามารถใช้ authorization list ควบคุมการใช้อ็อบเจ็กต์ในระบบไฟล์ QSYS.LIB. ดู “การจำกัดการเข้าถึงระบบไฟล์ QSYS.LIB” ในหน้า 110 สำหรับข้อมูลเพิ่มเติม.
2. บทที่ 11, “การใช้ Integrated File System ในการรักษาความปลอดภัยให้กับไฟล์ต่างๆ”, ในหน้า 103 มีข้อมูลเพิ่มเติมเกี่ยวกับประเด็นความปลอดภัยที่เกี่ยวกับ integrated file system.

จุดแข็งของ integrated file system คือความง่ายสำหรับผู้ใช้และผู้พัฒนา. ด้วยอินเตอร์เฟสเดี่ยวหนึ่งอินเตอร์เฟส, ผู้ใช้สามารถทำงานกับอ็อบเจ็กต์ในสภาพแวดล้อมหลายๆ แบบ. ผู้ใช้พีซีไม่ต้องใช้ซอฟต์แวร์พิเศษ หรือ APIs เพื่อเข้าถึงอ็อบเจ็กต์. แต่, ผู้ใช้พีซีสามารถใช้คำสั่งพีซีที่คุ้นเคยหรือการ “point and click” เพื่อทำงานกับอ็อบเจ็กต์โดยตรง.

สำหรับทุกระบบที่มีพีซีต่ออยู่, โดยเฉพาะอย่างยิ่งสำหรับระบบที่มีซอฟต์แวร์ของไคลเอ็นต์ ที่ใช้ integrated file system, การมีโครงร่างสิทธิอ็อบเจ็กต์ที่ดีเป็นสิ่งจำเป็นอย่างยิ่ง. เนื่องจากการรักษาความปลอดภัยถูกรวมอยู่ในผลิตภัณฑ์ OS/400 , คำร้องขอใดๆ ในการเข้าไปใช้ข้อมูลจะต้องผ่านกระบวนการในการตรวจสอบสิทธิ. การตรวจสอบสิทธิจะใช้กับทุกการร้องขอที่มาจากต้นทางใดๆ และใช้กับการเข้าถึงข้อมูลไม่ว่าจะใช้วิธีการใดๆ .

สิทธิอ็อบเจ็กต์กับการเข้าไปใช้งานเวิร์กสเตชัน

เมื่อคุณจัดเตรียมสิทธิสำหรับอ็อบเจ็กต์, คุณจำเป็นต้องประเมินว่า สิทธิใดที่จะให้กับผู้ใช้พีซี. ตัวอย่างเช่น, เมื่อผู้ใช้มีสิทธิ *USE ในไฟล์, ผู้ใช้สามารถดูหรือพิมพ์ข้อมูลในไฟล์นั้น. ผู้ใช้ไม่สามารถเปลี่ยนข้อมูลในไฟล์ หรือลบไฟล์นั้น. สำหรับผู้ใช้พีซี, การดูเทียบเท่ากับ “การอ่าน (reading)”, ซึ่งให้สิทธิที่เพียงพอกับผู้ใช้ในการก็อปปี้ไฟล์ในพีซี. ซึ่งอาจไม่ใช่สิ่งที่คุณตั้งใจให้เป็น.

สำหรับบางไฟล์ที่มีความสำคัญมาก, คุณอาจจำเป็นต้องกำหนดสิทธิพับลิกเป็น *EXCLUDE เพื่อป้องกันการดาวน์โหลด. คุณสามารถจัดวิธีการอื่นในการ “view” ไฟล์ที่อยู่บนเซิร์ฟเวอร์, อาทิเช่น การใช้เมนูและโปรแกรมที่รับสิทธิมา.

ทางเลือกอื่นในการป้องกันการดาวน์โหลดก็คือการใช้โปรแกรมทางออกที่รันเมื่อใดก็ตามที่ผู้ใช้พีซีเริ่มการทำงานของฟังก์ชันในเซิร์ฟเวอร์ (อย่างอื่นที่ไม่ใช่การ sign-on แบบโต้ตอบ). คุณสามารถระบุโปรแกรมทางออกในเน็ตเวิร์กแอ็ตทริบิวต์ PCSACC โดยการใช้คำสั่ง Change Network Attribute (CHGNETA). หรือ, คุณสามารถลงทะเบียนโปรแกรมทางออก โดยการใช้คำสั่ง Work with Registration Information (WRKREGINF). วิธีการที่คุณใช้ขึ้นอยู่กับวิธีการที่พีซีเข้าถึงข้อมูลในระบบของคุณ และไคลเอ็นต์โปรแกรมที่พีซีใช้. โปรแกรมทางออก (QIBM_QPWFS_FILE_SERV) สามารถใช้กับ iSeries Access และ Net Server ในการเข้าถึง IFS. แต่จะไม่ป้องกันการเข้าถึงจากพีซีด้วยกลไกอื่นๆ , เช่น FTP หรือ ODBC.

โดยทั่วไป ซอฟต์แวร์ของพีซีจะให้ความสามารถในการอัพโหลดไว้ด้วย, ดังนั้นผู้ใช้สามารถทำสำเนาข้อมูลจากพีซีไปยังไฟล์ฐานข้อมูลที่อยู่ในเซิร์ฟเวอร์. ถ้าคุณไม่ได้จัดเตรียมโครงร่างสิทธิของคุณอย่างถูกต้อง, ผู้ใช้พีซีอาจซ้อนทับข้อมูลทั้งหมดในไฟล์ด้วยข้อมูลจากพีซี. คุณจึงจำเป็นต้องมีความระมัดระวังในการให้สิทธิ *CHANGE. ทบทวนในภาคผนวก D ในหนังสือ *iSeries Security Reference* เพื่อทำความเข้าใจถึงสิทธิที่เป็นที่ต้องการสำหรับการทำงานเกี่ยวกับไฟล์.

iSeries Information Center มีข้อมูลเพิ่มเติมเกี่ยวกับสิทธิสำหรับฟังก์ชันของพีซี และเกี่ยวกับการใช้โปรแกรมทางออก. ดูรายละเอียดได้ใน “สิ่งที่ต้องรู้ก่อนและข้อมูลที่เกี่ยวข้อง” ในหน้า xiii.

การบริหารแอ็พพลิเคชัน

การบริหารแอ็พพลิเคชันเป็นส่วนประกอบที่เลือกติดตั้งได้ของเนวิเกเตอร์ของ iSeries, ส่วนการติดต่อกับผู้ใช้ที่เป็นรูปภาพ หรือ graphical user interface (GUI) สำหรับเซิร์ฟเวอร์ iSeries. การบริหารแอ็พพลิเคชันอนุญาตให้ผู้บริหารระบบควบคุมฟังก์ชันหรือแอ็พพลิเคชันต่างๆ ที่มีไว้ให้ผู้ใช้ และกลุ่มที่อยู่บนเซิร์ฟเวอร์จำเพาะ. ทั้งนี้รวมไปถึงการควบคุมฟังก์ชั่นที่มีสำหรับผู้ใช้ที่เข้าถึงเซิร์ฟเวอร์ได้โดยผ่านทางไคลเอ็นต์. สิ่งสำคัญที่ต้องสังเกตตรงนี้, คือถ้าคุณเข้าถึงเซิร์ฟเวอร์จากไคลเอ็นต์ Windows ผู้ใช้เซิร์ฟเวอร์iSeries ที่ไม่ได้เป็น ผู้ใช้ Windows จะเป็นผู้กำหนดว่าฟังก์ชันใดที่มีไว้สำหรับการบริหาร.

สำหรับเอกสารที่สมบูรณ์เกี่ยวกับ iSeries Navigator Application Administration, ให้ดูได้จาก iSeries Information Center->Connecting to iSeries—>What to connect with—>iSeries Navigator (../html/as400/v5r2/ic2924/info/rzaj3/rzaj3overview.htm).

การบริหาร Policy

policy เป็นเครื่องมือสำหรับนักบริหารที่ใช้เหมือนกับการตั้งค่าซอฟต์แวร์ บนพีซีของไคลเอ็นต์ของพวกเขา. policy สามารถจำกัดว่าฟังก์ชันและแอ็พพลิเคชันใด ที่ผู้ใช้เข้าถึงบนเครื่องพีซีได้. policy ยังสามารถให้คำแนะนำหรือให้อำนาจกับคอนฟิกูเรชัน ที่จะถูกใช้โดยผู้ใช้บางคนหรือพีซีบางเครื่อง.

หมายเหตุ: Policy ไม่ได้เสนอการควบคุมรีซอร์สของเซิร์ฟเวอร์. Polcy ไม่ใช่เป็นการแทนที่สำหรับการรักษาความปลอดภัยให้กับเซิร์ฟเวอร์. Policy สามารถถูกใช้ในการทำให้ iSeries Access สามารถเข้าไปใช้เซิร์ฟเวอร์จากพีซีบางส่วน, โดยผู้ใช้บางคน user. อย่างไรก็ตาม, จะไม่มีการเปลี่ยนรีซอร์สในเซิร์ฟเวอร์ให้สามารถเข้ามาใช้งานได้ผ่านทางวิธีการอื่นๆ .

policy ถูกเก็บอยู่ในไฟล์เซิร์ฟเวอร์. แต่ละครั้งที่ผู้ใช้ signs on ไปยังเวิร์กสเตชันที่เป็น Windows ของพวกเขา, policy ที่ใช้กับผู้ใช้ Windows จะถูกดาวน์โหลดมาจากไฟล์เซิร์ฟเวอร์. policy จะถูกใช้กับเรจิสตรี (registry) ก่อนที่ผู้ใช้จะทำสิ่งใดบนเวิร์กสเตชัน.

นโยบาย Microsoft® ต่อการดูแลแอ็พพลิเคชัน

iSeries Access Express สนับสนุนกลยุทธสองทางที่แตกต่างกันในการ สร้างการบริหารการควบคุมภายในเครือข่ายของคุณ: Microsoft system policies และ iSeries Navigator Application Administration. พิจารณาสิ่งต่อไปนี้ เมื่อ ต้องตัดสินใจว่า กลยุทธ์ใดที่จะเหมาะสมที่สุดกับความต้องการของคุณ.

นโยบายระบบของ Microsoft

policy ถูกกำหนดจากพีซี, ไม่ขึ้นกับรีลีสของ OS/400 รีลีสใดโดยเฉพาะ. policy สามารถใช้กับพีซี, เช่นเดียวกับผู้ใช้ Windows. นี่หมายความว่าผู้ใช้จะดูโปรไฟล์ผู้ใช้ของ Windows, ไม่ใช่ของโปรไฟล์ผู้ใช้ของเซิร์ฟเวอร์. policy สามารถใช้ในการ "ตั้งค่า" เช่นเดียวกับที่ใช้ในการควบคุม. policy โดยปกติจะมีส่วนย่อยๆ มากกว่า Application Administration, และสามารถให้การทำงานที่กว้างกว่า. ทั้งนี้เนื่องจากการเชื่อมต่อไปยังเซิร์ฟเวอร์ไม่มีความจำเป็นในการตัดสินว่าผู้ใช้สามารถใช้ฟังก์ชันต่างๆ ได้หรือไม่. . การนำ policy ไปใช้งานจริงมีความยุ่งยากกว่าการใช้ Application Administration เนื่องจาก ในการใช้งานจำเป็นต้องมี Microsoft system policy editor และการตั้งค่าเครื่องพีซี เพื่อดาวน์โหลด policy จะต้องทำเฉพาะแต่ละเครื่อง.

การดูแลแอ็พพลิเคชันเนวิเกเตอร์ของ iSeries

Application Administration เชื่อมโยงข้อมูลที่เกี่ยวกับโปรไฟล์ผู้ใช้, แทนที่จะเป็นโปรไฟล์ Windowsที่ policy ของระบบ Microsoft มีการเชื่อมโยงกัน. ในขณะที่เซิร์ฟเวอร์ iSeries กำลังรันV4R3 หรือหลังจากนั้น ผลิตภัณฑ์ ต้องรันOS/400 V4R3 เพื่อที่จะใช้ Application Administration, ฟังก์ชันบางอย่างจะมีอยู่ใน V4R4 หรือหลังจากนี้ไปเท่านั้น. Application Administration ใช้ graphical user interface ของ iSeriesเนวิเกเตอร์ในการบริหาร, ซึ่งจะทำให้ง่ายขึ้นแทนที่จะใช้ policy editor. ข้อมูลของ Application Administration มีผลกับผู้ใช้โดยไม่คำนึงถึงพีซีที่ผู้ใช้ sign on. ฟังก์ชันบางตัวภายใน iSeriesเนวิเกเตอร์สามารถถูกจำกัดการใช้ได้. Application Administration จะน่าใช้มากกว่า ถ้าฟังก์ชันทั้งหมด ที่คุณต้องการควบคุมเป็นฟังก์ชันที่ใช้กับ Application Administration ได้, และถ้าเวอร์ชันของ OS/400 ที่ใช้สนับสนุน Application Administration.

การใช้ SSL กับ iSeries Access for Windows

สำหรับข้อมูลเกี่ยวกับการใช้ iSeries Access Express ด้วย SSL, ให้ทบทวน iSeries Information Center หัวข้อ *Secure Sockets Layer Administration, Securing iSeries Access Express and iSeries Navigator, iSeries Developer Kit for Java , และ iSeries Java Toolbox* ภายใต้หัวข้อหลัก Java. คุณอาจทบทวนข้อมูลนี้ในซีดีที่ให้มากับระบบของคุณ.

iSeries Navigator security

iSeries Navigator มีอินเตอร์เฟสที่ง่ายในการใช้งานกับเซิร์ฟเวอร์ของคุณสำหรับผู้ใช้ที่มี iSeries Access. ด้วยรีลีสใหม่แต่ละตัวของผลิตภัณฑ์ OS/400 , ฟังก์ชันของเซิร์ฟเวอร์ที่มากขึ้นกลายเป็นให้ใช้งานได้ผ่านทาง iSeries Navigator. อินเตอร์เฟส ที่ง่ายต่อการใช้มีประโยชน์หลายอย่าง, รวมทั้งช่วยลดค่าใช้จ่ายในการสนับสนุนทางเทคนิค และมีรูปแบบที่ดีขึ้นสำหรับระบบของคุณ. ทั้งยังแสดงถึงการร้องขอในเรื่องของความปลอดภัย.

ในฐานะของผู้บริหารความปลอดภัย, คุณไม่สามารถอาศัยความไม่รู้ของผู้ใช้ของคุณ ในการป้องกันรีซอร์สได้อีกต่อไป. iSeries Navigator ทำให้หลายๆ ฟังก์ชันง่ายและมองเห็นได้สำหรับผู้ใช้ของคุณ. คุณจำเป็นต้องแน่ใจว่าคุณได้ออกแบบและสร้าง policy ความปลอดภัยสำหรับโปรไฟล์ผู้ใช้ และสำหรับความปลอดภัยของอ็อบเจ็กต์ ที่ตรงกับความต้องการด้านความปลอดภัยของคุณ.

V4R4 และเวอร์ชันต่อมาของ IBM e(logo)server iSeries Access for Windows มีวิธีดังต่อไปนี้ที่จะควบคุมฟังก์ชั่นที่ผู้ใช้สามารถกระทำผ่าน iSeriesNavigator:

- การเลือกติดตั้ง
- การดูแลแอ็พพลิเคชัน
- ระบบที่มีการสนับสนุน policy ของWindows NT®

iSeries Navigator จะถูกบรรจุมาด้วยส่วนประกอบหลายๆ ตัวซึ่งคุณสามารถติดตั้งแยกจากกันได้. ซึ่งเป็นการยอมให้คุณติดตั้งเฉพาะฟังก์ชันที่คุณต้องการ. การดูแลแอ็พพลิเคชัน อนุญาตให้ผู้บริหารฯ ในการควบคุมฟังก์ชันที่ผู้ใช้หรือกลุ่มสามารถเข้าไปใช้ผ่านiSeries เนวิเกเตอร์ได้ . การดูแลแอ็พพลิเคชันจัดแบ่งแอ็พพลิเคชันเป็นประเภท ดังนี้:

iSeries Navigator

รวมเอา iSeries Navigator และปลั๊กอินใดๆ .

Client applications

ประกอบด้วยไคลเอ็นต์แอ็พพลิเคชันอื่นๆ ทั้งหมด, รวมทั้ง iSeries Access, ที่มีฟังก์ชันบนไคลเอ็นต์ที่ถูกบริหารผ่าน Application Administration.

Host applications

รวมเอาแอ็พพลิเคชันทั้งหมดที่ตั้งอยู่บนเซิร์ฟเวอร์และมีฟังก์ชันที่ถูกควบคุมผ่านทาง Application Administration.

คุณสามารถใช้การติดตั้งแบบเลือกได้, application administration, และ policy ต่างๆ ในการจำกัดฟังก์ชันเนวิเกเตอร์ iSeries ที่ผู้ใช้สามารถเข้าถึงได้. อย่างไรก็ตาม, ไม่สามารถใช้วิธีการข้างต้นสำหรับความปลอดภัยของรีซอร์ส.

เริ่มต้นใน V4R4, IBM e(logo)server iSeries Access for Windows สนับสนุนการใช้ Windows NT System Policy Editor เพื่อควบคุมฟังก์ชันที่สามารถทำงานจากพีซีไคลเอ็นต์เฉพาะได้, โดยไม่คำนึงถึงผู้ที่กำลังใช้พีซีนั้น.

ดูใน iSeries Information Center สำหรับข้อมูลเพิ่มเติมของการติดตั้งเพียงบางส่วน (selective installation), Application Administration และ Policy Administration. ส่วน “ขอบเขตของการเข้าไปใช้ Program Function” ในหน้า 6 ของหนังสือนี้ มีการอธิบายบางส่วนของการบริหารแอ็พพลิเคชันด้วย.

การป้องกันการเข้าถึง ODBC

Open database connectivity (ODBC) เป็นเครื่องมือที่แอ็พพลิเคชันของพีซี สามารถใช้เข้าถึงข้อมูลของ iSeries เหมือนกับว่าข้อมูลนั้นเป็นข้อมูลของพีซี. โปรแกรมเมอร์ ODBC สามารถทำให้ตำแหน่งทางกายภาพของข้อมูลโปร่งใส (transparent) กับผู้ใช้แอ็พพลิเคชันของพีซี . สำหรับข้อมูลเพิ่มเติมเกี่ยวกับข้อควรพิจารณาเกี่ยวกับความปลอดภัยของ ODBC , ให้ดูในข้อมูลเกี่ยวกับ ″iSeries Access for Windows ODBC security″ (/rzaii/rzaiiodbc09.HTM), ที่อยู่ในiSeries Information Center.

ข้อควรพิจารณาเกี่ยวกับความปลอดภัยสำหรับรหัสผ่านของเซสชันของเวิร์กสเตชัน

โดยปกติ, เมื่อผู้ใช้พีซีเริ่มใช้งานซอฟต์แวร์เชื่อมต่อ, อาทิเช่นiSeries Access, ผู้ใช้พิมพ์ user ID กับรหัสผ่านสำหรับเซิร์ฟเวอร์ทันที. รหัสผ่านจะถูกเข้ารหัส และเก็บไว้ในหน่วยความจำของพีซี. เมื่อใดที่ผู้ใช้สร้างเซสชันใหม่ไปยังเซิร์ฟเวอร์เดิม, พีซีจะส่ง user ID และรหัสผ่านไปโดยอัตโนมัติ.

ซอฟต์แวร์ไคลเอ็นต์/เซิร์ฟเวอร์ บางตัวยังให้อ็อพชันของการข้ามหน้าจอ Sign On สำหรับเซสชันแบบโต้ตอบ. ซอฟต์แวร์จะส่ง user ID และรหัสผ่านที่เข้ารหัส เมื่อผู้ใช้เริ่มต้นเซสชันแบบโต้ตอบ (5250 อีมูเลชัน). เพื่อสนับสนุนตัวเลือกนี้, ค่าของระบบ QRMTSIGN ที่อยู่บนเซิร์ฟเวอร์ต้องถูกตั้งไว้เป็น *VERIFY.

เมื่อคุณเลือกที่จะอนุญาตการข้ามหน้าจอ Sign On, คุณจำเป็นต้องพิจาณาถึงข้อดีข้อเสีย (trade-off) ด้านความปลอดภัย.

ช่องโหว่ความปลอดภัย: สำหรับการอีมูเลชันแบบ 5250 หรือเซสชันแบบโต้ตอบอื่นๆ, หน้าจอ Sign On จะเป็นเช่นเดียวกันกับจอแสดงผลอื่นๆ . ถึงแม้ว่าไม่มีการแสดงรหัสผ่านบนหน้าจอเมื่อรหัสผ่านถูกพิมพ์, แต่รหัสผ่านถูกส่งผ่านการเชื่อมต่อ ในรูปแบบที่ไม่ได้เข้ารหัสเหมือนกับฟิลด์ข้อมูลอื่นๆ . สำหรับการเชื่อมต่อบางชนิด, อาจเป็นการเปิดโอกาสสำหรับผู้จะบุกรุกที่เฝ้าสังเกตสายต่อเชื่อมและตรวจจับ user ID และรหัสผ่าน. การเฝ้าสังเกตการเชื่อมต่อ โดยการใช้เครื่องมืออิเล็กทรอนิก มักถูกเรียกว่าเป็น **การดูดข้อมูล (sniffing)**. เริ่มต้นด้วย V4R4, คุณสามารถใช้ secure sockets layer (SSL) ในการเข้ารหัสการสื่อสารระหว่าง iSeries Access และเซิร์ฟเวอร์ iSeries. ซึ่งจะป้องกันข้อมูลของคุณ, รวมทั้งรหัสผ่าน, จากการดูดข้อมูล.

เมื่อคุณเลือกอ็อพชันในการข้ามหน้าจอ Sign On, พีซีจะเข้ารหัสรหัสผ่านก่อนที่จะส่งออกไป. การเข้ารหัส เป็นการหลีกเลี่ยงโอกาสที่รหัสผ่านจะถูกขโมยหรือถูกดูดข้อมูล. อย่างไรก็ตาม, คุณต้องแน่ใจว่าผู้ใช้พีซีของคุณทำตามขั้นตอนความปลอดภัย. พีซีที่ไม่ได้สนใจที่มีเซสชันที่แอ็คทีฟไปยัง

ระบบ iSeries เปิดโอกาสให้บางคนเริ่มต้นเซสชันอื่น โดยไม่ต้องทราบ user ID และรหัสผ่าน. ต้องมีการจัดเตรียมพีซีให้ถูกล็อกเมื่อระบบไม่แอ็คทีฟเป็นระยะเวลานาน, และต้องมีการป้อนรหัสผ่านเพื่อให้เซสชันทำงานต่อไป.

แม้ว่าคุณไม่ได้เลือกที่จะข้ามหน้าจอ Sign On, พีซีที่ปล่อยว่างไม่ได้ใช้แต่มีเซสชันที่แอ็คทีฟ แสดงถึงจุดอ่อนด้านความปลอดภัย. โดยการใช้ซอฟต์แวร์ของพีซี, บางคนสามารถจะเริ่มต้นเซสชันของเซิร์ฟเวอร์ และเข้าถึงข้อมูล, โดยไม่ต้องทราบ user ID และรหัสผ่าน. จุดอ่อนของ 5250 อีมูเลชันมีมากกว่า เนื่องจากต้องการข้อมูลน้อยกว่าในการเริ่มต้นเซสชันและเข้าถึงข้อมูล.

คุณยังจำเป็นที่จะต้องให้ความรู้กับผู้ใช้ของคุณเกี่ยวกับผลกระทบของการตัดการติดต่อเซสชัน iSeries Access ของผู้ใช้. ผู้ใช้ทั้งหลาย, สมมติว่า(ในเชิงตรรกะแต่ไม่ถูกต้อง) ตัวเลือก disconnect จะทำการหยุดการเชื่อมต่อเข้ากับอย่างสมบูรณ์เซิร์ฟเวอร์. ในความเป็นจริง, เมื่อผู้ใช้เลือกตัวเลือกเป็น disconnect , เซิร์ฟเวอร์จะทำให้เซสชันของผู้ใช้ (ที่เป็น ไลเซนส์) ว่างสำหรับผู้ใช้คนอื่นๆ. อย่างไรก็ตาม, การเชื่อมต่อของไปยังเซิร์ฟเวอร์ยังคงเปิดอยู่. ผู้ใช้อีกคนหนึ่งสามารถเดินไปยังพีซีที่ไม่ได้ป้องกันไว้ และขอสิทธิในการเข้าไปใช้รีซอร์สในเซิร์ฟเวอร์โดยไม่ต้องใส่ User ID และ password.

คุณสามารถแนะนำสองทางเลือกให้กับผู้ใช้ของคุณ ที่จำเป็นต้องตัดการติดต่อเซสชันของพวกเขา:

- ให้แน่ใจว่าพีซีของพวกเขามีฟังก์ชัน lockup ที่ต้องการรหัสผ่าน. ซึ่งจะทำให้ผู้อื่นที่ไม่ทราบรหัสผ่านไม่สามารถใช้พีซีที่ไม่ได้สนใจนั้นได้.
- เพื่อตัดการติดต่อเซสชันอย่างสมบูรณ์, จะต้อง log off Windows หรือ restart (reboot) พีซี. ซึ่งจะเป็นการสิ้นสุดเซสชันไปยัง iSeries.

คุณจำเป็นที่จะต้องให้ความรู้กับผู้ใช้ของคุณเกี่ยวกับช่องโหว่ด้านความปลอดภัยที่เป็นไปได้เมื่อเขาใช้ iSeries Access for Windows. เมื่อผู้ใช้ระบุค่า UNC (universal naming convention) เพื่อบ่งชี้รีซอร์สของ iSeries, ไคลเอ็นต์ของ Win95 หรือ NT สร้างการเชื่อมต่อเครือข่าย ไปยังเซิร์ฟเวอร์. เนื่องจากผู้ใช้ระบุค่า UNC, ผู้ใช้ไม่เห็นว่านี่เป็น Network Drive ที่ถูกแม็พไว้. บ่อยครั้ง, ผู้ใช้ไม่ทราบถึงความมีอยู่ของการติดต่อเครือข่าย. อย่างไรก็ตาม, การเชื่อมต่อของเน็ตเวิร์กนี้แสดงช่องโหว่ความปลอดภัยที่เกิดบนพีซีที่ไม่ได้ระวังไว้เนื่องจากเซิร์ฟเวอร์ปรากฏในลำต้นไดเร็กทอรีบนพีซี. ถ้าเซสชันของผู้ใช้มีโปรไฟล์ผู้ใช้ที่มีอำนาจ, รีซอร์สของเซิร์ฟเวอร์ก็อาจจะปรากฏให้เห็นบนพีซีที่ปล่อยว่างอยู่ได้. เช่นเดียวกับตัวอย่างข้างต้น, การแก้ไขคือก็คือให้แน่ใจว่าผู้ใช้ได้เข้าใจจุดอ่อนนี้และพวกเขาได้ใช้ฟังก์ชัน lockup บนพีซีของพวกเขา.

ปกป้องเซิร์ฟเวอร์จากคำสั่งและโพรซีเดอร์แบบรีโมต

ผู้ใช้พีซีที่มีความรู้ความสามารถใช้ซอฟต์แวร์อาทิ เช่น iSeries Access รันคำสั่งบนเซิร์ฟเวอร์โดยไม่จำเป็นต้องไปผ่านหน้าจอ Sign On . ต่อไปนี้เป็นวิธีต่างๆ ที่มีไว้สำหรับผู้ใช้พีซีในการรันคำสั่งของเซิร์ฟเวอร์. ซอฟต์แวร์ ไคลเอ็นต์/เซิร์ฟเวอร์จะกำหนดวิธีการ ที่ผู้ใช้พีซีจะสามารถใช้ได้.

- ผู้ใช้สามารถเปิดไฟล์ DDM และใช้ฟังก์ชันของคำสั่งรีโมตเพื่อรันคำสั่ง.
- ในบางซอฟต์แวร์, อาทิเช่นiSeries Access optimized clients, มีฟังก์ชันคำสั่งรีโมตผ่านทาง Distributed Program Call (DPC) APIs, โดยไม่จำเป็นต้องใช้ DDM.
- บางซอฟต์แวร์, เช่น remote SQL และ ODBC, จะให้ฟังก์ชันคำสั่งรีโมต โดยไม่ต้องมี DDM หรือ DPC.

สำหรับซอฟต์แวร์ไคลเอ็นต์/เซิร์ฟเวอร์ที่ใช้ DDM สำหรับการสนับสนุนคำสั่งรีโมต, คุณสามารถใช้เน็ตเวิร์กแอ็ตทริบิวต์ DDMACC เพื่อป้องกันคำสั่งรีโมต อย่างสมบูรณ์. สำหรับซอฟต์แวร์ไคลเอ็นต์/เซิร์ฟเวอร์ที่ใช้การสนับสนุนของเซิร์ฟเวอร์อื่น, คุณสามารถลงทะเบียนโปรแกรมทางออกสำหรับเซิร์ฟเวอร์นั้น. ถ้าคุณต้องการอนุญาตให้ใช้คำสั่งรีโมต, คุณต้องแน่ใจว่าโครงร่างสิทธิ์อบเจ็กต์ของคุณ ป้องกันข้อมูลของคุณได้อย่างพอเพียง. ความสามารถของคำสั่งรีโมต เทียบเท่ากับการให้บรรทัดรับคำสั่งกับผู้ใช้. นอกจากนี้, เมื่อ iSeries ได้รับคำสั่งรีโมตผ่านทาง DDM, ระบบจะไม่บังคับใช้ค่ากำหนด Limited capability (LMTCPB) ของโปรไฟล์ผู้ใช้.

ปกป้องเวิร์กสเตชันจากคำสั่งและโพรซีเดอร์รีโมต

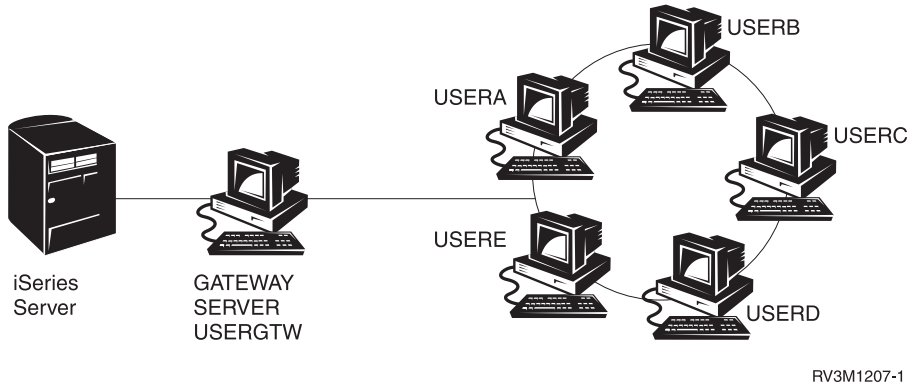
IBM iSeries Access สำหรับ Windows มีความสามารถในการรับคำสั่งรีโมตบนพีซี. คุณสามารถใช้คำสั่ง Run Remote Command (RUNRMTCMD) บนเซิร์ฟเวอร์ในการรันโพรซีเดอร์บนเครื่องพีซีที่ต่ออยู่ด้วย. ความสามารถของ RUNRMTCMD เป็นเครื่องมือที่มีค่าสำหรับผู้บริหารระบบ และบุคคลากรของแผนกให้คำแนะนำ. อย่างไรก็ตาม, มันยังทำให้มีโอกาสในการทำให้ข้อมูลบนพีซีเสียหาย ซึ่งอาจจะโดยเจตนาหรือโดยไม่เจตนา.

พีซีไม่มีฟังก์ชันของสิทธิ์อบเจ็กต์เดียวกันกับของเซิร์ฟเวอร์ iSeries . การปกป้องปัญหาจากคำสั่ง RUNRMTCMD ที่ดีที่สุดก็คือทำการจำกัดผู้ใช้ระบบที่มีความสามารถในการเข้าไปใช้คำสั่งอย่างระมัดระวัง. IBM iSeries Access สำหรับ Windows มีความสามารถในการจดทะเบียนว่าผู้ใช้คนใดสามารถรันคำสั่งรีโมตบนพีซีเครื่องที่จำเพาะเจาะจงได้. เมื่อการติดต่อผ่านทาง TCP/IP, คุณสามารถใช้คุณสมบัติของคอนโทรลพาเนล (control panel) บนไคลเอ็นต์เพื่อควบคุมการเข้าถึงคำสั่งรีโมต. คุณสามารถอนุญาตผู้ใช้โดย user ID หรือโดยชื่อของระบบรีโมต (remote system name). เมื่อการติดต่อผ่านทาง SNA, ซอฟต์แวร์บางตัวของไคลเอ็นต์มีความสามารถในการจัดเตรียมความปลอดภัยสำหรับการสนทนา. ด้วยซอฟต์แวร์ไคลเอ็นต์อื่น, คุณสามารถเลือกที่จะจัดเตรียมความสามารถของ incoming-command หรือไม่ก็ได้.

สำหรับแต่ละการรวมกัน (combination) ของซอฟต์แวร์ไคลเอ็นต์และประเภทของการติดต่อ (เช่น TCP/IP หรือ SNA), คุณจำเป็นต้องพิจารณาความเป็นไปได้ในการใช้ incoming-command ไปยังพีซีที่ต่ออยู่. ดูเอกสารของไคลเอ็นต์โดยการค้นหาคำว่า “incoming command ” หรือ “RUNRMTCMD”. ให้เตรียมตัวที่จะให้คำแนะนำแก่ผู้ใช้พีซี และผู้บริหารเครือข่ายของคุณ เกี่ยวกับวิธีการที่ถูกต้อง (ปลอดภัย) ในการตั้งค่าไคลเอ็นต์เพื่ออนุญาตให้ใช้หรือป้องกันความสามารถนี้.

เกตเวย์เซิร์ฟเวอร์

ระบบของคุณอาจอยู่ในเครือข่ายที่มีตัวกลางหรือเกตเวย์เซิร์ฟเวอร์อยู่ระหว่างระบบ iSeries กับพีซี. ตัวอย่างเช่น, ระบบ iSeries ของคุณอาจต่อเข้ากับ LAN ด้วยพีซีเซิร์ฟเวอร์ ที่มีพีซีอื่นๆ ต่ออยู่กับเซิร์ฟเวอร์นั้น. ประเด็นความปลอดภัยในสถานการณ์นี้ขึ้นอยู่กับ ความสามารถของซอฟต์แวร์ที่ทำงานอยู่บนเกตเวย์เซิร์ฟเวอร์. รูปที่ 13 ในหน้า 173 แสดงตัวอย่างของ gateway-server configuration:



รูปที่ 13. iSeries ระบบพร้อมด้วยเกตเวย์เซิร์ฟเวอร์

ด้วยบางซอฟต์แวร์, ระบบ iSeries ของคุณจะไม่ทราบเกี่ยวกับผู้ใช้ใดๆ (เช่น USERA หรือ USERC) ที่อยู่ในส่วนที่ต่อจากเกตเวย์เซิร์ฟเวอร์. เซิร์ฟเวอร์จะ sign on ไปยังระบบเป็นผู้ใช้เดี่ยว (USERGTW). โดยจะใช้ USERGTW user ID ในการจัดการการร้องขอทั้งหมดจากผู้ใช้ในอีกส่วนหนึ่ง. คำร้องขอจาก USERA จะดูเหมือนเป็นคำร้องขอจากผู้ใช้ USERGTW ต่อเซิร์ฟเวอร์ .

ถ้าเป็นกรณีนี้, คุณต้องพึ่งพาการบังคับใช้ความปลอดภัยของเกตเวย์เซิร์ฟเวอร์. คุณต้องทำความเข้าใจ และจัดการความสามารถด้านความปลอดภัยของเกตเวย์ซิร์ฟเวอร์. จากมุมมองของเซิร์ฟเวอร์ iSeries , ผู้ใช้ทุกคนมีสิทธิในการใช้งานเดียวกันกับ user ID ที่เกตเวย์เซิร์ฟเวอร์ใช้ในการเริ่มการทำงานของเซสชัน. คุณอาจคิดถึงกรณีนี้ว่าเหมือนกับการรันโปรแกรมที่รับสิทธิมา และมีบรรทัดรับคำสั่ง.

ด้วยซอฟต์แวร์อื่นๆ , เกตเวย์เซิร์ฟเวอร์ส่งผ่านคำร้องขอจากผู้ใช้รายบุคคลไปยังเซิร์ฟเวอร์ iSeries servers. เซิร์ฟเวอร์ iSeries ทราบว่า USERA กำลังร้องขอการเข้าไปใช้อ็อบเจ็กต์ใดอ็อบเจ็กต์หนึ่งโดยเฉพาะ. เกตเวย์ เกือบจะมีความเป็น transparent ต่อระบบ.

ถ้าระบบของคุณอยู่ภายในเครือข่ายที่มีเกตเวย์เซิร์ฟเวอร์, คุณจำเป็นต้องประเมินสิทธิที่จะให้แก่ user ID ที่ถูกใช้โดยเกตเวย์เซิร์ฟเวอร์. คุณยังต้องทำความเข้าใจในสิ่งต่อไปนี้:

- กลไกความปลอดภัยที่เกตเวย์เซิร์ฟเวอร์บังคับใช้.
- วิธีที่ผู้ใช้ที่อยู่อีกส่วนหนึ่งปรากฏต่อระบบ iSeries ของคุณ.

การสื่อสารแบบ wireless LAN

ไคลเอ็นต์บางตัวอาจใช้ iSeries Wireless LAN ในการสื่อสารกับระบบของคุณโดยไม่จำเป็นต้องใช้สายเชื่อมต่อ. & ; Wireless LAN ใช้เทคโนโลยีการสื่อสารแบบคลื่นความถี่วิทยุ. ในฐานะของผู้บริหารความปลอดภัย, คุณควรจะต้องตระหนักถึงลักษณะความปลอดภัยของผลิตภัณฑ์ iSeries Wireless LAN ต่อไปนี้:

- ผลิตภัณฑ์ LAN ไร้สายเหล่านี้ใช้เทคโนโลยีกระจายแถบความถี่ (spread spectrum). เทคโนโลยีเดียวกันนี้เคยถูกใช้โดยรัฐบาลในอดีต เพื่อให้ความปลอดภัยแก่การส่งข้อมูลโดยคลื่นวิทยุ. สำหรับบางคนที่พยายามเฝ้าสังเกตการส่งผ่านข้อมูลแบบอิเล็กทรอนิก, การส่งผ่านจะปรากฏเป็นสัญญาณรบกวน (noise) มากกว่าที่จะเป็นการส่งผ่านจริง.
- การติดต่อแบบไร้สาย มีสามคอนฟิกูเรชันพารามิเตอร์ที่เกี่ยวข้องกับความปลอดภัย:

- อัตราข้อมูล-data rate (มีสองอัตราข้อมูลที่เป็นไปได้)
- ความถี่-frequency (มีห้าความถี่ที่เป็นไปได้)
- system identifier (มี 8 ล้าน identifier ที่เป็นไปได้)

องค์ประกอบคอนฟิกกูเรชันเหล่านี้รวมกันเป็นคอนฟิกูเรชันที่เป็นไปได้ 80 ล้านแบบ, ซึ่งทำให้โอกาสการเดาคอนฟิกูเรชันที่ถูกต้องของนักเจาะระบบ มีความเป็นไปได้น้อยมาก.

- เช่นเดียวกับวิธีการสื่อสารอื่นๆ, ความปลอดภัยของการสื่อสารไร้สาย ได้รับผลจากความปลอดภัยของอุปกรณ์ไคลเอ็นต์. ข้อมูล system ID และคอนฟิกูเรชันพารามิเตอร์อื่นๆ อยู่ในไฟล์บนอุปกรณ์ไคลเอ็นต์และจะต้องได้รับการปกป้อง.
- ถ้าอุปกรณ์ไร้สายหายไปหรือถูกขโมยไป, มาตรการความปลอดภัยของเซิร์ฟเวอร์โดยปกติ, อาทิเช่น รหัสผ่านในการ sign-on และความปลอดภัยของอ็อบเจ็กต์, จะให้การปกป้องเมื่อผู้ใช้ที่ไม่ได้รับอนุญาตพยายามที่จะใช้อุปกรณ์หน่วยที่สูญหายไปหรือถูกขโมยไปในการเข้าถึงระบบของคุณ.
- ถ้าหน่วยไคลเอ็นต์ไร้สายสูญหายไปหรือถูกขโมย, คุณควรพิจาณาเปลี่ยนแปลงข้อมูล system ID สำหรับผู้ใช้ทุกคน, จุดที่เข้าถึง, และระบบ. ให้คิดว่าเหมือนการเปลี่ยนประตูของคุณ ถ้าชุดกุญแจถูกขโมย.
- คุณอาจต้องการแบ่งเซิร์ฟเวอร์ของคุณเป็นกลุ่มของไคลเอ็นต์ที่มี system ID ที่ไม่ซ้ำกัน. ซึ่งจะจำกัดผลกระทบที่เกิดขึ้น หากอุปกรณ์สูญหายไปหรือถูกขโมย. วิธีนี้จะใช้งานได้ ถ้าคุณสามารถจำกัดขอบเขตกลุ่มของผู้ใช้ไปยังส่วนเฉพาะของการติดตั้งของคุณ.
- ไม่เหมือนกับเทคโนโลยี LAN ที่ใช้สาย, เทคโนโลยี LAN แบบไร้สายเป็นแบบเฉพาะ. ดังนั้น, ไม่มีอุปกรณ์ดูดข้อมูลทางอิเล็กทรอนิก (sniffer) สำหรับผลิตภัณฑ์ LAN ไร้สายเหล่านี้ ที่เปิดเผยต่อสาธารณะ. sniffer เป็นอุปกรณ์อิเล็กทรอนิกที่ทำการมอนิเตอร์การส่งข้อมูลโดยไม่ได้รับอนุญาต.

บทที่ 15. โปรแกรมทางออกที่เกี่ยวกับความปลอดภัย

บางฟังก์ชันของเซิร์ฟเวอร์ iSeries มีทางออก ดังนั้นระบบของคุณจึงสามารถรันโปรแกรมที่ผู้ใช้สร้างขึ้นเพื่อทำงานเพิ่มเติมในส่วนของการทำการตรวจสอบและทำให้ใช้งานได้. ตัวอย่างเช่น, คุณสามารถจัดเตรียมระบบของคุณ เพื่อเรียกใช้โปรแกรมทางออกทุกครั้งที่มีบางคนพยายามเปิดไฟล์ DDM (distributed data management) ในระบบของคุณ. คุณสามารถใช้ฟังก์ชันการลงทะเบียน (registration function) เพื่อระบุโปรแกรมทางออกที่จะทำงานภายใต้บางสภาวะ.

เอกสาร iSeries หลายฉบับ มีตัวอย่างของโปรแกรมทางออกที่ทำงานเกี่ยวกับความปลอดภัย. ตารางที่ 24มีรายชื่อของโปรแกรมทางออกเหล่านี้ และแหล่งที่มาของโปรแกรมตัวอย่าง.

ตารางที่ 24. ที่มาของโปรแกรมทางออกตัวอย่าง

ประเภทของโปรแกมทางออก	วัตถุประสงค์	สามารถหาดูตัวอย่างได้ที่ไหน
การตรวจสอบรหัสผ่าน	ค่ากำหนดของระบบ QPWDVLDPGM สามารถระบุชื่อโปรแกรมหรือแสดงให้เห็นว่าค่ากำหนดของระบบที่ลงทะเบียนสำหรับจุดทางออก QIBM_QSY_VLD_PASSWRD ถูกใช้เพื่อตรวจสอบรหัสผ่านใหม่สำหรับความต้องการเพิ่มเติม ที่ไม่ได้ถูกจัดการด้วยค่ากำหนดของระบบ QPWDxxx. การใช้โปรแกรมนี้ต้องมีการเฝ้าสังเกตอย่างระมัดระวัง เนื่องจากโปรแกรมจะได้รับรหัสผ่าน ที่ไม่มีการเข้ารหัส. โปรแกรมนี้ **ต้องไม่** บันทึกรหัสผ่านไว้ในไฟล์หรือส่งผ่านไปยังโปรแกรมอื่น.	• *An Implementation Guide for iSeries Security and Auditing, GG24-4200* • *iSeries Security Reference*, SC41-5302-07
PC Support/400 or Client Access access[1]	คุณสามารถระบุชื่อโปรแกรมนี้ในพารามิเตอร์ Client request access (PCSACC) ของเน็ตเวิร์กแอ็ตทริบิวต์ เพื่อควบคุมฟังก์ชันต่อไปนี้: • ฟังก์ชัน virtual printer • ฟังก์ชันการโอนถ่ายไฟล์ • ฟังก์ชัน shared folders Type 2 • ฟังก์ชัน client access message • Data queues • ฟังก์ชัน remote SQL	*An Implementation Guide for iSeries Security and Auditing, GG24-4200*
การเข้าถึง Distributed Data Management (DDM)	คุณสามารถระบุชื่อโปรแกรมนี้ในพารามิเตอร์ DDM request access (DDMACC) ของเน็ตเวิร์กแอ็ตทริบิวต์ เพื่อควบคุมฟังก์ชันต่อไปนี้: • ฟังก์ชัน shared folders Type 0 และ 1 • ฟังก์ชัน Submit Remote Command	*An Implementation Guide for iSeries Security and Auditing, GG24-4200*

ตารางที่ 24. ที่มาของโปรแกรมทางออกตัวอย่าง (ต่อ)

ประเภทของโปรแกมทางออก	วัตถุประสงค์	สามารถหาดูตัวอย่างได้ที่ไหน
Remote sign on	คุณสามารถระบุโปรแกรมในค่ากำหนดของระบบ QRMTSIGN เพื่อควบคุมผู้ใช้ที่สามารถ sign on โดยอัตโนมัติจากตำแหน่งใด (pass-through.)	*An Implementation Guide for iSeries Security and Auditing, GG24-4200*
Open Database Connectivity (ODBC) with iSeries Access[1]	ควบคุมฟังก์ชันของ ODBC ต่อไปนี้: • ODBC ได้รับอนุญาตหรือไม่. • ฟังก์ชันใดที่ได้รับอนุญาตสำหรับไฟล์ฐานข้อมูล iSeries. • SQL statement ใดที่ได้รับอนุญาต. • ข้อมูลใดที่สามารถสืบค้นได้เกี่ยวกับอ็อบเจ็กต์เซิร์ฟเวอร์ฐานข้อมูล (database server object). • SQL catalog function ใดที่ได้รับอนุญาต.	ไม่มีอยู่เลย.
โปรแกรมจัดการ QSYSMSG break	คุณสามารถสร้างโปรแกรมเพื่อเฝ้าสังเกตคิวข้อความ QSYSMSG และกระทำสิ่งที่เหมาะสม (เช่น การแจ้งต่อผู้บริหารความปลอดภัย) ตามประเภทของข้อความ.	*An Implementation Guide for iSeries Security and Auditing, GG24-4200*
TCP/IP	เซิร์ฟเวอร์ TCP/IP หลายเซิร์ฟเวอร์ (เช่น FTP, TFTP, TELNET, และ REXEC) มีจุดทางออก. คุณสามารถใส่โปรแกรมทางออกเพื่อจัดการกับการล็อกออน และเพื่อตรวจสอบการร้องขอของผู้ใช้, เช่น การร้องขอที่จะ get หรือ put ไฟล์ที่กำหนด. คุณยังสามารถใช้จุดทางออกเหล่านี้ทำให้มี FTP ที่ไม่ระบุชื่อ (anonymous FTP) ในระบบของคุณ.	"TCP/IP User Exits ที่อยู่ในหนังสือคู่มือ *iSeries SysteI Reference* "
การเปลี่ยนแปลงโปรไฟล์ผู้ใช้	คุณสามารถสร้างโปรแกรมทางออก สำหรับคำสั่งของโปรไฟล์ผู้ใช้ต่อไปนี้: CHGUSRPRF CRTUSRPRF DLTUSRPRF RSTUSRPRF	• *iSeries Security Reference*, SC41-5302-07 • "TCP/IP User Exits อยู่ในหนังสือคู่มือ *iSeries System API Reference* "

หมายเหตุ:

1. ข้อมูลเพิ่มเติมในหัวข้อนี้ สามารถพบได้ใน iSeries Information Center. โปรดดูที่ "สิ่งที่ต้องรู้ก่อนและข้อมูลที่เกี่ยวข้อง" ในหน้า xiii สำหรับข้อมูลเพิ่มเติม.

บทที่ 16. ข้อควรพิจารณาเกี่ยวกับความปลอดภัยสำหรับอินเตอร์เน็ตบราวเซอร์

ผู้ใช้พีซีจำนวนมากในองค์กรของคุณ มีบราวเซอร์บนเวิร์กสเตชันของพวกเขา. พวกเขาอาจเชื่อมต่อกับอินเตอร์เน็ต. และอาจจะเชื่อมต่ออยู่กับเซิร์ฟเวอร์ของคุณด้วยเช่นกัน. ต่อไปนี้เป็นข้อควรพิจารณาเกี่ยวกับความปลอดภัยบางข้อสำหรับทั้งพีซี และ สำหรับเซิร์ฟเวอร์ของคุณ.

ความเสี่ยง: เวิร์กสเตชันเกิดการเสียหาย

เว็บเพจที่คุณเยี่ยมชมอาจมี "โปรแกรม" ที่เกี่ยวข้อง, เช่น Java แอ็พเพล็ต, Active-X control, หรือ plug-in บางประเภท. ถึงแม้ว่าจะมีไม่บ่อยครั้งที่, "โปรแกรม" ประเภทนี้เมื่อวิ่งบนพีซีจะมีขีดความสามารถที่จะทำลายข้อมูลบนพีซี. ในฐานะของผู้บริหารความปลอดภัย, ควรพิจารณาถึงการป้องกันพีซีในองค์กรของคุณ ดังนี้:

- เข้าใจถึงทางเลือกด้านความปลอดภัยของแต่ละบราวเซอร์ที่ผู้ใช้ของคุณมี. ตัวอย่างเช่น, สำหรับบางบราวเซอร์, คุณสามารถควบคุมการเข้าถึงที่Java applet มีภายนอกบราวเซอร์ (สภาพแวดล้อมการทำงานที่จำกัดของ Java เรียกว่า *sandbox*). ซึ่งจะสามารถป้องกันไม่ให้แอ็พเพล็ต ทำให้ข้อมูลของพีซีเสียหาย.

  หมายเหตุ: จะไม่มีหลักการของ sandbox และข้อจำกัดด้านความปลอดภัยที่เกี่ยวข้อง สำหรับ Active-X และ plug-in อื่นๆ .
- ให้คำแนะนำแก่ผู้ใช้ของคุณ เกี่ยวกับค่าติดตั้งของบราวเซอร์ของพวกเขา. คุณอาจจะไม่มีเวลาหรือทรัพยากรเพียงพอ ที่จะทำให้แน่ใจว่าผู้ใช้ของคุณได้ทำตามข้อแนะนำ. เพราะฉะนั้น, คุณต้องให้ความรู้แก่ผู้ใช้ เกี่ยวกับความเสี่ยงที่เป็นไปได้ของค่าติดตั้งที่ไม่เหมาะสม.
- พิจารณาตั้งมาตรฐานเว็บบราวเซอร์ ที่มีอ็อพชันความปลอดภัยที่คุณต้องการ.
- สอนผู้ใช้ของคุณให้แจ้งคุณเกี่ยวกับพฤติกรรมใดๆ ที่น่าสงสัย หรืออาการที่อาจจะเกี่ยวข้องกับบางเว็บไซต์.

ความเสี่ยง: การเข้าถึงไดเร็กทอรี iSeries ผ่านทางไดรฟ์ที่ถูกแม็พเอาไว้

สมมติว่ามีพีซีตัวหนึ่งต่ออยู่กับเซิร์ฟเวอร์ด้วย IBM iSeries Access สำหรับเซสชัน Windows. เซสชันจะจัดเตรียมไดร์ฟที่ถูกแม็พเอาไว้ เพื่อลิงก์ไปยัง iSeries integrated file system. ตัวอย่างเช่น, ไดรฟ์ G ของพีซีอาจจะแม็พเข้ากับ integrated file system ของเซิร์ฟเวอร์ SYSTEM1 ที่อยู่ในเน็ตเวิร์ก.

ตอนนี้สมมุติว่าผู้ใช้พีซีเครื่องเดิม มีบราวเซอร์และสามารถใช้อินเตอร์เน็ตได้. ผู้ใช้ร้องขอเว็บเพจที่รัน "โปรแกรม" ที่เป็นอันตราย เช่น Java applet หรือ Active-X control. มีความเป็นไปได้, ที่โปรแกรมนั้นจะพยายามลบทุกอย่างบนไดร์ฟ G ของพีซี.

คุณมีหลายวิธีในการปกป้องความเสียหายของแม็พไดร์ฟ:

- การปกป้องที่สำคัญที่สุดก็คือการรักษาความปลอดภัยของรีซอร์สที่อยู่บนเซิร์ฟเวอร์ของคุณ. ตัว Java applet หรือ Active-X control จะดูเหมือนกับผู้ใช้ที่เป็นผู้สร้างเซสชันของพีซีขึ้น. คุณจะต้องจัดการอย่างระมัดระวังว่าผู้ใช้พีซีใดที่จะได้รับอนุญาตให้ทำงานบนระบบของคุณ.
- แนะนำผู้ใช้พีซีของคุณให้ตั้งค่าบราวเซอร์ะเพื่อป้องกันการพยายามที่จะเข้าถึงไดรฟ์ที่ถูกแม็พเอาไว้. ซึ่งวิธีนี้ใช้ได้กับ Java applet แต่ใช้ไม่ได้กับ Active-X control, ซึ่งไม่มีหลักการ sandbox.
- ให้ความรู้กับผู้ใช้ของคุณเกี่ยวกับอันตรายของการเชื่อมต่อไปยังเซิร์ฟเวอร์ของคุณและอินเตอร์เน็ตในเซสชันเดียวกัน. รวมทั้ง, ตรวจสอบให้แน่ใจว่าผู้ใช้พีซีของคุณ (พร้อมทั้ง ไคลเอ็นต์ที่ใช้Windows 95 , เป็นต้น) เข้าใจว่าไดรฟ์จะถูกแม็พเอาไว้ทั้งที่มีปรากฏว่าเซสชัน iSeries Access นั้นได้สิ้นสุดลงไปแล้ว?.

ความเสี่ยง: แอ็พเพล็ตที่ถูก sign ซึ่งได้รับการไว้วางใจ

ผู้ใช้ของคุณอาจทำตามคำแนะนำของคุณ และจัดเตรียมบราวเซอร์ของพวกเขา เพื่อป้องกันแอ็พเพล็ตจากการเขียนไปยังไดร์ฟของพีซี. อย่างไรก็ตาม, ผู้ใช้พีซีของคุณจำเป็นต้องระวังเกี่ยวกับ *แอ็พเพล็ตที่ถูก sign (signed applet)* ที่สามารถแทนที่ค่าติดตั้งสำหรับบราวเซอร์ของพวกเขา.

แอ็พเพล็ตที่ถูก sign มีลายเซ็นดิจิตอลที่เกี่ยวข้องเพื่อสร้างการรับรอง. เมื่อผู้ใช้เข้าถึงเว็บเพจที่มีแอ็พเพล็ตที่มีการ sign, ผู้ใช้จะมองเห็นข้อความหนึ่ง. ที่แสดงถึงลายเซ็นของแอ็พเพล็ต (ใครคือผู้ sign และเวลาที่ถูก sign). เมื่อผู้ใช้ของคุณยอมรับแอ็พเพล็ตนั้น, ผู้ใช้จะยอมให้แอ็พเพล็ตนั้นแทนที่ค่าติดตั้งความปลอดภัยสำหรับบราวเซอร์. แอ็พเพล็ตที่มีการ sign สามารถเขียนในโลคัลไดร์ฟของพีซี, แม้ว่าค่ากำหนดดีฟอลต์ของบราวเซอร์จะป้องกันไว้ก็ตาม. แอ็พเพล็ตที่ถูก sign สามารถทำการเขียนลงไปบนไดรฟ์ที่ถูกแม็พเอาไว้บนเซิร์ฟเวอร์ของคุณเนื่องจากไดรฟ์เหล่านั้นปรากฏว่าเป็นเสมือนโลคัลไดร์ฟต่อพีซี.

สำหรับแอ็พเพล็ต Java ของคุณเองที่มาจากเซิร์ฟเวอร์ของคุณ, คุณอาจจำเป็นที่จะต้องใช้แอ็พเพล็ตที่ถูก sign เอาไว้. อย่างไรก็ตาม, คุณควรสอนผู้ใช้ของคุณว่า โดยปกติแล้วไม่ควรรับแอ็พเพล็ตที่ถูก sign จากต้นทางที่ไม่รู้จัก.

บทที่ 17. ข้อมูลที่เกี่ยวข้อง

Manuals

- *APPC Programming*, SC41-5443-00อธิบายในส่วนของการสนับสนุน advanced program-to-program communications (APPC) สำหรับระบบ iSeries. หนังสือนี้แนะนำในเรื่อง การพัฒนาแอ็พพลิเคชันโปรแกรม ที่ใช้ APPC และกำหนดสภาวะแวดล้อมของการสื่อสารสำหรับการสื่อสาร APPC. อันประกอบด้วย ข้อควรพิจารณาของแอ็พพลิเคชันโปรแกรม, ข้อกำหนดและคำสั่งในการตั้งค่า, การจัดการปัญหาสำหรับ APPC, และข้อควรพิจารณาเกี่ยวกับด้านเครือข่ายโดยทั่วไป. ดู iSeries Information Center CD-ROM.
- *AS/400 Internet Security: Protecting Your AS/400 from HARM in the Internet* Redbook, SG24-4929 อธิบายถึงประเด็นความปลอดภัย และความเสี่ยงที่เกี่ยวกับการเชื่อมต่อ iSeries ของคุณไปยังอินเตอร์เน็ต. ทั้งนี้ได้แสดงตัวอย่าง, คำแนะนำ, ข้อเสนอแนะและเทคนิคสำหรับแอพพลิเคชัน TCP/IP.
- *Backup and Recovery*, SC41-5304-07 และได้ให้ข้อมูลเกี่ยวกับการวางแผนกลยุทธ์ในการสำรองข้อมูลและการกู้คืน, การบันทึกข้อมูลจากระบบ, และ การกู้คืนระบบของคุณ. ดู iSeries Information Center. สำหรับข้อมูลเพิ่มเติมเกี่ยวกับหัวข้อเหล่านี้ สามารถดูได้ใน iSeries Information Center เช่นกัน. โปรดดูที่ “สิ่งที่ต้องรู้ก่อนและข้อมูลที่เกี่ยวข้อง” ในหน้า xiii สำหรับรายละเอียดเพิ่มเติม.
- *CL Programming*, SC41-5721-06, ได้ให้คำอธิบายไว้โดยละเอียดสำหรับการเขียนโปรแกรม data description specifications (DDS) สำหรับไฟล์ที่สามารถอธิบายได้จากภายนอก. ไฟล์เหล่านี้คือ ฟิสิคัลไฟล์, ลอจิคัลไฟล์, ไฟล์แสดงผล, ไฟล์พิมพ์, และไฟล์ intersystem communication function (ICF). ดู iSeries Information Center.
- หัวข้อ CL ใน Information Center (โปรดดูที่ “สิ่งที่ต้องรู้ก่อนและข้อมูลที่เกี่ยวข้อง” ในหน้า xiii สำหรับรายละเอียดเพิ่มเติม.) ได้กล่าวถึงรายละเอียดของ iSeries control language (CL) และคำสั่งOS/400 ทั้งหมด. การใช้คำสั่ง OS/400 ในการเรียกใช้ฟังก์ชันของโปรแกรมไลเซนส์ Operating System/400® (5722-SS1). คำสั่ง non-OS/400 CL ทั้งหมด--ที่เชื่อมโยงกันกับไลเซนส์โปรแกรมอื่นๆ, รวมไปถึงภาษา และยูทิลิตีต่างๆ--ได้ถูกอธิบายเอาไว้ในหนังสือคู่มือเล่มอื่นๆ ที่สนับสนุนการใช้ไลเซนส์โปรแกรมเหล่านั้น.
- *Implementing iSeries Security, 3rd Edition* โดย Wayne Madden และ Carol Woodbury. Loveland, Colorado: 29th Street Press, a division of Duke Communications International, 1998. ได้ให้คำแนะนำ และข้อเสนอแนะในทางปฏิบัติ สำหรับการวางแผน, การติดตั้ง, และการจัดการเกี่ยวกับการรักษาความปลอดภัยให้กับ iSeries.

  ISBN Order Number:

  1-882419-78-2
- สำหรับข้อมูลเพิ่มเติมเกี่ยวกับเซิร์ฟเวอร์ HTTP, โปรดดูที่ URL ดังต่อไปนี้:

  `http://www.ibm.com/eserver/iseries/software/http/docs/doc.htm`
- *iSeries Security Reference*, SC41-5302-07, ให้ข้อมูลที่สมบูรณ์เกี่ยวกับค่ากำหนดของระบบที่เกี่ยวกับการรักษาความปลอดภัย, โปรไฟล์ผู้ใช้, ความปลอดภัยของรีซอร์ส, และการ

ตรวจสอบความปลอดภัย. คู่มือนี้ไม่ได้อธิบายถึงความปลอดภัยสำหรับโปรแกรมไลเซนส์, ภาษา, และยูทิลิตีเฉพาะ.ดู iSeries Information Center.

- หัวข้อ "ปฏิบัติการของระบบในระดับต้น" ใน Information Center ได้กล่าวถึงรายละเอียดของแนวคิดและภารกิจหลักๆ ที่จำเป็นสำหรับปฏิบัติการระดับต้นของ iSeries basic operations. โปรดดูที่ "สิ่งที่ต้องรู้ก่อนและข้อมูลที่เกี่ยวข้อง" ในหน้า xiii สำหรับข้อมูลเพิ่มเติม.
- Information Center อธิบายถึงวิธีใช้และการตั้งค่า TCP/IP และแอพพลิเคชัน TCP/IP ต่างๆ, ได้แก่ FTP, SMTP, และ TELNET. โปรดดูที่ "สิ่งที่ต้องรู้ก่อนและข้อมูลที่เกี่ยวข้อง" ในหน้า xiii สำหรับรายละเอียดเพิ่มเติม.
- *TCP/IP File Server Support for OS/400 Installation and User's Guide*, SC41-0125, ให้ข้อมูลเบื้องต้น, ขั้นตอนการติดตั้ง, และวิธีการจัดเตรียมสำหรับโปรแกรมไลเซนส์ File Server Support. มีการอธิบายถึงฟังก์ชันที่มากับผลิตภัณฑ์ และมีตัวอย่างและข้อเสนอแนะสำหรับการใช้ฟังก์ชันนี้ในระบบอื่น.
- *Trusted Computer Systems Evaluation Criteria* DoD 5200.28.STD, อธิบายถึงเกณฑ์สำหรับระดับการไว้ใจได้สำหรับระบบคอมพิวเตอร์. TCSEC เป็นเอกสารของรัฐบาลสหรัฐอเมริกา. อาจขอทำสำเนาได้จาก:

  Office of Standards and Products
  National Computer Security Center
  Fort Meade, Maryland 20755-6000 USA
  Attention: Chief, Computer Security Standards
- Information Center มีหัวข้อต่างๆ เกี่ยวกับการจัดการระบบ และการจัดการระบบงานบน iSeries. ในบางหัวข้อจะรวมไปถึงการรวบรวมข้อมูลทางด้านประสิทธิภาพ, การจัดการค่ากำหนดของระบบ, และการจัดการหน่วยความจำ. สำหรับรายละเอียดเกี่ยวกับการเข้าถึง Information Center, โปรดดูที่ "สิ่งที่ต้องรู้ก่อนและข้อมูลที่เกี่ยวข้อง" ในหน้า xiii. การจัดการระบบงาน,SC41-5306-03, ให้ข้อมูลเกี่ยวกับวิธีการสร้างและเปลี่ยนแปลงสภาวะแวดล้อมในการจัดการระบบงาน. ดู iSeries Information Center.

นอกเหนือไปจากหัวข้อเหล่านี้ใน Information Center และคู่มือเพิ่มเติมแล้ว, คุณสามารถใช้รีซอร์สเพื่อการช่วยเหลือดังต่อไปนี้:

- **IBM SecureWay**
  IBM SecureWay ให้แบรนด์ทั่วไปสำหรับพอร์ตแบรนด์ไอบีเอ็มของข้อเสนอความปลอดภัย; ฮาร์ดแวร์, ซอฟต์แวร์, การให้คำปรึกษาและบริการ เพื่อช่วยเหลือลูกค้าในการรักษาความปลอดภัยในเทคโนโลยีสารสนเทศของพวกเขา. ไม่ว่าจะเป็นเพียงความต้องการเฉพาะบุคคล หรือการสร้างโซลูชันในระดับองค์กรทั้งหมด,IBM SecureWay ให้ความรู้ความชำนาญที่ต้องการในการวางแผน, ออกแบบ, การปฏิบัติงานโซลูชันด้านความปลอดภัยสำหรับธุรกิจ. สำหรับข้อมูลเพิ่มเติมเกี่ยวกับ IBM SecureWay offerings, เยี่ยมชมได้ที่โฮมเพจ IBM SecureWay:

  `http://www.ibm.com/secureway`
- **บริการที่นำเสนอ**
  การติดตั้งฮาร์ดแวร์หรือซอฟต์แวร์ใหม่ สามารถพัฒนาในส่วนของประสิทธิภาพและการดำเนินธุรกิจของคุณได้อย่างถึงที่สุด. แต่ก็ยังก่อให้เกิดสิ่งที่ต้องกังวลในเรื่องของความวุ่นวายและ downtime ของธุรกิจ,และอาจจะมีผลกระทบต่อรีซอร์สภายในที่มีคุณค่าของคุณอีกด้วย. IBM

Global Services มีบริการเกี่ยวกับการรักษาความปลอดภัย iSeries. เว็บไซต์ดังต่อไปนี้อนุญาตให้คุณค้นหารายการการให้บริการโดยสมบูรณ์สำหรับ iSeries ของคุณ :

`http://www.as.ibm.com/asus`

ประกาศ

ข้อมูลนี้ถูกพัฒนาขึ้นสำหรับผลิตภัณฑ์และบริการที่เสนอขายในประเทศสหรัฐอเมริกา.

IBM อาจจะไม่เสนอผลิตภัณฑ์, บริการ, หรือคุณลักษณะพิเศษที่กล่าวถึงในเอกสารนี้ ในประเทศอื่นๆ . ปรึกษาตัวแทนจำหน่าย IBMในท้องที่ สำหรับข้อมูลที่เกี่ยวกับผลิตภัณฑ์และบริการที่มีอยู่ในปัจจุบันในพื้นที่ของคุณ. การอ้างอิงใด ๆ ถึงผลิตภัณฑ์ IBM, โปรแกรม, หรือบริการไม่ได้มีเจตนาในการระบุหรือกล่าวถึงโดยนัยว่าต้องใช้ผลิตภัณฑ์, โปรแกรม หรือบริการดังกล่าวเท่านั้น. ผลิตภัณฑ์, โปรแกรม, หรือบริการใดๆ ที่สามารถทำงานได้เท่าเทียมกัน ที่ไม่ได้ละเมิดลิขสิทธิ์ทรัพย์สินทางปัญญาใดๆ ของ IBM จะถูกนำมาใช้แทนได้. อย่างไรก็ตาม, เป็นความรับผิดชอบของผู้ใช้ที่จะประเมินและตรวจสอบผลิตภัณฑ์, โปรแกรม, หรือบริการที่ไม่ใช่ของ IBM.

IBM อาจมีสิทธิบัตรหรือคำร้องขอมีสิทธิบัตรที่รออยู่ซึ่งจะครอบคลุมสิ่งที่ได้อธิบายไว้ในเอกสารนี้แล้ว. การตกแต่งเอกสารใหม่ไม่ได้ทำให้คุณได้สิทธิของสิทธิบัตรเหล่านั้น. คุณสามารถสอบถามเกี่ยวกับไลเซนส์, โดยเขียนและส่งไปที่:

IBM Director of Licensing
IBM Corporation
500 Columbus Avenue
Thornwood, NY 10594-1785
U.S.A.

สำหรับการสอบถามไลเซนส์เกี่ยวกับข้อมูล double-byte (DBCS) , ติดต่อแผนกทรัพย์สินทางปัญญาของIBM ในประเทศของคุณหรือส่งแบบสอบถามมาก็ได้, โดยการเขียน, ไปยัง:

IBM World Trade Asia Corporation
Licensing
2-31 Roppongi 3-chome, Minato-ku
Tokyo 106, Japan

ย่อหน้าต่อไปนี้ไม่ใช้กับประเทศสหราชอาณาจักร หรือประเทศอื่นที่สิ่งที่จัดหาให้ไม่สอดคล้องกับกฎหมายท้องถิ่น: INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. บางรัฐไม่อนุญาตการปฏิเสธของการรับประกันอย่างชัดแจ้ง หรือโดยนัยในการทำการซื้อขายบางอย่าง, ดังนั้นประโยคข้างต้นนี้อาจไม่ได้มีความหมายต่อคุณ.

ข้อมูลนี้ได้รวมความไม่ถูกต้องทางเทคนิคหรือความผิดพลาดทางการพิมพ์. การเปลี่ยนแปลงข้อมูลในนี้จะมีเป็นระยะๆ ซึ่งจะสอดคล้องกับการตีพิมพ์ในครั้งใหม่. IBM อาจทำการปรับปรุงและ/หรือ การเปลี่ยนแปลงในผลิตภัณฑ์ และ/หรือ โปรแกรมที่ได้อธิบายไว้ในการพิมพ์ครั้งนี้เมื่อไรก็ได้โดยไม่มีการแจ้งให้ทราบ.

การอ้างถึงเว็บไซต์ที่ไม่ใช่ของ IBM นั้นถูกจัดหามาเพื่อความสะดวกเท่านั้น และไม่ได้มีการรับรองเว็บไซต์เหล่านั้น. เนื้อหาของเว็บไซต์เหล่านั้นไม่ใช่ส่วนหนึ่งของเนื้อหาสำหรับผลิตภัณฑ์ IBM นี้และการใช้เว็บไซต์เหล่านั้นก็จะตกเป็นความเสี่ยงของตัวคุณเอง.

IBM อาจใช้ หรือเผยแพร่ข้อมูลใดๆ ที่คุณให้ไว้ในทางที่ไอบีเอ็มเชื่อว่าเหมาะสมโดยไม่มีข้อผูกมัดใดๆ กับคุณ.

สำหรับผู้ที่มีไลเซนส์ของโปรแกรมนี้ที่ต้องการมีข้อมูลเกี่ยวกับโปรแกรมสำหรับจุดประสงค์ให้ทำงานได้: (i) การแลกเปลี่ยนข้อมูลระหว่างโปรแกรมที่ถูกสร้างขึ้นอย่างเป็นอิสระและโปรแกรมอื่น (รวมทั้งโปรแกรมนี้) และ (ii) การใช้ข้อมูลร่วมกันที่ซึ่งมีการแลกเปลี่ยน ควรติดต่อ:

IBM Corporation
Software Interoperability Coordinator, Department 49XA
3605 Highway 52 N
Rochester, MN 55901
U.S.A.

ข้อมูลเหล่านี้อาจมีให้โดยขึ้นอยู่กับเงื่อนไขและสถานการณ์ที่เหมาะสม, ซึ่งรวมถึงบางกรณี, เช่น การจ่ายค่าธรรมเนียม.

ไลเซนส์โปรแกรมที่อธิบายไว้ในข้อมูลนี้และเนื้อหาที่มีไลเซนส์ทั้งหมดที่มีอยู่นั้นจะถูกจัดให้อยู่ IBM ภายใต้คำว่า IBM Customer Agreement, IBM International Program License Agreement, หรือข้อตกลงใดๆ ที่เท่าเทียมกันระหว่างเราและท่าน.

ข้อมูลประสิทธิภาพใดๆ ที่มีอยู่ในนี้ถูกกำหนดอยู่ในสภาพแวดล้อมที่ถูกควบคุม. ดังนั้น, ผลที่ได้จากสภาพแวดล้อมของการปฏิบัติการอื่นอาจแตกต่างกันเป็นอย่างมาก. การวัดบางอย่างอาจถูกทำขึ้นบนระบบในระดับของการพัฒนา และไม่ได้มีการรับรองว่า การวัดเหล่านี้จะเหมือนกันบนระบบที่ใช้กันอยู่ทั่วไป. นอกเหนือจากนี้, การวัดบางอย่างอาจเป็นการประมาณผ่านทางการคาดการณ์. ซึ่งผลที่แท้จริงอาจแตกต่างกัน. ผู้ใช้เอกสารนี้ ควรทำการตรวจสอบข้อมูลที่ใช้ได้ สำหรับสภาพแวดล้อมเฉพาะของพวกเขา.

ข้อมูลเกี่ยวกับผลิตภัณฑ์ที่ไม่ใช่ของ IBM ได้รับมาจากซัพพลายเออร์ของผลิตภัณฑ์เหล่านั้น, การประกาศทางสาธารณชน หรือแหล่งที่เป็นของสาธารณะอื่นๆ . IBM ไม่ได้ทำการทดสอบผลิตภัณฑ์เหล่านั้น และไม่สามารถยืนยันความถูกต้องของประสิทธิภาพการทำงาน, การใช้แทนกันได้, หรือการเรียกร้องใดๆ ที่เกี่ยวข้องกับผลิตภัณฑ์ที่ไม่ได้เป็นของ IBM . คำถามเกี่ยวกับผลิตภัณฑ์ที่ไม่ใช่ของ IBM ควรถามไปที่ซัพพลายเออร์ของผลิตภัณฑ์เหล่านั้น.

ทุกประโยคที่มีการเป็นเรื่องของทิศทางในอนาคตหรือความตั้งใจของ IBM อาจมีการเปลี่ยนแปลงหรือถอดถอนโดยไม่ต้องมีการแจ้งให้ทราบ, และเป็นการแสดงถึงจุดมุ่งหมายและวัตถุประสงค์เท่านั้น.

ข้อมูลนี้ไว้สำหรับวัตถุประสงค์ของการวางแผนเท่านั้น. ข้อมูลในนี้อาจมีการเปลี่ยนแปลง ก่อนที่ผลิตภัณฑ์ที่อธิบายนั้นมีวางจำหน่าย.

ข้อมูลนี้มีตัวอย่างของข้อมูลและรายงานที่ใช้ในการปฏิบัติงานประจำวัน. เพื่อแสดงให้เห็นอย่างสมบูรณ์ที่สุดที่เป็นไปได้, ตัวอย่างเหล่านี้ประกอบด้วย ชื่อของแต่ละราย, ชื่อของบริษัท, ตราสินค้า และผลิตภัณฑ์. ชื่อทั้งหมดเหล่านี้ถูกทำขึ้น และคล้ายคลึงกับชื่อและที่อยู่ของหน่วยธุรกิจจริงๆ .

COPYRIGHT LICENSE:

ข้อมูลนี้ประกอบด้วยโปรแกรมแอพพลิเคชันตัวอย่างในภาษาต้นฉบับ (source language), ซึ่งแสดงเทคนิคของโปรแกรมบนระบบปฏิบัติการที่หลากหลาย. คุณสามารถทำสำเนา, เปลี่ยนแปลง, และจำหน่ายโปรแกรมตัวอย่างเหล่านี้ในรูปแบบต่างๆ โดยไม่จำเป็นต้องชำระเงินให้กับ IBM, สำหรับจุดประสงค์ในการพัฒนา, การใช้, การทำการตลาด หรือการจัดจำหน่ายแอ็พพลิเคชันโปรแกรมที่ใช้กับ application programming interface สำหรับแพล็ตฟอร์มระบบปฏิบัติการที่โปรแกรมตัวอย่างได้ถูกพัฒนาขึ้น. ตัวอย่างเหล่านี้ ไม่ได้ผ่านการทดสอบภายใต้ทุกสถานการณ์. IBM, ดังนั้น, ไม่สามารถรับประกันหรือกล่าวเป็นนัยถึงความเชื่อถือได้, การให้บริการได้, หรือฟังก์ชันของโปรแกรม เหล่านี้. คุณสามารถทำสำเนา, แก้ไข, และจัดจำหน่ายโปรแกรมตัวอย่างเหล่านี้ในรูปแบบใดๆ โดยไม่มีการชำระเงินให้กับ IBM สำหรับจุดประสงค์ในการพัฒนา, การใช้งาน, การทำการตลาด, หรือแอ็พพลิเคชันโปรแกรมนี้ที่มีการปรับเข้ามาตรฐานแบบกระจายให้เข้ากับอินเตอร์เฟสแอ็พพลิเคชันโปรแกรมของ IBM ได้.

ถ้าคุณกำลังดูสำเนาชั่วคราว (softcopy) ของข้อมูล, ภาพหรือสีที่แสดงอาจไม่ปรากฏ.

เครื่องหมายการค้า (Trademark)

คำ (term) ต่อไปนี้ เป็นเครื่องหมายการค้าของ International Business Machines Corporation ในประเทศสหรัฐอเมริกา, หรือในประเทศอื่น, หรือทั้งสองกรณี:

Advanced Peer-to-Peer Networking
APPN
AS/400
DB2
DRDA
e (logo)
IBM
iSeries
Net.Data
Operating System/400
OS/400
PowerPC
SecureWay
System/36
System/38
400

ActionMedia, LANDesk, MMX, Pentium, และ ProShare เป็นเครื่องหมายการค้า หรือเครื่องหมายการค้าจดทะเบียนของ Intel Corporation ในประเทศสหรัฐอเมริกา, ประเทศอื่น, หรือทั้งคู่.

Microsoft, Windows, Windows NT, และ Windows logo เป็นเครื่องหมายการค้าของ Microsoft Corporation ในประเทศสหรัฐอเมริกา, ประเทศอื่น, หรือทั้งคู่.

Java และเครื่องหมายการค้าที่เกี่ยวกับ Java ทั้งหมดเป็นเครื่องหมายการค้าของ Sun Microsystems, Inc. ในประเทศสหรัฐอเมริกา, ประเทศอื่น, หรือทั้งคู่.

UNIX เป็นเครื่องหมายการค้าจดทะเบียนของ The Open Group ในสหรัฐอเมริกา และประเทศอื่น.

ชื่ออื่นๆ ของบริษัท, ผลิตภัณฑ์, และการบริการ อาจเป็นเครื่องหมายการค้า หรือเครื่องหมายการบริการของผู้อื่น.

ดัชนี

อักขระพิเศษ

ตัวเลข

A

B

C

D

E

F

G

H

I

J

L

M

N

O

P

Q

R

S

T

U

V

W

ความคิดเห็นจากผู้อ่าน — เราต้องการฟังความคิดเห็นจากคุณ

iSeries
คำแนะนำและทูลในการรักษาความปลอดภัยให้กับเซิร์ฟเวอร์ iSeries
เวอร์ชัน 5

หมายเลขสิ่งตีพิมพ์ SC09-3448-03

กรุณาตอบแบบสอบถามข้อคิดเห็นนี้ เพื่อช่วยให้ไอบีเอ็มตอบสนองต่อความต้องการของคุณได้ดียิ่งขึ้น

โดยรวมแล้ว, คุณพึงพอใจเพียงไรกับข้อมูลในหนังสือเล่มนี้

	พึงพอใจมาก	พึงพอใจ	เฉยๆ	ไม่พอใจ	ไม่พอใจมาก
ความพึงพอใจโดยรวม	☐	☐	☐	☐	☐

คุณพึงพอใจเพียงไรกับข้อมูลในหนังสือเล่มนี้

	พึงพอใจมาก	พึงพอใจ	เฉยๆ	ไม่พอใจ	ไม่พอใจมาก
ความถูกต้อง	☐	☐	☐	☐	☐
ความสมบูรณ์	☐	☐	☐	☐	☐
ความง่ายในการค้นหา	☐	☐	☐	☐	☐
ความง่ายในการเข้าใจ	☐	☐	☐	☐	☐
การจัดเรียงลำดับ	☐	☐	☐	☐	☐
การมีส่วนช่วยในงานของคุณ	☐	☐	☐	☐	☐

โปรดแนะนำเราในการทำหนังสือเล่มนี้ให้ดีขึ้น:

_____

_____

_____

_____

ขอขอบคุณสำหรับความคิดเห็นของคุณ คุณจะอนุญาตให้เราติดต่อคุณได้หรือไม่ ? ☐ ได้ ☐ ไม่ได้

เมื่อคุณส่งความคิดเห็นให้กับไอบีเอ็ม, เท่ากับว่าคุณได้ให้สิทธิ์ต่อไอบีเอ็มในการใช้หรือส่งต่อความคิดเห็นของคุณด้วยวิธีการใดๆ ที่ไอบีเอ็มคิดว่าเหมาะสมโดยไม่ต้องมีพันธะผูกพันต่อคุณ.

_____ _____

ชื่อ ที่อยู่

_____ _____

บริษัทหรือองค์กร

_____ _____

หมายเลขโทรศัพท์

(โปรดส่งข้อมูลนี้กลับมายังศูนย์ลูกค้าสัมพันธ์, บริษัท ไอบีเอ็ม ประเทศไทย จำกัด, โทรสาร: 0-2273-0188 หรือตามที่อยู่ในหน้าถัดไป)

ความคิดเห็นจากผู้อ่าน — เราต้องการฟังความคิดเห็นจากคุณ

SC09-3448-03

ตัดหรือพับตามเส้นนี้

พับและปิดผนึก **กรุณาหลีกเลี่ยงการเย็บลวด** พับและปิดผนึก

กรุณาติด
ตรา
ไปรษณียากร
ที่นี่

ศูนย์ลูกค้าสัมพันธ์
บริษัท ไอบีเอ็ม ประเทศไทย จำกัด
388 ถนนพหลโยธิน พญาไท
กรุงเทพฯ
10400

พับและปิดผนึก **กรุณาหลีกเลี่ยงการเย็บลวด** พับและปิดผนึก

ตัดหรือพับตามเส้นนี้

พิมพ์ในสหรัฐอเมริกา

SC09-3448-03