IBM

eserver

iSeries

iSeries biztonsági tanácsok és technikák

5. verzió

SC22-5311-07

IBM

@server

iSeries

iSeries biztonsági tanácsok és technikák

5. verzió

SC22-5311-07

Megjegyzés

Mielőtt a jelen leírást és a vonatkozó terméket használná, feltétlenül olvassa el a “Megjegyzések” oldalszám: 163 helyen lévő tájékoztatót.

Nyolcadik kiadás (2004. április)

Ez a kiadás a V5R3M0 szintű IBM Operating System/400 (száma: 5722-SS1) termékre és minden azt követő változatra és módosításra vonatkozik, amíg ez másképpen nincs jelezve. Ez a verzió nem fut minden csökkentett utasításkészletű (RISC) rendszeren és CISC modellen.

Ez a kiadás az SC22-5311-06 kiadványt váltja fel.

Tartalom

Ábrák

Táblázatok:

Néhány szó az iSeries biztonsági tanácsok és technikák (SC22-5311-07) című kiadványról

A számítógépeknek a különféle szervezetekben betöltött szerepe napjainkban gyors változáson megy keresztül. Az IT szakembereknek, szoftver szállítóknak és biztonsági adminisztrátoroknak újból szemügyre kell venniük sok olyan területet, amelyre korábban esetleg csak legyintettek egyet. Az iSeries biztonságának mindenképpen bele kell esnie ebbe a körbe.

Ezek a rendszerek a hagyományos könyvelési és nyilvántartási alkalmazásoktól igencsak eltérő funkciókkal gazdagodtak. A felhasználók is új módszerekkel léphetnek be a rendszerre: helyi hálózaton, kapcsolt vonalakon, vezetéknélküli kapcsolatokon és még sok más hálózattípuson. A felhasználók gyakran nem is találkoznak a bejelentkezési képernyővel. Egyre több szervezet válik “kiterjesztett vállalattá”, akár saját hálózatok, akár az Internet felhasználásával.

Mindezek következtében a rendszerek tulajdonképpen egy sor új ablakot és ajtót nyitnak a világ felé. A rendszerek fenntartóinak és a biztonsági adminisztrátoroknak egyaránt figyelniük kell az információs tulajdon megfelelő védelmére napjaink folyamatosan változó környezetében.

Ebben a kiadványban számos praktikus javaslat olvasható az iSeries biztonsági szolgáltatásainak használatáról és a biztonsági követelményeknek megfelelő eljárások létrehozásáról. A kiadvány ajánlásai átlagos biztonsági követelményekkel és kockázatokkal rendelkező környezetre érvényesek. Az iSeries biztonsági szolgáltatásainak teljes körű tárgyalása meghaladja jelen kiadványunk kereteit. Ha a megadottnál több lehetőségről kíván olvasni, vagy részletesebb háttérinformációkat igényel, akkor nézze meg a 17. fejezet, “Kapcsolódó információk”, oldalszám: 161 szakaszban megadott kiadványokat.

A kiadvány leírja az OS/400 biztonsági eszközeinek beállítását és használatát is. A biztonsági eszközökre vonatkozó referenciainformációkat a 4. fejezet, “iSeries beállítása a Biztonsági eszközök használatára”, oldalszám: 29 és a “Biztonsági parancsok parancsnevei és menüi” oldalszám: 30 szakaszokban találja. A kiadvány az eszközök használatára példákat is bemutat.

Kiknek szól ez a könyv?

A könyv a rendszer biztonságáért felelős **adatvédelmi megbízottnak** vagy **biztonsági adminisztrátornak** szól. A felelősség általában a következő feladatok végrehajtásával jár együtt:

- Felhasználói profilok beállítása és kezelése
- A biztonságra vonatkozó rendszerszintű értékek beállítása
- Objektumokra vonatkozó jogosultságok felügyelete
- Biztonsági stratégiák betartatása és megfigyelése

A könyvet iSeries rendszerekért felelős biztonsági adminisztrátoroknak ajánljuk. A kiadványban megadott útmutatások feltételezik a következőket:

- Ismeri az iSeries használatával kapcsolatos alapvető eljárásokat, például a bejelentkezést és a parancsok használatát.
- Ismeri az iSeries biztonságának alapelemeit, úgymint a biztonsági szinteket, biztonsággal kapcsolatos rendszerváltozókat, a felhasználói profilokat és az objektum biztonságot.

Megjegyzés: Ezeket az elemeket a 1. fejezet, “Az iSeries biztonságának alapvető elemei”, oldalszám: 3 szakasz ismerteti. Az alapelemek ismeretének hiányában olvassa el az iSeries Információs központ *Alapvető biztonság és tervezés* témakörét. További részletek: “Előfeltétel és kapcsolódó információk”.

- A biztonsági szint (QSECURITY) rendszerváltozó legalább 30-as beállításával aktiválta a rendszer biztonságát.

Az IBM folyamatosan fejleszti az iSeries biztonsági képességeit. A továbbfejlesztések által nyújtott előnyök kihasználása érdekében rendszeresen vizsgálja meg az adott kiadáshoz rendelkezésre álló összesített javítócsomagot, hogy az milyen biztonsággal kapcsolatos javításokat tartalmaz.

A kiadvány használata

Ha nem állította be a rendszert a biztonsági eszközök használatára, vagy a Security ToolKit for OS/400 egy korábbi kiadáshoz készült változata van telepítve, akkor tegye a következőket:

1. Kezdje a 2. fejezet, “iSeries biztonsági varázsló és eServer biztonsági tervező”, oldalszám: 11 helyen. Ez a szakasz írja le, hogyan használhatók az említett szolgáltatások az adott környezet számára javasolt biztonsági eszközök kiválasztására, és ezek használatba vételére.
2. További biztonsági információkért áttekintheti az iSeries Információs központban online elérhető Security Reference című kiadványt.

Megjegyzés

Jelen kiadvány *jelentős mennyiségű* javaslatot tárgyal az iSeries biztonságával kapcsolatban. Az adott rendszer elképzelhető, hogy csak bizonyos területeken igényel védelmet. A kiadvány alapján ismerje meg a lehetséges biztonsági kockázatokat és ezek ellenszerét. Ezután koncentrálja erőfeszítéseit a rendszer szempontjából leginkább kritikus területekre.

Előfeltétel és kapcsolódó információk

Az iSeries technikai információk keresésének kiindulópontjaként használja az iSeries Információs központot.

Az Információs központ kétféleképpen érhető el:

- A következő Internet címen:

  `http://www.ibm.com/eserver/iseries/infocenter`
- Az *iSeries Információs központ*, SK3T-0524-04 CD lemezről. A CD-ROM az új iSeries hardverrel vagy az IBM Operating System/400 szoftver megrendeléssel érkezik. A CD lemezt megrendelheti az IBM Publications Center címén is:

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

Az iSeries Információs központ új és frissített iSeries információkat tartalmaz a következőkről: szoftver és hardver telepítés, Linux, WebSphere, Java, magas rendelkezésre állás, adatbázis, logikai partíciók, CL parancsok és alkalmazásprogramozási csatolók (API). Ezen túlmenően tanácsadó és kereső eszközöket biztosít az iSeries hardver és szoftver tervezéséhez, hibakereséséhez és beállításához.

Minden hardver megrendeléshez hozzátartozik az *iSeries telepítési és üzemeltetési CD-ROM*, SK3T-7336-02 is. A CD-ROM tartalma: IBM **@server** IBM e(logo)server iSeries Access for Windows és EZ-Setup varázsló. Az iSeries Access Family hatékony kliens és szerver

képességek biztosításával nyújt lehetőséget a személyi számítógépek és az iSeries szerverek összekapcsolásához. Az EZ-Setup varázsló automatizál számos iSeries beállítási feladatot.

Megjegyzések küldése

Visszajelzése nagy segítséget nyújt számunkra ahhoz, hogy a legmegfelelőbb és a legjobb minőségű információkat tudjuk biztosítani. Ha bármilyen megjegyzése van ezzel a könyvvel, vagy bármely más iSeries dokumentációval kapcsolatban, akkor töltse ki a könyv hátuljában található olvasói megjegyzések űrlapot.

- Ha a megjegyzéseit levélben kívánja eljuttatni hozzánk, akkor az olvasói megjegyzések űrlapot a könyv hátulján található címre küldje. Ha az Egyesült Államokon kívüli országból küldi az olvasói feljegyzést, akkor a megjegyzéseit a helyi IBM telephelynek vagy IBM képviselőnek is feladhatja.
- Ha a megjegyzéseit faxon kívánja elküldeni, akkor az alábbi számok állnak a rendelkezésére:
  - Egyesült Államok, Kanada és Puerto Rico: 1-800-937-3430
  - Más országok: 1-507-253-5192
- A megjegyzések elektronikus elküldésénél az alábbi e-mail címeket használhatja:
  - Könyvekkel kapcsolatos megjegyzések:

    RCHCLERK@us.ibm.com
  - Az iSeries Információs központtal kapcsolatos megjegyzések:

    RCHINFOC@us.ibm.com

Ne felejtse ki a következőket:

- A könyv címe vagy az iSeries Információs központ témaköre.
- A könyv kiadási száma.
- Az oldalszám vagy a téma, amelyre a megjegyzés vonatkozik.

1. rész iSeries biztonsági alapelemek

1. fejezet Az iSeries biztonságának alapvető elemei

Ez a témakör röviden bemutatja azokat az alapelemeket, amelyek együttműködése nyújtja az iSeries biztonságát. A biztonsági elemeknek az alapokon túlmenő tárgyalása, alkalmazása és a hozzájuk kapcsolódó tanácsok a könyv más részeiben találhatók.

Biztonsági szintek

A biztonsági szint (QSECURITY) rendszerváltozó beállításával adhatja meg, hogy a rendszernek milyen szintű biztonsági intézkedéseket kell foganatosítania. A rendszer öt biztonsági szintet nyújt:

10-es szint:

A rendszer semmiféle biztonságot nem foganatosít. Jelszó nem szükséges. Ha a megadott felhasználói profil nem létezik a rendszeren a bejelentkezéskor, akkor a rendszer létrehozza azt.

FIGYELEM:

A V4R3 kiadással kezdődően a QSECURITY rendszerváltozó nem állítható a 10-es szintre. Ha a rendszeren a biztonsági szint értéke jelenleg 10, akkor ez változatlan marad a V4R3 kiadás telepítésekor. Ha azonban a biztonsági szintet ettől eltérő értékre állítja, akkor az a későbbiekben már nem állítható vissza 10-re. Mivel a 10-es szint nem biztosít semmiféle védelmet, az IBM nem javasolja ennek használatát. Az **IBM a 10-es biztonsági szinten bekövetkezett problémákra vonatkozóan semmiféle támogatást nem nyújt, kivéve, ha a probléma magasabb biztonsági szinteken is előáll.**

20-as szint:

A rendszer a bejelentkezéshez felhasználói azonosítót és jelszót kér. A 20-as biztonsági szintet éppen ezért **bejelentkezési biztonságnak** is hívják.Alapértelmezésben minden felhasználó hozzáfér minden objektumhoz, mivel minden felhasználó rendelkezik az *ALLOBJ speciális jogosultsággal.

30-as szint:

A rendszer a bejelentkezéshez felhasználói azonosítót és jelszót kér. A felhasználóknak jogosultsággal kell rendelkezniük az objektumokhoz, mivel alapértelmezésben semmilyen jogosultságuk nincs. Ezt a szintet **erőforrás biztonságnak** is nevezik.

40-es szint:

A rendszer a bejelentkezéshez felhasználói azonosítót és jelszót kér. Az erőforrás biztonságon felül a rendszer **integritásvédelmi** funkciókat is biztosít. Az integritásvédelmi funkciók, például az operációs rendszer illesztőinek átadott paraméterek ellenőrzése a rendszert és az objektumokat is védi a tapasztalt felhasználók matatásaival szemben. A legtöbb környezetben a 40-es az ajánlott biztonsági szint. V4R5 vagy újabb kiadást futtató új iSeries rendszer kézhez vételekor a biztonsági szint 40-re van állítva.

50-es szint:

A rendszer a bejelentkezéshez felhasználói azonosítót és jelszót kér. A rendszer az erőforrás biztonságot és a 40-es szint integritásvédelmét is foganatosítja, de ezt kiegészíti egy **kiterjesztett integritásvédelemmel** is, amely megakadályozza

például a felhasználói- és rendszerprogramok közötti üzenettovábbítást. Az 50-es biztonsági szint a magas biztonsági követelményekkel rendelkező iSeries rendszereken ajánlott.

Megjegyzés: Az 50-es szint szükséges a C2 (és FIPS-140) tanúsítvány megszerzéséhez.

A biztonsági szintekről, illetve az ezek közti átmenetekről további információkat az *iSeries biztonsági összefoglaló* című kiadvány 2. fejezetéből szerezhet.

Globális beállítások

A rendszer különféle globális beállításokkal határozza meg, hogyan léphetnek be a jobok a rendszerbe, és a rendszer miként jelenik meg a többi rendszer felhasználói számára. Ilyen beállítások például a következők:

Biztonságra vonatkozó rendszerváltozók:
A biztonságra vonatkozó rendszerváltozók felügyelik a rendszer biztonságát. Ezek a változók négy csoportra oszthatók:
- Általános biztonsági rendszerváltozók
- Biztonságra vonatkozó egyéb rendszerváltozók
- Jelszavakra vonatkozó rendszerváltozók
- Megfigyelést irányító rendszerváltozók

Az adott rendszerváltozók biztonsági következményeit jelen könyv több témaköre is tárgyalja. A biztonsággal kapcsolatos rendszerváltozók összefoglaló listáját az *iSeries biztonsági összefoglaló* című kiadvány tartalmazza.

Hálózati attribútumok:
A hálózati attribútumok határozzák meg, hogyan vesz részt (vagy különül el) a rendszer a hálózatokban. A hálózati attribútumokról további részleteket a *Work Management* című kiadványban olvashat.

Alrendszerleírások és más jobkezelési elemek:
A jobkezelési elemek határozzák meg, hogy a jobok hogyan lépnek be a rendszerbe, és ott milyen környezetben futnak. Bizonyos jobkezelési beállítások biztonsági következményeivel a könyv több helyen is foglalkozik. Összefoglaló információkat a *Work Management* című könyv nyújt.

Kommunikációs konfiguráció:
Bizonyos kommunikációs beállítások szintén hatással vannak a jobok rendszerbe lépésének módjára. A kiadvány több témakörében is találhat a rendszer hálózati részvételével kapcsolatos tanácsokat.

Felhasználói profilok

A rendszer minden felhasználójának rendelkeznie **kell** egy felhasználói profillal. A felhasználói profilt létre kell hozni, mielőtt a felhasználó bejelentkezhetne a rendszerre. A felhasználói profilok emellett használhatók a különféle szolgáltatásokra, például a lemeztömbökre vagy főtár kiírásokra vonatkozó hozzáférés felügyeletére is. További információkat a “Szervizeszközök kezelése” oldalszám: 62 szakaszban talál.

A felhasználói profil erőteljes és rugalmas eszköz. Felügyeli, hogy a felhasználó mit tehet meg a rendszeren, illetve segítségével meghatározható, hogy milyen legyen a rendszer megjelenése a felhasználó szemszögéből. A felhasználói profilok paramétereinek összefoglaló listáját az *iSeries biztonsági összefoglaló* című kiadvány tartalmazza.

Csoport profilok

A csoport profilok különleges felhasználói profilnak tekinthetők. Csoport profil segítségével felhasználók csoportjainak határozható meg a jogosultsága, nem pedig külön-külön az egyedi felhasználóknak. A csoport profilok emellett a profil másolási funkcióval felhasználhatók sablonként egyedi felhasználói profilok létrehozásakor, és az iSeries navigátorban a biztonsági stratégiák menü segítségével szerkesztheti a felhasználói jogosultságokat.

A csoport profilok tervezéséről és használatáról további információkkal az *iSeries biztonsági összefoglaló* kiadvány 5. és 7. fejezete szolgál.

Erőforrás biztonság

A rendszeren alkalmazott erőforrás biztonság határozza meg, hogy ki használhatja az objektumokat és hogyan. Egy objektum elérésének képességét nevezzük **jogosultságnak**. Az objektum jogosultságok beállításakor figyelmesen kell eljárni ahhoz, hogy a felhasználóknak legyen elegendő jogosultságuk a munkájuk elvégzéséhez, mindazonáltal ne legyenek jogosultak a rendszer teljes körű böngészésére vagy módosítására. Az objektum jogosultságok adnak engedélyt a felhasználónak egy adott objektumra vonatkozóan, és határozzák meg, hogy a felhasználó milyen műveleteket hajthat végre az objektumon. Az objektum erőforrások részletes felhasználói jogosultságokkal, például rekordok hozzáadására vagy módosítására vonatkozó engedélyekkel korlátozhatók. A rendszer erőforrások segítségével a felhasználóknak bizonyos rendszer által meghatározott jogosultság részhalmazok adhatók: *ALL, *CHANGE, *USE és *EXCLUDE.

Az erőforrás biztonság védelmét igénylő leggyakoribb rendszerobjektumok a fájlok, programok, könyvtárak és katalógusok, bár jogosultság a rendszer tetszőleges egyedi objektumára vonatkozóan megadható.

Az objektum jogosultságok kialakításának fontosságát a 5. fejezet, “Információs tulajdon védelme objektum jogosultságokkal” szakasz tárgyalja. Az erőforrás biztonság beállítására vonatkozó lehetőségeket az *iSeries biztonsági összefoglaló* című kiadvány 5. fejezete írja le.

Program funkciók elérésének korlátozása

A program funkciók elérésének korlátozása lehetővé teszi az olyan programok védelmét is, amelyekhez nem tartozik iSeries objektum, amelyet védeni lehetne. Mielőtt a program funkciók elérésének korlátozása megjelent volna a V4R3 kiadásban, ehhez jogosultsági listát vagy más objektumot kellett létrehozni, és a program funkciójára vonatkozó hozzáférést a létrehozott objektum jogosultságainak ellenőrzésével lehetett felügyelni. A program funkciók elérésének korlátozásával könnyedén felügyelheti egy alkalmazás, egy alkalmazás valamely része vagy egy bizonyos program funkciójának elérését.

A felhasználóknak az alkalmazások funkcióira vonatkozó hozzáférését kétféleképpen kezelheti az iSeries navigátorban. Az első módszer az Alkalmazás adminisztrációt használja.

1. Kattintson a jobb egérgombbal a módosítani kívánt funkciót tartalmazó rendszeren.
2. Válassza az előugró menü **Alkalmazás adminisztráció** menüpontját.
3. Ha az adminisztrációs rendszeren van, akkor válassza a **Helyi beállítások** elemet. Ellenkező esetben folytassa a következő lépéssel.
4. Válasszon ki egy adminisztrálható funkciót.
5. Az igénynek megfelelően válassza ki az **Alapértelmezett hozzáférés** beállítást. Ennek kiválasztásával alapértelmezésben valamennyi felhasználó hozzáférhet a funkcióhoz.

6. Az igénynek megfelelően válassza ki a **Minden objektum elérése** beállítást. Ennek kiválasztása esetén a funkció csak az *ALLOBJ jogosultsággal rendelkező felhasználók számára használható.
7. Az igénynek megfelelően válassza ki a **Testreszabás** beállítást. A **Hozzáférés testreszabása** párbeszédablak **Hozzáadás** és **Eltávolítás** gombjaival vehet fel és távolíthat el felhasználókat vagy csoportokat az **Engedélyezett hozzáférés** és a **Tiltott hozzáférés** listában.
8. Az igénynek megfelelően válassza ki a **Testreszabás eltávolítása** beállítást. Ennek kiválasztásával törölheti a kijelölt funkció esetleges meglévő egyéni hozzáférését.
9. Az **Alkalmazás adminisztráció** párbeszédablak bezárásához kattintson az **OK** gombra.

A felhasználói hozzáférés kezelésének másik módja az iSeries navigátor Felhasználók és csoportok támogatásának használata:

1. Az iSeries navigátorban bontsa ki a **Felhasználók és csoportok** kategóriát.
2. Válassza ki a **Minden felhasználó**, a **Csoportok** vagy a **Csoporton kívüli felhasználók** nézetek valamelyikét a felhasználók és csoportok listájának megjelenítéséhez.
3. Kattintson a jobb egérgombbal egy felhasználóra vagy csoportra, majd válassza az előugró menü **Tulajdonságok** menüpontját.
4. Kattintson az **Engedélyek** gombra.
5. Kattintson az **Alkalmazások** lapra.
6. Ezen a lapon módosíthatja a felhasználó vagy csoport hozzáférési beállításait.
7. Kattintson minkét párbeszédablak **OK** gombjára a **Tulajdonságok** párbeszédablak bezárásához.

Az iSeries navigátor biztonsági kérdéseivel kapcsolatban további információkhoz az “iSeries navigátor biztonság” oldalszám: 150 szakaszból juthat.

Az alkalmazások írói a program funkció elérésének korlátozása API segítségével a következőket valósíthatják meg:

- Funkció regisztrálása
- Funkcióra vonatkozó információk lekérdezése
- Funkció használatára jogosultak és nem jogosultak meghatározása
- A felhasználónak a funkció használatára vonatkozó jogosultságának ellenőrzése

Megjegyzés: Ez a támogatás **nem** helyettesíti az erőforrás biztonságot. A program funkció elérésének korlátozása nem akadályozza meg a felhasználót egy erőforrás (például fájl vagy program) más felületen keresztül megvalósított elérésében.

Ahhoz, hogy a támogatást használni lehessen egy alkalmazásban, az alkalmazás szállítójának regisztrálnia kell a funkciókat az alkalmazás telepítése során. A regisztrált funkció az alkalmazás adott funkciójához tartozó kódblokknak felel meg. Amikor a felhasználó futtatja az alkalmazást, akkor az alkalmazás meghívja az API-t a kódblokk meghívása előtt. Az API meghívja a használat ellenőrző API-t annak megállapítása érdekében, hogy a felhasználó jogosult-e a funkció használatára. Ha a felhasználónak megengedett a regisztrált funkció használata, akkor a kódblokk lefut. Ha a funkció használata nem engedélyezett a felhasználónak, akkor a kódblokk nem fut le.

Megjegyzés: Az API-k használata egy 30 karakteres függvényazonosító regisztrálásával jár a regisztrációs adatbázisban (WRKREGINF). Bár a funkció hozzáférés korlátozási API-k által használt funkcióazonosítóra nem vonatkoznak kilépési pontok, a kilépési pontoknak meg kell lenniük. Ahhoz, hogy bármit is regisztrálni lehessen az adatbázisban, biztosítani **kell** egy kilépési pont formátumnevet. Ehhez a Funkció regisztrálása API létrehoz egy

ál-formátumnevet az összes regisztrált funkcióhoz. Mivel a formátumnév nem valódi, végprogram sohasem kerül meghívásra.

A rendszeradminisztrátor határozza meg, hogy ki jogosult egy funkcióra, és ki nem. Az adminisztrátor a program funkció elérésének kezelésére használhatja az API-t is és az iSeries navigátor Alkalmazás adminisztráció felületét is. A program funkció elérésének korlátozása API-t az *iSeries server API Reference* című kiadvány tárgyalja. A funkciók hozzáférés felügyeletéről további információkat az “iSeries navigátor biztonság” oldalszám: 150 szakaszban talál.

Biztonsági megfigyelések

A rendszerbiztonság megfigyelését több ok is indokolhatja:

- A biztonsági terv teljességének ellenőrzése.
- A tervezett biztonsági elemek meglétének és megfelelő működésének ellenőrzése. Az ilyen jellegű megfigyelést általában az adatvédelmi megbízott végzi a napi biztonsági adminisztráció részeként. Emellett - gyakran részletesebben is - végezheti egy belső vagy külső auditor a rendszeres biztonsági felülvizsgálat során.
- Annak megállapítása, hogy a rendszer biztonsága lépést tart a rendszer környezetének változásával. Néhány változás, amely hatással lehet a biztonságra:
  - Rendszer felhasználók által létrehozott új objektumok
  - Új felhasználók a rendszeren
  - Objektum tulajdonjog változása (jogosultság változása nélkül)
  - Felelősségi kör változása (felhasználói csoport változása)
  - Ideiglenes jogosultság (visszavonásának elfelejtése)
  - Újonnan telepített termékek
- Jövőbeni eseményekre, például új alkalmazás telepítésére, magasabb biztonsági szint beállítására vagy kommunikációs hálózat kialakulására való felkészülés.

A leírt technikák az összes ilyen szituációra alkalmazhatók. A megfigyelendő dolgok és a megfigyelés gyakorisága a szervezet méretétől és biztonsági igényeitől függ.

A biztonsági megfigyelés parancsok kiadásával, illetve naplóinformációk elérésével és megtekintésével jár. Érdemes létrehozni egy speciális profilt, amelyet a rendszer biztonsági megfigyelését végző személy használ. A megfigyelési profilnak *AUDIT speciális jogosultságra van szüksége a rendszer megfigyelési jellemzőinek módosításához. A fejezetben megadott megfigyelési feladatok némelyike *ALLOBJ és *SECADM speciális jogosultságot is igényel. A megfigyelési időszak végén a megfigyelési profil jelszavát állítsa a *NONE értékre.

A biztonsági megfigyelésről további információkat a *Security Reference* című kiadvány 9. fejezetében talál.

Példa: Jelentés a rendszer biztonsági attribútumairól

Az 1. ábra: oldalszám: 8 a Rendszer biztonsági attribútumok kinyomtatása (PRTSYSSECA) parancs kimenetére mutat be egy példát. A jelentésben a szokásos biztonsági követelményeket támasztó rendszerek számára ajánlott biztonsággal kapcsolatos rendszerváltozók és hálózati attribútumok találhatók. Emellett megadja a rendszer jelenlegi beállításait is.

Megjegyzés: A rendszer jelenlegi beállítása az *Aktuális érték* oszlopban látható. A lehetséges biztonsági kockázatok felmérése érdekében hasonlítsa össze az oszlop tartalmát az ajánlott értékkel.

```
Rendszer biztonsági attribútumok

Rendszerváltozó
neve             Aktuális érték         Ajánlott érték
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
```

1. ábra: Jelentés a rendszer biztonsági attribútumairól - Példa (rész 1 / 4)

```
QAUTOCFG         0                      0
QAUTORMT         1                      0
QAUTOVRT         9999                   0
QCMNRCYLMT       0 0                    0 0
QCRTAUT          *CHANGE                Könyvtárszinten való megadás.
QCRTOBJAUD       *NONE                  Könyvtárszinten való megadás.
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
```

1. ábra: Jelentés a rendszer biztonsági attribútumairól - Példa (rész 2 / 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             *NONE
QUSEADPAUT       *NONE                  CRTAUTL AUTL(QUSEADPAUT) AUT(*EXCLUDE)
                                        CHGOBJOWN OBJ(QUSEADPAUT) OBJTYPE(*AUTL)
                                        CHGSYSVAL SYSVAL(QUSEADPAUT) VALUE(QUSEADPAUT)
QVFYOBJRST       1                      3
```

1. ábra: Jelentés a rendszer biztonsági attribútumairól - Példa (rész 3 / 4)

```
Rendszer biztonsági attribútumok

Hálózati attribútum
neve            Aktuális érték         Ajánlott érték
DDMACC          *OBJAUT                *REJECT
JOBACN          *FILE                  *REJECT
PCSACC          *OBJAUT                *REJECT
```

1. ábra: Jelentés a rendszer biztonsági attribútumairól - Példa (rész 4 / 4)

2. fejezet iSeries biztonsági varázsló és eServer biztonsági tervező

Az iSeries biztonsági varázsló és eServer biztonsági tervező segíthet annak eldöntésében, hogy az iSeries szerveren milyen biztonsági értékeket állítson be. Az iSeries navigátorban található iSeries biztonsági varázsló a megadott válaszok alapján összeállít egy jelentést a biztonsági igényekről. Ennek alapján konfigurálhatja a rendszer biztonságát.

Az iSeries biztonsági varázslóval és az eServer biztonsági tervezővel könnyen alakíthat ki alapvető biztonsági stratégiát az iSeries szervereken. Mindkét eszköz célja, hogy leegyszerűsítse a rendszerek biztonságának megvalósítását és kezelését. Az OS/400 részeként rendelkezésre álló varázsló több felhasználói szintű kérdést is feltesz a szerver környezetére vonatkozóan, és a válaszok alapján előáll egy sor tanáccsal, amelyet a varázsló segítségével azonnal alkalmazhat is a rendszerre.

Az eServer biztonsági tervező a biztonsági varázsló online változata. A tervező a különféle biztonsági igényeknek megfelelően több lehetséges választ is megad, amelyek közül választhat, majd a végén egy jelentésben összegzi az adott környezet biztonságosabbá tételéhez ajánlott beállításokat.

Az eServer biztonsági tervező a varázsló webes változata. A varázslóhoz hasonlóan tanácsokat ad a rendszer biztonságának megvalósítására vonatkozóan. A tervező nem tudja azonban alkalmazni a javaslatokat. Ehelyett a kérdésekre adott válaszok alapján elkészít egy listát a rendszeren beállítandó rendszerváltozókról és egyéb attribútumokról.

Biztonsági varázsló

Az iSeries biztonságra vonatkozó rendszerváltozóinak egy adott környezetben megfelelő beállításainak meghatározása fogas kérdés lehet. Ha még nincsenek kellő tapasztalatai az iSeries szerverek biztonságának megvalósításáról, vagy az iSeries szervert tartalmazó környezet a közelmúltban megváltozott, akkor a biztonsági varázsló hasznos segítséget nyújthat a döntések meghozatalakor.

Mi az a varázsló?

- A varázslók olyan eszközök, amelyek a kezdő felhasználókat átvezetik valaminek a telepítésén vagy beállításán.
- A varázsló a szükséges információkat különféle kérdések megkérdezésével gyűjti össze. Az egyes kérdésekre adott válasz határozza meg a következő feltett kérdést.
- Az összes kérdés feltétele után megjelenik egy befejezés párbeszédablak. Itt a felhasználó a **Befejezés** gomb megnyomásával telepítheti vagy állíthatja be az adott elemet.

A biztonsági varázsló céljai

A biztonsági varázsló célja, hogy a felhasználó által adott válaszok alapján beállítsa a következőket:

- Biztonsággal kapcsolatos rendszerváltozók és hálózati attribútumok.
- A rendszer biztonsági célú megfigyelése.
- Adminisztrátori és felhasználói információs jelentés előállítása:
  - Az adminisztrátori információs jelentés tartalmazza az ajánlott biztonsági beállításokat, és a ajánlások hatályba helyezése előtt elvégzendő esetleges eljárásokat.

  - A felhasználói információs jelentés a szervezet biztonsági házirendjeként felhasználható információkat tartalmaz. Ebben a jelentésben találhatók például a jelszó összeállítási szabályok.
- Tanácsadás a rendszer különféle biztonsággal kapcsolatos elemeinek beállításához.

A biztonsági varázsló feladatai

- A biztonsági varázsló feladatai a következők:
  - A varázsló kérdéseire a felhasználó által adott válaszok alapján a rendszer biztonsági értékek kívánatos beállításainak meghatározása, majd igény szerint a beállítások alkalmazása.
  - A varázsló részletes információs jelentéseket állít elő, amelyben a következők szerepelnek:
    - A varázsló javaslatainak részletes magyarázata.
    - A megvalósítás előtt végrehajtandó eljárások részletezése.
    - A rendszer felhasználói számára készült végfelhasználói információk.
- Ezek az elemek egy alapszintű biztonsági stratégiát valósítanak meg a rendszeren.
- A varázsló javasol különféle megfigyelési jelentéseket is, amelyek ütemezhetők rendszeres időközönkénti futtatásra is. Ütemezésük esetén a jelentések a következőkhöz nyújthatnak segítséget:
  - Biztonsági stratégiák követésének ellenőrzése.
  - Biztonsági stratégiák változásainak nyomon követése.
  - Jelentések ütemezése a rendszer biztonsággal kapcsolatos eseményeinek megfigyeléséhez.
- A varázsló lehetővé teszi a javaslatok mentését, illetve ezek egy részének vagy egészének alkalmazását a rendszerre.

Megjegyzés: A biztonsági varázsló egynél többször is használható azonos rendszeren, így lehetővé téve a felhasználóknak az aktuális biztonsági helyzet áttekintését a régebbi kiadású rendszereken. A biztonsági varázsló a V3R7 (az iSeries navigátor bevezetése) és újabb kiadású rendszereken használható.

Az iSeries navigátor használatához telepíteni kell az IBM iSeries Access for Windows terméket egy Windows 95/NT személyi számítógépre, és be kell állítani egy iSeries szerver kapcsolatot. A varázslót használó felhasználónak csatlakoznia kell az iSeries szerverhez. A felhasználónak rendelkeznie kell *ALLOBJ, *SECADM, *AUDIT és *IOSYSCFG speciális jogosultságokkal. Ha segítségre van szüksége a Windows PC és az iSeries rendszer közötti kapcsolat megteremtéséhez, akkor nézze meg az Információs központ IBM iSeries Access for Windows című témakörét (a részleteket lásd: “Előfeltétel és kapcsolódó információk” oldalszám: xii).

A biztonsági varázsló elérése:

1. Az iSeries navigátorban bontsa ki a szervert.
2. Kattintson a jobb egérgombbal a **Biztonság** kategórián, majd válassza az előugró menü **Beállítás** menüpontját.
   - Az iSeries navigátor **Biztonság** kategóriájának megnyitásakor a program megkéri az iSeries szervert a felhasználó speciális jogosultságainak ellenőrzésére.
   - Amennyiben a felhasználó nem rendelkezik az összes szükséges speciális jogosultsággal (úgymint *ALLOBJ, *AUDIT, *IOSYSCFG és *SECADM), úgy a **Beállítás** menüpont nem jelenik meg, így a biztonsági varázsló nem érhető el számára.
3. Feltéve, hogy a felhasználó rendelkezik a szükséges jogosultságokkal:
   - A varázsló megkeresi a korábbi válaszokat.
   - A varázsló lekérdezi az aktuális biztonsági beállításokat.

A biztonsági varázsló három lehetséges üdvözlő képernyőt jeleníthet meg. A megjelenő képernyő a következő helyzeteket tükrözheti:

- A varázsló még sohasem futott a cél iSeries szerveren.
- A varázsló már lefutott, de a biztonsággal kapcsolatos módosítások még nem kerültek alkalmazásra.
- A varázsló már lefutott, és a biztonsággal kapcsolatos módosítások is hatályba léptek.

Ha nem használja az iSeries navigátort, akkor is kaphat segítséget a biztonsági igények tervezéséhez. Az eServer biztonsági tervező a biztonsági varázsló online változata, ahhoz képest egyetlen különbséggel. A tanácsadó nem állítja be automatikusan a rendszert. A válaszok alapján előállít azonban egy jelentést az ajánlott biztonsági beállításokról. Az eServer biztonsági tervezőt az eServer Információs központban érheti el:

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

eServer biztonsági tervező

Az eServer biztonsági tervező a biztonsági varázsló online változata. Ugyanazokat a kérdéseket teszi fel, mint a biztonsági varázsló, és a válaszok alapján ugyanazokat a javaslatokat is teszi. A két eszköz közötti lényegesebb különbségek a következők:

- Az eServer biztonsági tervező **nem**
  - Állít elő jelentéseket.
  - Hasonlítja össze az aktuális beállításokat az ajánlott beállításokkal.
  - Állítja be automatikusan a rendszert.
- Az eServer biztonsági tervező javaslatait nem alkalmazhatja a rendszerre.

Az eServer biztonsági tervező egy CL programot készít, amelyet kimásolhat a böngészőből, beillesztheti, és esetleges utólagos szerkesztés után felhasználhatja a biztonsági beállítások automatizálására. Az eServer biztonsági tervezőből emellett közvetlenül eljuthat az iSeries dokumentációhoz is. Így információkhoz juthat az egyes rendszerváltozókkal vagy jelentéssel kapcsolatban, és megállapíthatja, hogy a javasolt beállítás helyénvaló-e az adott környezetben.

Az eServer biztonsági tervező a következő Internet címen található:

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

3. fejezet Interaktív bejelentkezés felügyelete

Amennyiben a rendszerbe való belépés korlátozását fontolgatja, akkor kezdje a nyilvánvalóval: a Bejelentkezés képernyővel. A Bejelentkezés képernyőn keresztüli belépés megnehezítésére a következő lehetőségek állnak rendelkezésre.

Jelszó szabályok beállítása

A rendszer bejelentkezés biztonságossá tételéhez tegye a következőket:
- Állítson be egy olyan stratégiát, amely nem engedi meg triviális jelszavak használatát és a jelszavak megosztását.
- Állítsa be az ezt betartató rendszerváltozókat. A rendszerváltozók ajánlott beállításait a 1. táblázat: sorolja fel.

Az értékeknek a 1. táblázat: helyen megadott kombinációja eléggé megszorító, tehát jelentősen lecsökkentheti a triviális jelszavak használatának valószínűségét. A felhasználók viszont meglehetősen frusztrálónak találhatják ilyen jelszavak kitalálását.

Fontolja meg, hogy a felhasználók számára kiadja a következőket:
1. A jelszavakra vonatkozó feltételek listája.
2. Néhány példát érvénytelen jelszavakra.
3. Javaslatokat jó jelszavak kitalálásához.

Futtassa a Rendszer biztonság beállítása (CFGSYSSEC) parancsot ezen értékek beállításához. A Rendszer biztonsági attribútumok kinyomtatása (PRTSYSSECA) paranccsal nyomtassa ki a rendszerváltozók aktuális beállításait.

Az *iSeries biztonsági összefoglaló* című kiadvány 3. fejezete és “A rendszer biztonságának beállítása parancs által beállított értékek” oldalszám: 38 szakasz nyújt további információkat a CFGSYSSEC parancsról.

1. táblázat: Jelszavakra vonatkozó rendszerváltozók

Rendszerváltozó neve	Leírás	Ajánlott érték
QPWDEXPITV	Milyen gyakran kell cserélniük a felhasználóknak a jelszavakat. A felhasználói profilban ettől eltérő érték is beállítható.	60 (nap)
QPWDLMTAJC	A rendszer megakadályozza-e az egymás utáni azonos karaktereket.	1 (igen)
QPWDLMTCHR	A jelszavakban nem használható karakterek.[2]	AEIOU#$@
QPWDLMTREP	A rendszer megakadályozza-e, hogy egy karakter egynél többször szerepeljen a jelszóban.	2 (egymás után nem megengedett)
QPWDLVL	A felhasználói profil jelszavak maximális hossza 10 karakter vagy 128.	0[3]
QPWDMAXLEN	A jelszó maximális karaktereinek száma.	8
QPWDMINLEN	A jelszó minimális karaktereinek száma.	6
QPWDPOSDIF	A jelszó valamennyi pozíciójában az előző jelszó azonos pozíciójához képest eltérő karakternek kell-e állnia.	1 (igen)
QPWDRQDDGT	A jelszóban szerepelnie kell-e legalább egy számjegynek.	1 (igen)
QPWDRQDDIF	Mennyi ideig kell várakoznia a felhasználónak, mielőtt ugyanazt a jelszót használhatná.[2]	5 vagy kevesebb (érvényességi időtartam)[1]
QPWDVLDPGM	Milyen végprogram kerül meghívásra az új jelszó ellenőrzéséhez.	*NONE

1. táblázat: Jelszavakra vonatkozó rendszerváltozók (Folytatás)

Rendszerváltozó neve	Leírás	Ajánlott érték

Megjegyzések:

1. A QPWDEXPITV rendszerváltozó határozza meg, hogy milyen gyakran kell cserélni a jelszót. Ez az **érvényességi időtartam**. A QPWDRQDDIF rendszerváltozó azt adja meg, hogy hány érvényességi időtartam után használható fel ismét egy korábbi jelszó. A felsorolt rendszerváltozók együttműködéséről további részleteket az *iSeries biztonsági összefoglaló* című kiadvány tartalmaz.
2. A QPWDLMTCHR rendszerváltozót a rendszer nem foganatosítja 2. vagy 3. jelszó szintek esetén. További részletek: “Jelszó szintek”.
3. A felhasználók számára megfelelő jelszó szint meghatározásáról a “Jelszó szint módosításának megtervezése” szakaszban olvashat.

Jelszó szintek

Az operációs rendszer V5R1 kiadásától kezdődően a QPWDLVL rendszerváltozó magasabb jelszó biztonságot nyújt. A korábbi kiadásokban a felhasználók legfeljebb 10 karakteres jelszavakat választhattak, azokat is korlátozott karakterkészletből. A rendszeren beállított jelszó szint függvényében a felhasználók most már akár 128 karakteres jelszót (vagy jelmondatot) is választhatnak. A jelszó szintek a következők:

- **0. szint:** Ez a rendszerek gyári alapértelmezése. A 0. szinten a jelszavak legfeljebb 10 karakterből állhatnak, és csak az A–Z, 0–9, #, @, $ és _ karaktereket tartalmazhatják. A 0. szint jelszavai kevésbé biztonságosak a magasabb jelszó szintekhez képest.
- **1. szint:** Ugyanazok a szabályok hatályosak, mint a 0. szinten, de az iSeries támogatás a Windows Hálózatokhoz (a továbbiakban iSeries hálózati szerver) jelszavak nem kerülnek mentésre.
- **2. szint:** Ez a szint biztonságos jelszavakat alkalmaz. A szint tesztelési célokra használható. A legfeljebb 10 karakterből álló és a 0. vagy 1. szintnek megfelelő karakterkészletet alkalmazó jelszavak a 0. vagy 1. szintnek megfelelően kerülnek mentésre. A jelszavak (vagy jelmondatok) jellemzői a következők lehetnek:
  - legfeljebb 128 karakterből állhatnak
  - tetszőleges karaktert tartalmazhatnak
  - nem állhatnak csak üres karakterekből; a rendszer az üres karaktereket a jelszó végéről levágja
  - a kis- és nagybetűket megkülönböztetik
- **3. szint:** A jelszavak ezen a szinten a legbiztonságosabbak, tárolásuk a legfejlettebb titkosítási algoritmusok védelme alatt történik. Az itt alkalmazható jelszavak megegyeznek a 2. szint jelszavaival, az iSeries hálózati szerver jelszavak pedig nem kerülnek mentésre.

A 2. és 3. jelszó szinteket akkor alkalmazhatja, ha a hálózat valamennyi rendszere megfelel a következő feltételeknek:

- Az operációs rendszer V5R1 vagy újabb
- A jelszó szint 2 vagy 3

A felhasználók mindegyikének azonos jelszó szint mellett kell bejelentkeznie. A jelszó szintek globálisak, a felhasználók nem választhatják meg, hogy a jelszavaikat milyen szint szerint óhajtják tárolni.

Jelszó szint módosításának megtervezése

A jelszó szintek módosítása körültekintő tervezést igényel. Nem megfelelő tervezés esetén meghiúsulhat a többi rendszerrel való együttműködés és a felhasználók bejelentkezése. A

QPWDLVL rendszerváltozó módosítása előtt győződjön meg róla, hogy mentette a biztonsági adatokat a SAVSECDTA vagy SAVSYS parancsok valamelyikével. Ha rendelkezik naprakész mentéssel, akkor lehetőség van a felhasználói profilokhoz tartozó jelszavak visszaállítására az alacsonyabb jelszó szinteknek megfelelően.

A rendszeren használt termékek és a kliensek problémákba ütközhetnek a jelszó szint (QPWDLVL) rendszerváltozó 2 vagy 3 értéke esetén. A jelszavakat a bejelentkezési képernyőn megadott nyílt szöveges forma helyett titkosított formában küldő valamennyi terméket és klienst frissíteni kell a 2-es vagy 3-as QPWDLVL új jelszó titkosítási szabályainak megfelelően. A titkosított jelszó küldését **jelszó helyettesítésnek** is hívjuk.

A jelszó helyettesítés akadályozza meg a jelszavak megszerzését a hálózaton keresztüli átvitel során. A QPWDLVL 2 vagy 3 értéke esetén alkalmazott új algoritmust nem támogató régebbi kliensek által előállított jelszó helyettesítőket a rendszer akkor sem fogadja el, ha a megadott karakterek egyébként helyesek voltak. Ez az iSeries - iSeries szerverek közötti olyan egyenrangú hozzáférésre is vonatkozik, amely titkosított értékekkel hitelesíti egymás felé a rendszereket.

A problémát tovább bonyolítja, hogy bizonyos érintett termékek (például a Java eszközkészlet) közbenső szintű termékként kerül szállításra. Az ilyen termékek korábbi változataira épülő harmadik féltől származó termékek nem fognak működni mindaddig, amíg nem kerülnek újraépítésre a közbenső szintű termék frissített változatának felhasználásával.

Ezt tekintve könnyen belátható, hogy miért olyan fontos a körültekintő tervezés a QPWDLVL rendszerváltozó módosítása előtt.

Szempontok a QPWDLVL beállításához a 0. szintről az 1. szintre

Az 1. jelszó szint lehetővé teszi az iSeries hálózati szerver jelszavak tárolásának beszüntetését a rendszeren az olyan esetekben, amikor nincs szükség kommunikációra az AS/400 támogatás a Windows Hálózatokhoz (iSeries hálózati szerver) termék Windows 95/98/ME kliens támogatásával. A szükségtelen titkosított jelszavak megszüntetése növeli a rendszer általános biztonságát.

A QPWDLVL 1-es értéke mellett a V5R1 előtti összes jelszó helyettesítési és jelszó hitelesítési mechanizmus működőképes marad. Ez rendkívül csekély mennyiségű problémalehetőséget rejt magában, kivéve persze az iSeries hálózati szerver jelszót igénylő funkciókat és szolgáltatásokat.

Szempontok a QPWDLVL beállításához a 0. vagy 1. szintről a 2. szintre

A 2. jelszó szint bevezeti a kis- és nagybetűket megkülönböztető, legfeljebb 128 karakterből álló jelszavakat (más néven hosszú jelszavakat vagy jelmondatokat), és a lehetőségekhez képest maximálisan támogatja a visszaállást a QPWDLVL 0 vagy 1 értékére.

A rendszer jelszó szintjétől függetlenül 2. és 3. szintű jelszavak jönnek létre minden alkalommal, amikor egy jelszó megváltozik vagy egy felhasználó bejelentkezik a rendszerre. 2. vagy 2. szintű jelszó létrehozása a rendszer 0. vagy 1. jelszó szintjén megkönnyíti a váltást a 2. vagy 3. jelszó szintre.

A QPWDLVL 2 értékének beállítása előtt a DSPAUTUSR vagy a PRTUSRPRF TYPE(*PWDINFO) paranccsal keresse ki azokat a felhasználói profilokat, amelyek nem rendelkeznek a 2. jelszó szintnek megfelelő jelszóval. A parancsok által felsorolt profiloktól függően a következő eljárások valamelyikével adjon hozzá egy 2. és 3. szintű jelszót a profilokhoz.

- Módosítsa a felhasználói profil jelszavát a CHGUSRPRF vagy CHGPWD CL parancsok, vagy a QSYCHGPW API segítségével. Ennek hatására a rendszer módosítja a 0. és 1.

szinten használható jelszót; emellett létrehoz két egymással egyenértékű, kis- és nagybetűket megkülönböztető jelszót is, amelyek a 2. és 3. szinten használhatók. A 2. és 3. jelszó szint számára a jelszónak egy csupa kisbetűs és egy csupa nagybetűs változata jön létre.

A C4D2RB4Y jelszó beállításakor például a rendszer a 2. jelszó szint számára a C4D2RB4Y és c4d2rb4y jelszavakat állítja elő.

- Jelentkezzen be a rendszerre jelszó helyettesítést nem alkalmazó (a jelszó sima szöveges formában elküldő) szolgáltatáson keresztül. Ha a jelszó érvényes, és a felhasználói profil nem rendelkezik 2. és 3. jelszó szinten használható jelszóval, akkor a rendszer létrehoz két egymással egyenértékű, kis- és nagybetűket megkülönböztető jelszót, amely használható a 2. és 3. jelszó szinten. A 2. és 3. jelszó szint számára a jelszónak egy csupa kisbetűs és egy csupa nagybetűs változata jön létre.

A 2. vagy 3. szinten használható jelszó hiánya akkor jelenthet problémát, ha a felhasználói profil 0. vagy 1. szintű jelszóval sem rendelkezik, vagy amikor a felhasználó jelszó helyettesítést alkalmazó szolgáltatáson keresztül próbál bejelentkezni. Ezekben az esetekben a felhasználó nem tud bejelentkezni a jelszó szint 2-re állítása után.

Ha a felhasználói profil nem rendelkezik a 2. és 3. jelszó szinten használható jelszóval, de rendelkezik 0. és 1. szinten használható jelszóval, és a felhasználó bejelentkezik a rendszerre egy sima szöveges jelszót küldő szolgáltatáson keresztül, akkor a rendszer a felhasználót a 0. jelszó szintnek megfelelő jelszóval hitelesíti, majd létrehozza a felhasználói profil (fentiekben leírt) 2. jelszó szinten használható jelszavát. Az ezt követő bejelentkezések érvényesítése a 2. szintű jelszóval történik.

A jelszó helyettesítést alkalmazó kliensek és szolgáltatások nem fognak működni a QPWDLVL 2 értéke mellett, ha a kliens vagy szolgáltatás nem került frissítésre az új jelszó (jelmondat) helyettesítési sémának megfelelően. Az adminisztrátornak ellenőriznie kell, hogy a kliens vagy szolgáltatás frissítésre került-e az új jelszó helyettesítési sémának megfelelően.

Jelszó helyettesítést alkalmazó kliensek vagy szolgáltatások egyebek között a következők:

- TELNET
- iSeries Access
- iSeries hoszt szerverek
- QFileSrv.400
- iSeries hálózati szerver nyomtatási támogatás
- DDM
- DRDA
- SNA LU6.2

A biztonsági adatokat határozottan javallt menteni a QPWDLVL 2. szintjének beállítása előtt. Ez megkönnyíti a visszaállást a 0. vagy 1. jelszó szintre, amennyiben ez szükségessé válik.

A jelszóra vonatkozó többi rendszerváltozót, például a QPWDMINLEN-t és a QPWDMAXLEN-t tesztelési célból egy ideig érdemes változatlanul hagyni a 2. jelszó szint bevezetése után. Ez szintén megkönnyíti a QPWDLVL 1 vagy 0 értékének visszaállítását. A QPWDVLDPGM rendszerváltozót viszont be kell állítani a *REGFAC vagy *NONE értékre, mielőtt a rendszer engedélyezné a QPWDLVL 2-re állítását. Ennek megfelelően ha rendelkezik jelszó ellenőrzési programmal, akkor valószínűleg újat kell írni, amelyet az ADDEXITPGM paranccsal be kell jegyezni a QIBM_QSY_VLD_PASSWRD kilépési ponthoz.

Az iSeries hálózati szerver jelszavak továbbra is támogatottak a QPWDLVL 2 értéke mellett, így az iSeries hálózati szerver jelszót igénylő funkciók és szolgáltatások továbbra is működőképesek maradnak.

Miután a rendszeren az élet visszazökkent a normális kerékvágásba a QPWDLVL 2 értéke mellett, az adminisztrátor megkezdheti a jelszóra vonatkozó rendszerváltozók módosítását a hosszabb jelszavak előnyeinek kihasználásához. Figyelembe kell azonban venni, hogy a hosszabb jelszavak a következőket fogják eredményezni:

- 10 karakternél hosszabb jelszó beállítása esetén a 0. és 1. szinten használható jelszó törlődik. Az ilyen felhasználói profilok a 0. vagy 1. jelszó szintre való visszaállás után nem fognak tudni bejelentkezni.
- Ha a jelszavak speciális karaktereket tartalmaznak, vagy nem követik az egyszerű objektumok nevére vonatkozó megállapodásokat (a kis- és nagybetűk közötti különbségen túlmenően), akkor a 0. és 1. szinten használható jelszó szintén törlődik.
- 14 karakternél hosszabb jelszó megadása esetén törlődik a felhasználói profil iSeries hálózati szerver jelszava.
- A jelszavakkal kapcsolatos rendszerváltozók csak az új 2. jelszó szintre vonatkoznak, a rendszer által előállított 0. vagy 1. szintű jelszóra, illetve az iSeries hálózati szerver jelszóra (már amennyiben ilyen létrejön) nem.

Szempontok a QPWDLVL beállításához a 2. szintről a 3. szintre

Miután a rendszer már egy ideje problémamentesen fut a QPWDLVL 2. szintje mellett, az adminisztrátor a jelszó biztonság maximálisra növelése érdekében megfontolhatja az áttérést a 3. jelszó szintre.

A 3. jelszó szinten az összes iSeries hálózati szerver jelszó törlődik a rendszerről, ennek megfelelően a 3. jelszó szintre való átállást mindaddig nem lehet elvégezni, amíg igény van iSeries hálózati szerver jelszavakra.

A QPWDLVL 3 értéke mellett a 0. és 1. jelszó szinten használható jelszavak törlődnek. Az adminisztrátor a DSPAUTUSR vagy a PRTUSRPRF parancsokkal keresheti meg azon felhasználói profilokat, amelyek nem rendelkeznek 2. vagy 3. szintű jelszóval.

Váltás alacsonyabb jelszó szintre

Az alacsonyabb QPWDLVL értékekre való visszaállás annak ellenére hogy lehetséges, várhatóan nem lesz fájdalommentes folyamat. Az alacsonyabb QPWDLVL értékektől a magasabbak felé vezető utat általában érdemes egyirányú utcának tekinteni. Bizonyos esetekben azonban ettől függetlenül szükség lehet a jelenleginél alacsonyabb QPWDLVL értékek beállítására.

Az alacsonyabb jelszó szintekre való visszaállással kapcsolatos teendőket az alábbi szakaszok részletezik.

Szempontok a QPWDLVL beállításához a 3. szintről a 2. szintre: Ez a váltás viszonylag egyszerű. A QPWDLVL 2-re állítása után az adminisztrátornak meg kell határoznia, hogy vannak-e olyan felhasználói profilok, amelyeknek szükségük van iSeries hálózati szerver jelszóra illetve 0. vagy 1. szinten használható jelszóra, és az ilyen profiloknak le kell cserélni a jelszavát egy megengedett értékre.

Emellett a jelszóval kapcsolatos rendszerváltozókat vissza kell állítani olyan értékekre, amelyek kompatíbilisek az iSeries hálózati szerver jelszavakkal illetve a 0. és 1. szinten használható jelszavakkal, amennyiben szükség van ilyenekre.

Szempontok a QPWDLVL beállításához a 3. szintről az 1. vagy 0. szintre: A rendszeren tapasztalt problémák bekövetkezésének rendkívül magas valószínűsége miatt (például a 0. és 1. szintű jelszavak törlése miatt senki nem tud bejelentkezni) ez a váltás közvetlenül nem

támogatott. Ha a QPWDLVL értékét 3-ról 1-re vagy 0-ra kívánja módosítani, akkor köztes lépésként először 2-es jelszó szintet kell beállítani.

Szempontok a QPWDLVL beállításához a 2. szintről az 1. szintre: A QPWDLVL 1-re állítása előtt az adminisztrátornak a DSPAUTUSR vagy PRTUSRPRF TYPE(*PWDINFO) paranccsal meg kell keresnie az olyan felhasználói profilokat, amelyek nem rendelkeznek 0. vagy 1. szintű jelszóval. Ha a felhasználói profil jelszót fog igényelni a QPWDLVL módosítása után, akkor az adminisztrátornak az alábbi módszerek valamelyikével biztosítania kell, hogy a profil 0. vagy 1. szintű jelszava létrejöjjön:

- Módosítsa a felhasználói profil jelszavát a CHGUSRPRF vagy CHGPWD CL parancsok, vagy a QSYCHGPW API segítségével. Ennek hatására a rendszer módosítja a 2. és 3. szinten használható jelszót; emellett létrehoz egy ezzel egyenértékű csupa nagybetűs jelszót a 0. és 1. szint számára. A rendszer csak akkor képes a 0. és 1. jelszó szint jelszavának létrehozására, ha a jelszóra teljesülnek a következők:
  - A jelszó legfeljebb 10 karakterből áll.
  - A jelszó átalakítható nagybetűs EBCDIC karakterekre: A-Z, 0-9, @, #, $ és aláhúzás.
  - A jelszó nem kezdődik számmal vagy aláhúzással.

  A RainyDay jelszó beállításakor például a rendszer a 0. és 1. jelszó szint számára a RAINYDAY jelszót állítja elő. A ″Rainy Days in April″ jelszó beállításakor azonban a rendszer törli a 0. és 1. szint jelszavát, mivel a megadott jelszó túl hosszú, és üres karaktert tartalmaz.

  A 0. és 1. szintű jelszó létrehozásának meghiúsulását semmiféle üzenet nem jelzi.
- Jelentkezzen be a rendszerre jelszó helyettesítést nem alkalmazó (a jelszó sima szöveges formában elküldő) szolgáltatáson keresztül. Ha a jelszó érvényes, és a felhasználói profil nem rendelkezik 0. és 1. jelszó szinten használható jelszóval, akkor a rendszer létrehoz egy ezzel egyenértékű, csupa nagybetűs jelszót, amely használható a 0. és 1. jelszó szinten. A rendszer csak akkor képes a 0. és 1. jelszó szint jelszavának létrehozására, ha a fenti feltételek teljesülnek.

Az adminisztrátor ezután módosíthatja a QPWDLVL értékét 1-re. Ennek hatására a QPWDLVL 1 értékének hatályba lépésekor (következő IPL) valamennyi iSeries hálózati szerver jelszó törlődik a rendszerről.

Szempontok a QPWDLVL beállításához a 2. szintről a 0. szintre: A szempontok megegyeznek a QPWDLVL értékének 2 → 1 módosításával. Az egyetlen kivétel, hogy valamennyi iSeries hálózati szerver jelszó megtartásra kerül.

Szempontok a QPWDLVL beállításához az 1. szintről a 0. szintre: A QPWDLVL 0-ra állítása után az adminisztrátornak a DSPAUTUSR vagy PRTUSRPRF paranccsal meg kell keresnie azon felhasználói profilokat, amelyek nem rendelkeznek iSeries hálózati szerver jelszóval. Ha a felhasználói profilnak szüksége van iSeries hálózati szerver jelszóra, akkor ennek létrehozásához a felhasználó jelszavát le kell cserélni, vagy be kell jelentkeznie egy olyan szolgáltatáson keresztül, amely a jelszót sima szöveges formában küldi el.

Az adminisztrátor ezután módosíthatja a QPWDLVL-t 0-ra.

Ismert jelszavak módosítása

A következők végrehajtásával zárja be az iSeries szerveren esetleg meglévő közismert bejáratokat.

__ Lépés 1. Győződjön meg róla, hogy egyetlen felhasználói profil sem használ alapértelmezett (a profil nevével megegyező) jelszót. Ehhez használja az

Alapértelmezett jelszavak elemzése (ANZDFTPWD) parancsot. (Lásd: “Alapértelmezett jelszavak elkerülése” oldalszám: 26.)

__ Lépés 2. Próbáljon meg bejelentkezni a rendszerre a 2. táblázat: helyen megadott felhasználói profilok és jelszavak kombinációival. Ezek a jelszavak dokumentálva vannak, tehát ha valaki be akar törni a rendszerbe, akkor kézenfekvő, hogy ezekkel próbálkozik elsőként. Ha a bejelentkezés sikeres, akkor a Felhasználói profil módosítása (CHGUSRPRF) paranccsal módosítsa a jelszót az ajánlott értékre.

__ Lépés 3. Indítsa el a Kijelölt szervizeszközöket (DST), és próbáljon bejelentkezni a 2. táblázat: helyen felsorolt jelszavakkal. További részletekért nézze meg az iSeries Információs központ Biztonság → Szervizeszközök témakörét. Az iSeries Információs központ elérésével kapcsolatban nézze meg az “Előfeltétel és kapcsolódó információk” oldalszám: xii szakaszt.

__ Lépés 4. Ha bármelyik felsorolt jelszóval sikeresen be tudott jelentkezni a DST-be, akkor a jelszót le kell cserélni. A szervizeszköz felhasználói azonosítók és jelszavak cseréjére vonatkozó részletes útmutatásokat az iSeries Információs központ Biztonság → Szervizeszközök című témakörében találja. Az iSeries Információs központ elérésével kapcsolatban nézze meg az “Előfeltétel és kapcsolódó információk” oldalszám: xii szakaszt.

__ Lépés 5. Végül győződjön meg róla, hogy nem tud bejelentkezni a Bejelentkezés képernyőn felhasználói azonosító és jelszó megadása nélkül, egyszerűen az Enter megnyomásával. Próbáljon ki több különböző képernyőt is. Ha a Bejelentkezés képernyőn információk megadása nélkül be tud jelentkezni, akkor tegye a következők valamelyikét:

- Módosítsa a biztonsági szintet (a QSECURITY rendszerváltozót) 40-re vagy 50-re.

  Megjegyzés: Az alkalmazások elképzelhető, hogy eltérően futnak 40-es vagy 50-es biztonsági szinten.

- Módosítsa az interaktív alrendszerek valamennyi munkaállomás bejegyzését úgy, hogy ezek USER(*RQD) beállítással rendelkező jobleírásokra mutassanak.

2. táblázat: Az IBM által szállított profilok jelszavai

Felhasználói azonosító	Jelszó	Ajánlott érték
QSECOFR	QSECOFR[1]	Csak a biztonsági adminisztrátor számára ismert nemtriviális érték. **A választott jelszót írja le, és tárolja biztonságos helyen.**
QSYSOPR	QSYSOPR	*NONE[2]
QPGMR	QPGMR	*NONE[2]
QUSER	QUSER	*NONE[2, 3]
QSRV	QSRV	*NONE[2]
QSRVBAS	QSRVBAS	*NONE[2]

2. táblázat: Az IBM által szállított profilok jelszavai (Folytatás)

Felhasználói azonosító	Jelszó	Ajánlott érték

Megjegyzések:

1. A rendszeren gyári alapértelmezésben a QSECOFR felhasználónál a *Jelszó beállítása lejártnak* értéke *YES. Ez azt jelenti, hogy a QSECOFR jelszavát az első bejelentkezés alkalmával le kell cserélni.
2. A rendszernek ezekre a felhasználói profilokra különféle rendszerfunkciókhoz van szüksége, a felhasználóknak azonban nem szabad engedélyezni, hogy ezekkel a profilokkal bejelentkezzenek. Az operációs rendszer V3R1 vagy újabb kiadásaival rendelkező új rendszereken ez a jelszó *NONE.

   A CFGSYSSEC parancs lefuttatásakor a rendszer szintén a *NONE értékre állítja ezen jelszavakat.
3. Az iSeries Access for Windows TCP/IP feletti használatához a QUSER felhasználói profilt engedélyezni kell.

3. táblázat: Kijelölt szervizeszközök (DST) jelszavai

DST szint	Felhasználói azonosító[1]	Jelszó	Ajánlott érték
Alapvető képességek	11111111	11111111	Csak a biztonsági adminisztrátor számára ismert nemtriviális érték.[2]
Teljes képesség	22222222	22222222[3]	Csak a biztonsági adminisztrátor számára ismert nemtriviális érték.[2]
Biztonsági képesség	QSECOFR	QSECOFR[3]	Csak a biztonsági adminisztrátor számára ismert nemtriviális érték.[2]
Szerviz képesség	QSRV	QSRV[3]	Csak a biztonsági adminisztrátor számára ismert nemtriviális érték.[2]

Megjegyzések:

1. Felhasználói azonosítóra csak a PowerPC AS (RISC) operációs rendszer kiadásoknál van szükség.
2. Ha a hardver szerviz képviselőjének be kell jelentkeznie ezzel a felhasználói azonosítóval és jelszóval, akkor a szerviz képviselő távozása után módosítsa a jelszót egy új értékre.
3. A szervizeszköz felhasználói profil az első használatnál azonnal lejár.

Megjegyzés: A DST jelszavakat csak hitelesített eszköz módosíthatja. Ez igaz az összes jelszóra és a megfelelő azonos felhasználói azonosítókra is. A hitelesített eszközökről további információkkal az iSeries Információs központ Műveleti konzol témaköre szolgál.

Bejelentkezési értékek beállítása

A 4. táblázat: több értéket is felsorol, amelyekkel megnehezítheti a jogosulatlan személyek számára a rendszerre való bejelentkezést. A rendszerváltozók ajánlott értékeit a CFGSYSSEC parancs futtatásával állíthatja be. A rendszerváltozókról további részleteket az *iSeries biztonsági összefoglaló* című kiadvány 3. fejezetében olvashat.

4. táblázat: Bejelentkezéssel kapcsolatos rendszerváltozók

Rendszerváltozó neve	Leírás	Ajánlott beállítás
QAUTOCFG	Megadja, hogy a rendszer automatikusan konfigurálja-e az új eszközöket.	0 (Nem)

4. táblázat: Bejelentkezéssel kapcsolatos rendszerváltozók (Folytatás)

Rendszerváltozó neve	Leírás	Ajánlott beállítás
QAUTOVRT	A rendszer által automatikusan létrehozott virtuális eszköz leírások száma, amennyiben nincs használható eszköz.	0
QDEVRCYACN	A rendszer által végzett tevékenység egy eszköz hiba utáni újracsatlakozásakor.[1]	*DSCMSG
QDSCJOBITV	Megadja, hogy a rendszer mennyi ideig várakozzon a szétkapcsolt jobok befejezésével.	120
QDSPSGNINF	Megadja, hogy a rendszer megjelenítse-e a felhasználó bejelentkezésekor a korábbi bejelentkezésre vonatkozó információkat.	1 (Igen)
QINACTITV	Megadja, hogy a rendszer mennyi idő után tesz lépéseket az inaktív interaktív jobok ügyében.	60
QINACTMSGQ	Megadja a rendszer tevékenységét a QINACTITV időtartam eltelése után.	*ENDJOB
QLMTDEVSSN	Megadja, hogy a rendszer megakadályozza-e, hogy a felhasználók egyszerre több munkaállomásról is bejelentkezzenek.	1 (Igen)
QLMTSECOFR	Megadja, hogy az *ALLOBJ vagy *SERVICE speciális jogosultságokkal rendelkező felhasználók csak adott munkaállomásokról léphetnek be.	1 (Igen)[2]
QMAXSIGN	Az egymás után következő helytelen bejelentkezési kísérletek (helytelen felhasználói profil vagy jelszó) maximális száma.	3
QMAXSGNACN	A rendszer tevékenysége a QMAXSIGN korlát elérésekor.	3 (Felhasználói profil és eszköz letiltása)

Megjegyzések:

1. A rendszer képes a Telnet szekciók leválasztására és újracsatlakoztatására a szekció eszközleírásának explicit hozzárendelésekor.
2. Ha a rendszerváltozónak az 1 (Igen) értéket adja, akkor kifejezetten fel kell jogosítani az *ALLOBJ vagy *SERVICE speciális jogosultsággal rendelkező felhasználókat az egyes eszközökre. Ennek legegyszerűbb módja, ha a QSECOFR felhasználói profilnak *CHANGE jogosultságot ad az adott eszközökre vonatkozóan.

Bejelentkezési hibaüzenetek módosítása

A betörők szeretik tudni, hogy haladnak-e a rendszer feltörésével. Ha a bejelentkezési képernyőn Helytelen jelszó üzenet jelenik meg, akkor a betörő joggal feltételezheti, hogy a megadott felhasználói azonosító helyes. Az Üzenetleírás módosítása (CHGMSGD) paranccsal módosíthatja a két bejelentkezési hibaüzenet szövegét, ily módon elbizonytalanítva a betörőt. Az ajánlott szöveget a 5. táblázat: adja meg.

5. táblázat: Bejelentkezési hibaüzenetek

Üzenetazonosító	Eredeti szöveg	Ajánlott szöveg
CPF1107	CPF1107 – A felhasználói profil jelszava helytelen.	A bejelentkezési információk helytelenek. **Megjegyzés:** Az üzenetazonosítót ne vegye bele az üzenet szövegébe.
CPF1120	CPF1120 – Az XXXXX felhasználó nem létezik.	A bejelentkezési információk helytelenek. **Megjegyzés:** Az üzenetazonosítót ne vegye bele az üzenet szövegébe.

Felhasználói profilok elérhetőségének ütemezése

Bizonyos felhasználói profiloknál érdemes lehet beállítani, hogy csak a hét bizonyos napjain, és csak bizonyos időtartamon belül legyenek alkalmasak a bejelentkezésre. Ha például van egy auditori felhasználói profil, akkor ezt érdemes úgy beállítani, hogy csak az auditor munkaidejében álljon rendelkezésre. Emellett érdemes letiltani az *ALLOBJ speciális jogosultsággal rendelkező felhasználói profilokat (a QSECOFR profillal együtt) a munkaidőn kívüli időszakban.

Az Aktiválás ütemezési bejegyzés módosítása (CHGACTSCDE) paranccsal állíthatja be a felhasználói profilok automatikus engedélyezését és letiltását. Minden egyes ütemezni kívánt felhasználói profilhoz létrejön egy bejegyzés, amely meghatározza a felhasználói profil ütemezését.

Ha például be kívánja állítani, hogy a QSECOFR profil csak reggel 7 és este 10 között legyen elérhető, akkor a írja be a CHGACTSCDE parancsot, amelynek hatására megjelenik a CHGACTSCDE képernyő:

```
              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
```

2. ábra: Profil aktiválás ütemezése képernyő – Példa

A QSECOFR profilt érdemes csak igen korlátozott időtartamon belül elérhetővé tenni. A legtöbb rendszerfunkcióhoz ilyenkor használhat egy másik *SECOFR osztályú felhasználói profilt. Ezzel kiküszöbölhető egy közismert felhasználói profilra való betörések kockázata.

A Megfigyelési napló bejegyzések megjelenítése (DSPAUDJRNE) paranccsal rendszeres időközönként nyomtassa ki a CP (Profil módosítás) naplóbejegyzéseket. Ezekkel a bejegyzésekkel ellenőrizheti, hogy a rendszer a felhasználói profilok engedélyezését és letiltását a tervezett ütemezésnek megfelelően végzi.

A felhasználói profilok tervezett ütemezésnek megfelelő letiltásának ellenőrzésére egy másik módszert a Felhasználói profil nyomtatása (PRTUSRPRF) parancs kínál. Ha megadja a *PWDINFO értéket a jelentés típusának, akkor a jelentésbe a kijelölt felhasználói profilok állapota is bekerül. Ha például rendszeresen letiltja az *ALLOBJ speciális jogosultsággal rendelkező felhasználói profilokat, akkor beütemezheti a profilok letiltása utánra azonnal a következő parancsot:

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

Inaktív felhasználói profilok eltávolítása

A rendszeren csak a szükséges felhasználói profiloknak szabad lenniük. Ha egy felhasználói profilra a továbbiakban nincs szükség, például azért, mert a felhasználó kilépett, vagy más munkakörbe került át, akkor távolítsa el a felhasználói profilt. Ha egy felhasználó hosszabb időre távozik, akkor tiltsa le (inaktiválja) a profilját. A szükségtelen felhasználói profilok jogosulatlan belépéshez vezethetnek.

Felhasználói profilok automatikus letiltása

A Profil tevékenység elemzése (ANZPRFACT) paranccsal rendszeres időközönként letilthatja a megadott időtartamon keresztül inaktív felhasználói profilokat. Az ANZPRFACT parancs használatakor azt kell megadni, hogy a rendszer hány napon keresztül inaktív profilokat keressen. A rendszer a felhasználói profil legutóbbi használatának dátumát, visszaállításának dátumát és létrehozásának dátumát ellenőrzi.

Miután megadta a megfelelő értéket az ANZPRFACT parancsnak, a rendszer az érték első megadásának napja utáni naptól kezdődően minden héten, hajnali 1 órakor lefuttat egy ilyen jobot. A job megvizsgál minden profilt, és letiltja az inaktív profilokat. Az ANZPRFACT parancsot csak akkor kell ismét használnia, ha módosítani kívánja az inaktív napok számát.

Az Aktív profilok listájának módosítása (CHGACTPRFL) paranccsal vehet ki bizonyos profilokat az ANZPRFACT feldolgozás alól. A CHGACTPRFL parancs létrehoz egy olyan felhasználói profil listát, amelyet az ANZPRFACT parancs az inaktív napok számától függetlenül sohasem fog letiltani.

Amikor a rendszer az ANZPRFACT parancsot futtatja, egy CD bejegyzést ír minden egyes letiltott felhasználói profil megfigyelési naplójába. Az újonnan letiltott felhasználói profilok listázására a DSPAUDJRNE parancsot használhatja.

Megjegyzés: A megfigyelési bejegyzés írására csak akkor kerül sor, ha a QAUDCTL értéke *AUDLVL, és a QAUDLVL rendszerváltozó beállítása *SECURITY.

A felhasználói profilok tervezett ütemezésnek megfelelő letiltásának ellenőrzésére egy másik módszert a Felhasználói profil nyomtatása (PRTUSRPRF) parancs kínál. Ha megadja a *PWDINFO értéket a jelentés típusának, akkor a jelentésbe a kijelölt felhasználói profilok állapota is bekerül.

Felhasználói profilok automatikus eltávolítása

A Lejárat ütemezési bejegyzés módosítása (CHGEXPSCDE) paranccsal kezelheti a felhasználói profilok letiltását vagy eltávolítását. Ha tudja, hogy egy felhasználó hosszabb időre távol fog maradni, akkor beütemezheti a profiljának eltávolítását vagy letiltását.

A CHGEXPSCDE parancs az első használat során létrehoz egy job ütemezési bejegyzést, amely minden nap lefut 1 perccel éjfél után. A job a QASECEXP fájl alapján határozza meg, hogy aznapra van-e eltávolítandó felhasználói profil.

A CHGEXPSCDE paranccsal a felhasználói profilok letiltása és eltávolítása is lehetséges. Ha a felhasználói profilok törlését választja, akkor beállíthatja, hogy mi történjen a felhasználó által birtokolt objektumokkal. A felhasználói profil törlésre ütemezése előtt meg kell vizsgálni a felhasználó által birtokolt objektumokat. Ha például a felhasználó jogosultságot átvevő programokat birtokol, akkor ezeket érdemes beállítani, hogy az új tulajdonos jogosultságát vegyék át. Érdemes továbbá megnézni, hogy az új tulajdonos nem rendelkezik-e a korábbihoz képest valamilyen többletjogosultsággal (például speciális jogosultságokkal). Bizonyos esetekben a legjobb megoldás egy új felhasználói profil létrehozása a program birtoklására, ilyenkor ugyanis pontosan megadhatók a szükséges jogosultságok.

Érdemes megvizsgálni emellett, hogy a felhasználói profil törlése okoz-e valamilyen problémát valamelyik alkalmazásnál. Vannak például olyan jobok, amelyek a törölni kívánt felhasználói profilt adják meg alapértelmezett felhasználóként?

A Lejárat ütemezésének megjelenítése (DSPEXPSCD) parancs segítségével jelenítheti meg a letiltásra vagy eltávolításra ütemezett profilok listáját.

A rendszer összes felhasználói profiljának listáját a Jogosult felhasználók megjelenítése (DSPAUTUSR) paranccsal tekintheti meg. Az elévült profilok törlésére használja a Felhasználói profil törlése (DLTUSRPRF) parancsot.

Biztonsági megjegyzés:: A felhasználói profilok letiltása azt jelenti, hogy az állapota *DISABLED lesz. A felhasználói profilok letiltásakor a profil elérhetetlenné válik interaktív felhasználásra. A letiltott felhasználói profilokkal nem lehet bejelentkezni, illetve a jobok nem állíthatók be tiltott felhasználói profilra. A kötegelt jobok azonban futhatnak a letiltott felhasználói profil alatt.

Alapértelmezett jelszavak elkerülése

Új felhasználói profilok létrehozásakor az jelszó alapértelmezésben megegyezik a felhasználói profil nevével. Ha valaki ismeri a felhasználói profilok nevének kialakítására vonatkozó megállapodásokat, és tudja valakiről, hogy belép a szervezetbe, akkor ez lehetővé teheti számára, hogy bejelentkezzen a rendszerbe.

Új felhasználói profilok létrehozásakor fontolja meg egyedi, nemtriviális jelszavak hozzárendelését az alapértelmezett jelszó helyett. A jelszót bizalmasan, például egy “Üdvözöljük a rendszerben” levélben hozza az új felhasználó tudomására, amelyben egyben leírhatja a rendszer biztonsági házirendjét is. A felhasználói profil PWDEXP(*YES) beállításával követelje meg, hogy a felhasználó cserélje le a jelszavát az első bejelentkezés alkalmával.

Az alapértelmezett jelszóval rendelkező felhasználói profilok kikeresésére az Alapértelmezett jelszavak elemzése (ANZDFTPWD) parancsot használhatja. A jelentés kinyomtatásakor lehetősége van megadni, hogy a rendszer reagáljon a profil nevével megegyező jelszavak esetén, például a felhasználói profil letiltásával. Az ANZDFTPWD parancs kinyomtatja a megtalált profilok listáját, és az ezeken végrehajtott tevékenységet.

Megjegyzés: A jelszavak tárolása a rendszer egyirányú módon titkosított formában történik. Ez azt jelenti, hogy a visszafejtésük nem lehetséges. A rendszer a megadott jelszót titkosítja, és a szintén titkosított formában tárolt jelszóval hasonlítja össze. A jogosultsági hibák (*AUTFAIL) megfigyelésekor a rendszer PW megfigyelési napló bejegyzést ír minden olyan felhasználói profilnál, amely *nem* alapértelmezett jelszóval rendelkezik (V4R1 vagy korábbi kiadások esetén). A V4R2 kiadással kezdődően a rendszer az ANZDFTPWD parancs futtatásakor nem ír PW naplóbejegyzéseket.

Bejelentkezési és jelszó tevékenység megfigyelése

Ha aggódik a jogosulatlan rendszerbe lépési kísérletek miatt, akkor a PRTUSRPRF parancs segítségével figyelheti meg a bejelentkezési és jelszó tevékenységet.

Néhány javaslat a jelentés használatához:

- Nézze meg, hogy a rendszeren vannak-e a rendszerváltozóban megadottnál hosszabb lejárati idővel rendelkező felhasználói profilok, és az eltérés indokolt-e. Ha például a jelentésben az USERY jelszavának érvényessége 120 nap, akkor érdemes utánanézni, hogy ez miért van így.
- A jelentést futtassa rendszeres időközönként a sikertelen bejelentkezési kísérletek megfigyelése érdekében. Ha valaki megpróbál betörni a rendszerbe, az valószínűleg tisztában van azzal, hogy a rendszer valamilyen módon reagál bizonyos számú sikertelen bejelentkezési kísérlet esetén. Ebben az esetben a betörő éjszakánként megpróbálkozhat néhány (kevesebb, mint a QMAXSIGN) bejelentkezési kísérlettel anélkül, hogy ez riasztáshoz vezetne. Ha viszont a jelentést minden reggel lefuttatva látja, hogy bizonyos profiloknál sikertelen bejelentkezési kísérletek történtek, akkor erősen gyanítható, hogy valamilyen probléma lépett fel.
- Ellenőrizze azokat a profilokat, amelyeket hosszú ideje nem használtak, vagy amelyek jelszava hosszú ideje nem változott.

Jelszó információk tárolása

Bizonyos hálózati funkciók és kommunikációs követelmények támogatása érdekében az iSeries szerverek lehetőséget nyújtanak visszafejthető jelszavak biztonságos tárolására. A rendszer ezekkel a jelszavakkal lép például SLIP kapcsolatba egy másik rendszerrel. (A tárolt jelszavak ilyetén felhasználását a “Kimenő szekciók biztonsága” oldalszám: 126 szakasz írja le.)

Az iSeries szerverek ezeket a speciális jelszavakat olyan védett területen tárolják, amely nem érhető el felhasználói programok vagy illesztők számára. Ilyen jelszavakat csak erre kifejezetten feljogosított rendszerfunkciók állíthatnak be vagy kérdezhetnek le.

A SLIP kapcsolatok jelszavának tárolását például a konfigurációs profilt létrehozó (WRKTCPPTP) rendszer parancs végzi el. A parancs használatához *IOSYSCFG jogosultság szükséges. A hívás során a jelszót egy speciálisan kódolt kapcsolati parancsfájl kérdezi le és fejti vissza. A titkosított jelszó sem a felhasználó számára nem jelenik meg, sem munkanaplóba nem kerül be.

A biztonsági adminisztrátornak kell eldöntenie, hogy engedélyezi-e a rendszeren a visszafejthető jelszavak tárolását. Ez a Szerver biztonsági adatok megtartása (QRETSVRSEC) rendszerváltozóval adható meg. Az alapértelmezett érték 0 (Nem). Más szavakkal a rendszer nem tárol visszafejthető jelszavakat, kivéve akkor, ha ezt kifejezetten engedélyezi a rendszerváltozó beállításával.

Ha bizonyos hálózati vagy kommunikációs szolgáltatások tárolt jelszót igényelnek, akkor ki kell alakítani az ennek megfelelő stratégiákat, illetve meg kell ismerni és érteni a kommunikációs partnerek által alkalmazott stratégiákat és gyakorlatot. Ha például SLIP kapcsolaton keresztül csatlakozik egy másik iSeries szerverhez, akkor meg kell fontolni mindkét rendszeren egy speciális, csak a szekció kialakításához használható felhasználói profil létrehozását. A speciális profilok a rendszeren csak korlátozott jogosultságokkal rendelkezzenek. Ez korlátozza a rendszerre gyakorolt káros hatások kiterjedését abban az esetben, ha a partner rendszeren tárolt jelszó ismertté válik.

4. fejezet iSeries beállítása a Biztonsági eszközök használatára

Ez a szakasz írja le a rendszer beállítását az OS/400 részeként rendelkezésre álló biztonsági eszközök használatára. A biztonsági eszközök az OS/400 telepítése után készen állnak a használatra. A biztonsági eszközök használati eljárásaival kapcsolatban az alábbi témakörök szolgálnak javaslatokkal.

Biztonsági eszközök biztonságos használata

Az OS/400 telepítésekor a biztonsági eszközökhöz tartozó objektumok védettek. A biztonsági eszközök biztonságos használatához kerülje a biztonsági eszközök objektumaira vonatkozó jogosultságok módosítását.

A biztonsági eszközök objektumaira vonatkozó biztonsági beállítások és követelmények a következők:

- A biztonsági eszközök programjai és parancsai a QSYS termékkönyvtárban találhatók. A parancsok és programok alapértelmezett nyilvános jogosultsága *EXCLUDE. Több biztonsági eszköz parancs is létrehoz különféle fájlokat a QUSRSYS könyvtárban. Az ilyen fájlok létrehozásakor az ezekre vonatkozó nyilvános jogosultság szintén *EXCLUDE.

  A megváltozott jelentések előállításához szükséges információkat tároló fájlok nevének kezdete QSEC. A felhasználói profilok kezelésére vonatkozó információkat tartalmazó fájlok nevének kezdete QASEC. Ezek a fájlok bizalmas rendszerinformációkat tartalmaznak. Ennek megfelelően a fájlok nyilvános jogosultságát ne módosítsa.
- A biztonsági eszközök a szokásos rendszerbeállításokat használják a közvetlenül nyomtatott kimenetekhez. Ezek a jelentések bizalmas rendszerinformációkat tartalmaznak. A kimenet védett kimeneti sorba irányításához végezze el a biztonsági eszközöket futtató felhasználói profil vagy a felhasználók jobleírásának megfelelő módosítását.
- Biztonsági funkcióik miatt illetve mivel a rendszeren igen sok objektumhoz hozzáférhetnek, a biztonsági eszköz parancsok *ALLOBJ speciális jogosultságot igényelnek. Egyes parancsok emellett *SECADM, *AUDIT vagy *IOSYSCFG speciális jogosultságot is megkövetelhetnek. A parancsok sikeres futtatása érdekében a biztonsági eszközök használatához érdemes adatvédelmi megbízottként bejelentkezni. Ilyenkor nincs szükség magánjogosultságok adományozására a biztonsági eszköz parancsok futtatásához.

Fájl ütközések elkerülése

A biztonsági eszközök jelentési parancsainak nagy része létrehoz egy adatbázisfájlt, amelyet a jelentés megváltozott változatának kinyomtatására használhat fel. Az egyes parancsok által használt fájlok neveit a “Biztonsági parancsok parancsnevei és menüi” oldalszám: 30 írja le. Egy parancsot egyszerre csak egy jobból futtathat. A parancsok legnagyobb része ezt ellenőrzi és be is tartatja. Ha egy parancsot úgy kíván futtatni, hogy egy másik job még nem fejezte be ugyanannak a parancsnak a feldolgozását, akkor hibaüzenet jelenik meg.

A nyomtatási jobok nagy része hosszú ideig futó job. A fájl ütközések elkerülése miatt körültekintéssel kell eljárni, ha a jelentéseket kötegelt jobokhoz adja hozzá vagy job ütemezőbe veszi fel. Elképzelhető például, hogy a PRTUSRPRF jelentésnek kétféle változatát szeretné kinyomtatni eltérő kiválasztási feltételek mellett. Ha a jelentéseket köteghez adja hozzá, akkor ehhez olyan jobsort kell használnia, amely egyszerre csak egy jobot futtat, így biztosítva, hogy a jelentési jobok egymás után futnak le.

A job ütemező használata esetén a két jobot elég távolra kell ütemezni egymástól, hogy az első változat a második job elindulása előtt befejeződhessen.

Biztonsági eszközök mentése

A biztonsági eszköz programok mentésére a Rendszer mentése (SAVSYS) parancs valamennyi futtatásakor sor kerül, beleértve azokat az eseteket is, amikor a parancs a Mentés menü valamelyik menüpontjának kiválasztásakor fut le.

A biztonsági eszközökhöz tartozó fájlok a QUSRSYS könyvtárban vannak. Ezt a könyvtárat a szokásos mentési eljárások részeként egyébként is menteni kellene. A QUSRSYS könyvtár a rendszer több licencprogramjának adatait is tartalmazza. A QUSRSYS könyvtár mentését elvégző parancsokról és menüpontokról további részleteket az Információs központból tudhat meg.

Biztonsági parancsok parancsnevei és menüi

Ez a szakasz írja le a biztonsági eszközök parancsait és menüit. A szakasz példákat is bemutat a parancsok használatára.

A biztonsági eszközökhöz két menü áll rendelkezésre:

- A SECTOOLS (Biztonsági eszközök) menü használható a parancsok interaktív futtatására.
- A SECBATCH (Biztonsági jelentések kötegelt elküldése vagy ütemezése) menü segítségével futtathatók a parancsok kötegelt módon. A SECBATCH menü két részből áll. A menü első része a Job elküldése (SBMJOB) parancs segítségével küldi el kötegelve a jelentéseket azonnali feldolgozás céljából.

  A menü második része a Job ütemezési bejegyzés hozzáadása (ADDJOBSCDE) parancsot alkalmazza. Segítségével lehetősége nyílik a biztonsági jelentések ütemezésére.

Biztonsági eszközök menü menüpontjai

A menüpontokat és a hozzájuk tartozó parancsokat a 6. táblázat: sorolja fel:

6. táblázat: Felhasználói profilokra vonatkozó parancsok

Menüpont[1]	Parancs neve	Leírás	Felhasznált adatbázisfájl
1	ANZDFTPWD	Az Alapértelmezett jelszavak elemzése parancs használható a profil nevével megegyező jelszóval rendelkező felhasználói profilok kikeresésére, és ezeken a megadott tevékenység végrehajtására.	QASECPWD[2]
2	DSPACTPRFL	Az Aktív profilok listájának megjelenítése parancs használható az ANZPRFACT feldolgozás alól kivett felhasználói profilok listájának megjelenítésére vagy nyomtatására.	QASECIDL[2]
3	CHGACTPRFL	Az Aktív profilok listájának módosítása paranccsal szerkesztheti az ANZPRFACT parancs alól kivételt képező felhasználók profiljait. Az aktív profilok listáján szereplő felhasználói profilok folyamatosan aktívak (amíg el nem távolítja a profilt a listából). Az ANZPRFACT parancs az inaktív időtartamra való tekintet nélkül nem tilt le olyan profilt, amely szerepel az aktív profilok listáján.	QASECIDL[2]

6. táblázat: Felhasználói profilokra vonatkozó parancsok (Folytatás)

Menüpont[1]	Parancs neve	Leírás	Felhasznált adatbázisfájl
4	ANZPRFACT	A Profil aktivitás elemzése parancs segítségével tilthatja le a megadott számú napon keresztül inaktív felhasználói profilokat. Miután az ANZPRFACT paranccsal meghatározta a napok számát, a rendszer éjszakánként automatikusan futtatja az ANZPRFACT jobot. A letiltás alól kivenni kívánt felhasználói profilokat a CHGACTPRFL paranccsal határozhatja meg.	QASECIDL[2]
5	DSPACTSCD	A Profil aktiválás ütemezésének megjelenítése paranccsal jelenítheti meg vagy nyomtathatja ki a a felhasználói profilok engedélyezésre vagy letiltásra ütemezésére vonatkozó információit. Az ütemezést a CHGACTSCDE paranccsal hozhatja létre.	QASECACT[2]
6	CHGACTSCDE	Az Aktiválás ütemezési bejegyzés módosítása paranccsal adhatja meg, hogy egy felhasználói profil csak bizonyos időkben legyen elérhető bejelentkezés céljából. A rendszer valamennyi ütemezett felhasználói profilhoz létrehozza a profil engedélyezését és letiltását végző jobok ütemezési bejegyzéseit.	QASECACT[2]
7	DSPEXPSCD	A Lejárat ütemezésének megjelenítése paranccsal jelenítheti meg vagy nyomtathatja ki a letiltásra vagy eltávolításra beütemezett felhasználói profilok listáját. A felhasználói profilok érvényességét a CHGEXPSCDE paranccsal állíthatja be.	QASECEXP[2]
8	CHGEXPSCDE	A Lejárat ütemezési bejegyzés módosítása paranccsal ütemezhet be eltávolításra egy felhasználói profilt. Az eltávolítás lehet ideiglenes (letiltás) vagy végleges (törlés). A parancs által használt job ütemezési bejegyzés minden nap 1 perccel éjfél után fut le. A job a QASECEXP fájl alapján határozza meg, hogy aznap milyen felhasználói profilok járnak le. A lejáratra beütemezett felhasználói profilok listájának megjelenítésére a DSPEXPSCD parancsot használhatja.	QASECEXP[2]
9	PRTPRFINT	A Profil belső információk nyomtatása parancs segítségével nyomtathatja ki a felhasználói profilban lévő bejegyzések számára vonatkozó információkat. A bejegyzések száma határozza meg a felhasználói profil méretét.	

Megjegyzések:

1. A SECTOOLS menü menüpontjai.
2. Ez a fájl a QUSRSYS könyvtárban található.

A képernyő lapozásával további lehetőségeket jeleníthet meg. A 7. táblázat: oldalszám: 32 a biztonsági megfigyeléssel kapcsolatos parancsokat és menüpontokat sorolja fel:

7. táblázat: Biztonsági megfigyelésre vonatkozó parancsok

Menüpont[1]	Parancs neve	Leírás	Felhasznált adatbázisfájl
10	CHGSECAUD	A Biztonsági megfigyelés módosítása paranccsal állíthatja be a biztonsági megfigyelést, illetve módosíthatja a biztonsági megfigyelést vezérlő rendszerváltozókat. A CHGSECAUD parancs futtatásakor a rendszer létrehozza a biztonsági megfigyelési (QAUDJRN) naplót, amennyiben az még nem létezik. A CHGSECAUD parancs lehetőségeivel a QAUDLVL (megfigyelési szint) rendszerváltozó egyszerűben beállítható. Az *ALL megadásával minden lehetséges megfigyelési szint aktiválható. A *DFTSET megadása csak a leggyakrabban használt beállításokat (*AUTFAIL, *CREATE, *DELETE, *SECURITY és *SAVRST) aktiválja. **Megjegyzés:** Ha a biztonsági eszközök segítségével állítja be a megfigyelést, akkor ne feledje el megtervezni a megfigyelési napló fogadóinak kezelését. Ennek hiányában hamar lemezkihasználtsági problémákba ütközhet.	
11	DSPSECAUD	A Biztonsági megfigyelés megjelenítése parancs segítségével jelenítheti meg a biztonsági megfigyelési naplóra vonatkozó információkat, illetve a biztonsági megfigyeléssel kapcsolatos rendszerváltozók értékét.	

Megjegyzések:

1. A SECTOOLS menü menüpontjai.

Kötegelt biztonsági jelentések menü használata

A következő ábrán látható a SECBATCH menü első része:

```
SECBATCH         Submit or Schedule Security Reports To Batch
                                                                  System:
Select one of the following:

  Submit Reports to Batch
     1. Adopting objects
     2. Audit journal entries
     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
```

A menüpontok kiválasztásakor a Job elküldése (SBMJOB) képernyő jelenik meg. Ha módosítani kívánja a parancs alapértelmezett paramétereit, akkor nyomja meg a *Futtatandó parancs* sorban az F4 (Parancssor) billentyűt.

A Kötegelt jelentések ütemezése lehetőség megjelenítéséhez görgesse lefelé a SECBATCH menüt. A menünek ezen a részén található menüpontok használatával állíthatja be, hogy a

rendszer rendszeres időközönként lefuttassa a megváltozott változatokat. A további menüpontok megjelenítéséhez görgesse lefelé a képernyőt. A menünek ebben a szakaszában található menüpontok kiválasztásakor a Job ütemezési bejegyzés hozzáadása (ADDJOBSCDE) képernyő jelenik meg.

Ha a jelentésben az alapértelmezéstől eltérő beállításokat kíván alkalmazni, akkor vigye a kurzort a *Futtatandó parancs* sor fölé, és nyomja meg az F4 (Parancssor) billentyűt. A jobnak jelentéssel bíró nevet adjon meg, hogy felismerje a job ütemezési bejegyzések megtekintése esetén.

Kötegelt biztonsági jelentések menü menüpontjai

A biztonsági jelentésekhez kapcsolódó menüpontokat és parancsneveket a 8. táblázat: sorolja fel.

A biztonsági jelentések futtatásakor a rendszer csak azokat az információkat nyomtatja ki, amelyek megfelelnek a megadott feltételeknek és az eszköz feltételeinek is. A felhasználói profil nevet megadó jobleírások például biztonsággal kapcsolatosak. Ennek megfelelően a jobleírás (PRTJOBDAUT) jelentés a megadott könyvtárnak csak azon jobleírásait nyomtatja ki, amelynek nyilvános jogosultsága nem *EXCLUDE *és* amelyek a USER paraméterben megadják egy felhasználói profil nevét.

Hasonlóan, az alrendszer információk kinyomtatásakor (PRTSBSDAUT parancs) a rendszer egy alrendszerről csak akkor nyomtatja ki az információkat, ha az rendszerleírás felhasználói profilt meghatározó bejegyzéssel rendelkező kommunikációs bejegyzést tartalmaz.

Ha egy adott jelentés a vártnál kevesebb információt nyomtat ki, akkor az online súgó segítségével tájékozódjon a jelentésben alkalmazott kiválasztási feltételek felől.

8. táblázat: Biztonsági jelentések parancsai

Menüpont[1]	Parancs neve	Leírás	Felhasznált adatbázisfájl
1, 40	PRTADPOBJ	Az Átvevő objektumok kinyomtatása paranccsal nyomtathatja ki a megadott felhasználói profil jogosultságait átvevő objektumok listáját. Megadható egyetlen profil, általános profilnév (például minden Q betűvel kezdődő profil) vagy minden felhasználói profil. A jelentés két változatban készülhet. A teljes jelentés a kiválasztási feltételnek megfelelő összes átvevő objektumot felsorolja. A változások jelentése a rendszer jelenlegi átvevő objektumai és a legutóbbi futtatás alkalmával a rendszeren talált átvevő objektumok közötti különbségeket sorolja fel.	QSECADPOLD[2]
2, 41	DSPAUDJRNE	A Megfigyelési napló bejegyzések nyomtatása paranccsal jelenítheti meg vagy nyomtathatja ki a biztonsági megfigyelési napló bejegyzéseinek információit. Kiválaszthat bizonyos bejegyzéstípusokat, egyéni felhasználókat vagy időtartamot.	QASYxxJ4[3]

8. táblázat: Biztonsági jelentések parancsai (Folytatás)

Menüpont[1]	Parancs neve	Leírás	Felhasznált adatbázisfájl
3, 42	PRTPVTAUT *AUTL	A Magánjogosultságok kinyomtatása parancs *AUTL objektumokon való használatával kaphatja meg a rendszer összes jogosultsági listájának felsorolását. A jelentés minden egyes listánál tartalmazza a jogosult felhasználókat, és az általuk birtokolt jogosultságokat. A parancs által nyújtott információkat segítségképpen használhatja fel a rendszer objektumaira vonatkozó jogosultságok forrásainak elemzése során. A jelentés három változatban készülhet. A teljes jelentés a rendszer valamennyi jogosultsági listáját tartalmazza. A változásokról készült jelentés a legutóbbi futtatás óta történt hozzáadásokat és módosításokat tartalmazza. A törlésekről készült jelentés azokat a felhasználókat sorolja fel, amelyeknek a jogosultsági listán megadott jogosultsága törlődött a jelentés legutóbbi elkészítése óta. Teljes jelentés nyomtatásakor lehetőség van az egyes jogosultsági listák által védett objektumok listájának kinyomtatására is. A rendszer ilyenkor minden jogosultsági listához külön jelentést állít elő.	QSECATLOLD[2]
6, 45	PRTCMNSEC	A Kommunikációs biztonság kinyomtatása paranccsal nyomtathatja ki a rendszer kommunikációját befolyásoló objektumok biztonsággal kapcsolatos beállításait. Ezek a beállítások határozzák meg, hogyan léphetnek be a jobok és felhasználók a rendszerre. A parancs két jelentést állít elő: az egyik jelentésben a rendszer konfigurációs listáinak beállításai szerepelnek; a másikban a vonalleírások, vezérlők és eszközleírások biztonsággal kapcsolatos paraméterei találhatók. Mindegyik jelentésnek van teljes és változásokat felsoroló változata.	QSECCMNOLD[2]
15, 54	PRTJOBDAUT	A Jobleírás jogosultságának kinyomtatása paranccsal nyomtathatja ki a felhasználói profilt meghatározó, ezzel egyidőben az *EXCLUDE-tól eltérő nyilvános jogosultsággal rendelkező jobleírások listáját. A jelentésben szerepelnek a jobleírásban megadott felhasználói profil speciális jogosultságai is. A jelentés két változatban készülhet. A teljes jelentés a kiválasztási feltételeknek megfelelő összes jobleírás objektumot tartalmazza. A változásokról készült jelentés a rendszer jelenlegi jobleírás objektumai és a legutóbbi futtatás alkalmával a rendszeren talált jobleírás objektumok közötti különbségeket sorolja fel.	QSECJBDOLD[2]

8. táblázat: Biztonsági jelentések parancsai (Folytatás)

Menüpont[1]	Parancs neve	Leírás	Felhasznált adatbázisfájl
Lásd a 4. megjegyzést.	PRTPUBAUT	A Nyilvános jogosultsággal rendelkező objektumok kinyomtatása paranccsal nyomtathatja ki azon objektumok listáját, amelyek nyilvános jogosultsága nem *EXCLUDE. A parancs futtatásakor meg kell adni egy objektumtípust és az objektumok keresési könyvtárait. A PRTPUBAUT parancs segítségével nyomtathatja ki azoknak az objektumoknak a listáját, amelyekhez a rendszer valamennyi felhasználója hozzáférhet. A jelentés két változatban készülhet. A teljes jelentés a kiválasztási feltételnek megfelelő összes objektumot felsorolja. A változásokról készült jelentés a rendszeren jelenleg található megadott objektumok és a jelentés legutóbbi futtatásának alkalmával a rendszeren talált (azonos típusú és könyvtárban található) objektumok közötti különbségeket sorolja fel.	QPBxxxxxx[5]
Lásd az 5. megjegyzést.	PRTPVTAUT	A Magánjogosultságok kinyomtatása paranccsal nyomtathatja ki a megadott könyvtár adott típusú, magánjogosultságokkal rendelkező objektumait. Ezt a jelentést segítségképpen használhatja fel az objektumokra vonatkozó jogosultságok forrásainak meghatározásakor. A jelentés három változatban készülhet. A teljes jelentés a kiválasztási feltételnek megfelelő összes objektumot felsorolja. A változásokról készült jelentés a rendszeren jelenleg található megadott objektumok és a jelentés legutóbbi futtatásának alkalmával a rendszeren talált (azonos típusú és könyvtárban található) objektumok közötti különbségeket sorolja fel. A törlésekről készült jelentés azokat a felhasználókat sorolja fel, amelyeknek egy objektumra vonatkozó jogosultsága törlődött a jelentés legutóbbi elkészítése óta.	QPVxxxxxx[5]
24, 63	PRTQAUT	A Sor jelentés kinyomtatása paranccsal nyomtathatja ki a rendszer kimeneti- és jobsorainak biztonsági beállításait. Ezek a beállítások határozzák meg, hogy ki tekintheti meg és módosíthatja a kimeneti- vagy jobsor bejegyzéseit. A jelentés két változatban készülhet. A teljes jelentés a kiválasztási feltételnek megfelelő összes kimeneti- és jobsor objektumot felsorolja. A változásokról készült jelentés a rendszer jelenlegi kimeneti- és jobsor objektumai illetve a legutóbbi futtatás alkalmával a rendszeren talált kimeneti- és jobsor objektumok közötti különbségeket sorolja fel.	QSECQOLD[2]

8. táblázat: Biztonsági jelentések parancsai (Folytatás)

Menüpont[1]	Parancs neve	Leírás	Felhasznált adatbázisfájl
25, 64	PRTSBSDAUT	Az Alrendszerleírás kinyomtatása paranccsal nyomtathatja ki a rendszeren található alrendszerleírások biztonsággal kapcsolatos kommunikációs bejegyzéseit. Ezek a beállítások határozzák meg, hogyan léphetnek be a jobok a rendszerbe, és hogyan futnak le. A jelentésben csak azok az alrendszerleírások szerepelnek, amelyek felhasználói profilt meghatározó kommunikációs bejegyzéssel rendelkeznek. A jelentés két változatban készülhet. A teljes jelentés a kiválasztási feltételeknek megfelelő összes alrendszerleírás objektumot tartalmazza. A változásokról készült jelentés a rendszer jelenlegi alrendszerleírás objektumai és a legutóbbi futtatás alkalmával a rendszeren talált alrendszerleírás objektumok közötti különbségeket sorolja fel.	QSECSBDOLD[2]
26, 65	PRTSYSSECA	A Rendszer biztonsági attribútumok kinyomtatása paranccsal nyomtathatja ki a biztonsággal kapcsolatos rendszerváltozókat és hálózati attribútumokat. A jelentés az aktuális értékeket és a javasolt értékeket tartalmazza.	
27, 66	PRTTRGPGM	A Trigger programok kinyomtatása parancs használható a rendszer adatbázisfájljaihoz társított trigger programok listájának kinyomtatására. A jelentés két változatban készülhet. A teljes jelentésben minden olyan trigger program szerepel, amely hozzá van rendelve, és megfelel a kiválasztási feltételeknek. A változásokról készült jelentés csak azokat a trigger programokat sorolja fel, amelyek a jelentés legutóbbi futtatása óta kerültek hozzárendelésre.	QSECTRGOLD[2]
28, 67	PRTUSROBJ	A Felhasználói objektumok kinyomtatása paranccsal nyomtathatja ki a könyvtárak felhasználói (vagyis nem az IBM által szállított) objektumainak listáját. Ezzel a jelentéssel szerezheti meg a könyvtárlista rendszer részének könyvtáraiban (például QSYS) található felhasználói objektumok listáját. A jelentés két változatban készülhet. A teljes jelentés a kiválasztási feltételeknek megfelelő összes felhasználói objektumot tartalmazza. A változásokról készült jelentés a rendszer jelenlegi felhasználói objektumai és a legutóbbi futtatás alkalmával a rendszeren talált felhasználói objektumok közötti különbségeket sorolja fel.	QSECPUOLD[2]
29, 68	PRTUSRPRF	A Felhasználói profil kinyomtatása paranccsal elemezheti a megadott feltételeknek megfelelő felhasználói profilokat. A felhasználói profilok speciális jogosultságok, felhasználói osztály vagy a speciális jogosultságok és a felhasználói osztály közötti különbségek alapján választhatók ki. A jelentésben jogosultsági információk, környezeti információk és jelszó szintre vonatkozó információk nyomtathatók ki.	

8. táblázat: Biztonsági jelentések parancsai (Folytatás)

Menüpont[1]	Parancs neve	Leírás	Felhasznált adatbázisfájl
30, 69	PRTPRFINT	A Profil belső információk nyomtatása paranccsal nyomtathatja ki a bejegyzések számára vonatkozó belső információkat.	
31, 70	CHKOBJITG	Az Objektum integritásának ellenőrzése paranccsal határozhatja meg, hogy a működtethető objektumok (például programok) megváltoztak-e fordítóprogram közreműködése nélkül. Ezzel a paranccsal ismerhetők fel a vírusok vagy jogosulatlan funkciókat végző programrészek bejuttatását célzó kísérletek. A CHKOBJITG parancsról további részleteket az *iSeries biztonsági összefoglaló* című kiadványban talál.	

Megjegyzések:

1. A SECBATCH menü menüpontjai.
2. Ez a fájl a QUSRSYS könyvtárban található.
3. Az xx a naplóbejegyzés kétkarakteres típusa. Az AE naplóbejegyzések modell kimeneti fájlja például a QSYS/QASYAEJ4. A modell kimeneti fájlokat az *iSeries biztonsági összefoglaló* című kiadvány F függeléke írja le.
4. A SECBATCH menü az olyan objektumtípusokhoz tartalmaz beállításokat, amelyek általában gondot szoktak okozni a biztonsági adminisztrátoroknak. A 11. vagy 50. menüponttal futtathatja a PRTPUBAUT parancsot *FILE objektumokon. Az objektumtípus meghatározásához használja az általános beállításokat (18 és 57).
5. A SECBATCH menü az olyan objektumtípusokhoz tartalmaz beállításokat, amelyek általában gondot szoktak okozni a biztonsági adminisztrátoroknak. A 12. vagy 51. menüponttal futtathatja például a PRTPVTAUT parancsot *FILE objektumokon. Az objektumtípus meghatározásához használja az általános beállításokat (19 és 58).
6. A fájl nevében az xxxxxx az objektumtípust jelöli. A program objektumok fájlja például QPBPGM nyilvános jogosultságok és QPVPGM magánjogosultságok esetén. Ezek a fájlok a QUSRSYS könyvtárban találhatók.

   A fájl minden könyvtárra vonatkozóan tartalmaz egy membert, amelyről a jelentést kinyomtatta. A member neve megegyezik a könyvtár nevével.

Biztonság testreszabására szolgáló parancsok

A 9. táblázat: a rendszer biztonságának testreszabására használható parancsokat sorolja fel. Ezek a parancsok a SECTOOLS menüben találhatók.

9. táblázat: Rendszer testreszabására szolgáló parancsok

Menüpont[1]	Parancs neve	Leírás	Felhasznált adatbázisfájl
60	CFGSYSSEC	A Rendszer biztonság beállítása paranccsal állíthatja be a biztonsággal kapcsolatos rendszerváltozókat az ajánlott értékekre. A parancs emellett a rendszer biztonsági megfigyelését is beállítja. A parancs tevékenységét “A rendszer biztonságának beállítása parancs által beállított értékek” oldalszám: 38 szakasz írja le. **Megjegyzés:** Egy adott helyzetre vonatkozó biztonsági javaslatokért a parancs végrehajtása helyett futtassa az iSeries biztonsági varázslót, vagy használja az iSeries biztonsági tanácsadót. Az eszközöket részletesen a 2. fejezet, “iSeries biztonsági varázsló és eServer biztonsági tervező”, oldalszám: 11 szakasz írja le.	

9. táblázat: Rendszer testreszabására szolgáló parancsok (Folytatás)

Menüpont[1]	Parancs neve	Leírás	Felhasznált adatbázisfájl
61	RVKPUBAUT	A Nyilvános jogosultság visszavonása paranccsal állíthatja be a rendszer biztonsági szempontból érzékeny parancsainak nyilvános jogosultságát az *EXCLUDE értékre. A RVKPUBAUT parancs tevékenységét “A Nyilvános jogosultság visszavonása parancs funkciói” oldalszám: 40 szakasz írja le.	

Megjegyzések:

1. A SECTOOLS menü menüpontjai.

A rendszer biztonságának beállítása parancs által beállított értékek

A CFGSYSSEC parancs által beállított rendszerváltozókat a 10. táblázat: sorolja fel. A CFGSYSSEC parancs a QSYS/QSECCFGS nevű programot futtatja.

10. táblázat: A CFGSYSSEC parancs által beállított értékek

Rendszerváltozó neve	Beállítás	Rendszerváltozó leírása
QALWOBJRST	*NONE	Megadja, hogy a rendszerállapotú és jogosultságot átvevő programok visszaállíthatók-e.
QAUTOCFG	0 (Nem)	Új eszközök automatikus konfigurációja.
QAUTOVRT	0	A rendszer által automatikusan létrehozott virtuális eszköz leírások száma, amennyiben nincs használható eszköz.
QDEVRCYACN	*DSCMSG (Szétkapcsolás és üzenet)	A rendszer tevékenysége a kommunikáció ismételt kialakításakor.
QDSCJOBITV	120	A rendszer által a szétkapcsolt jobokon végrehajtott tevékenység előtti várakozási idő.
QDSPSGNINF	1 (Igen)	Megadja, hogy a felhasználóknak megjelenik-e a bejelentkezési képernyő.
QINACTITV	60	A rendszer által az inaktív interaktív jobokon végrehajtott tevékenység előtti várakozási idő.
QINACTMSGQ	*ENDJOB	A rendszer által az inaktív jobokon végrehajtott tevékenység.
QLMTDEVSSN	1 (Igen)	Megadja, hogy a felhasználók egyszerre csak egy eszközön léphetnek-e be.
QLMTSECOFR	1 (Igen)	Megadja, hogy az *ALLOBJ vagy *SERVICE speciális jogosultsággal rendelkező felhasználók csak adott eszközökön léphetnek-e be.
QMAXSIGN	3	Az egymást követő sikertelen bejelentkezési kísérletek megengedett száma.
QMAXSGNACN	3 (Mindkettő)	Megadja, hogy a QMAXSIGN korlát elérésekor a rendszer letiltja-e a munkaállomás vagy a felhasználói profilt.
QRMTSIGN	*FRCSIGNON	A távoli (átjelentkezés vagy Telnet) bejelentkezési kísérletek kezelésének módja.
QRMTSVRATR	0 (Ki)	Engedélyezi a rendszer távoli elemzését.
QSECURITY [1] oldalszám: 39	50	A biztonsági szint.
QVFYOBJRST	3 (Aláírások ellenőrzése visszaállítás során)	Objektum ellenőrzése a visszaállítás során.
QPWDEXPITV	60	Milyen gyakran kell cserélniük a felhasználóknak a jelszavakat.
QPWDMINLEN	6	Jelszavak minimális hossza.

10. táblázat: A CFGSYSSEC parancs által beállított értékek (Folytatás)

Rendszerváltozó neve	Beállítás	Rendszerváltozó leírása
QPWDMAXLEN	8	Jelszavak maximális hossza.
QPWDPOSDIF	1 (Igen)	Megadja, hogy az új jelszó minden pozíciójában az előző jelszó azonos pozíciójában szereplő karaktertől különböző karakternek kell állnia.
QPWDLMTCHR	Lásd: Megjegyzés 2.	Jelszavakban nem megengedett karakterek.
QPWDLMTAJC	1 (Igen)	Megadja, hogy a jelszavakban tiltottak-e az egymást követő számok.
QPWDLMTREP	2 (Egymást követően nem ismételhető)	Megadja, hogy a karakterek ismétlése tiltott-e a jelszavakban.
QPWDRQDDGT	1 (Igen)	Megadja, hogy a jelszavakban lennie kell-e legalább egy számnak.
QPWDRQDDIF	1 (32 egyedi jelszó)	Hány egyedi jelszót kell beállítani, mielőtt egy jelszó ismételhető lenne.
QPWDVLDPGM	*NONE	A rendszer által a jelszavak ellenőrzése céljából meghívott végprogram.

Megjegyzések:

1. Ha a rendszer jelenleg 40-es vagy alacsonyabb QSECURITY érték mellett fut, akkor magasabb biztonsági szintre váltás előtt olvassa el az *iSeries biztonsági összefoglaló* 2. fejezetét.
2. A tiltott karakterek a QSYS/QCPFMSG üzenetfájlban tárolódnak a CPXB302 üzenetazonosító alatt. Gyári alapértelmezés szerint ezek a következők: AEIOU@$#. A korlátozott karakterek módosításához használja az Üzenetleírás módosítása (CHGMSGD) parancsot. A QPWDLMTCHR rendszerváltozó 2. és 3. jelszó szinteken nem érvényesül.

A CFGSYSSEC parancs emellett *NONE-ra állítja a következő IBM által szállított felhasználói profilok jelszavait:

QSYSOPR

QPGMR

QUSER

QSRV

QSRVBAS

Végül a CFGSYSSEC a Biztonsági megfigyelés módosítása (CHGSECAUD) paranccsal beállítja a rendszeren a biztonsági megfigyelést. A CFGSYSSEC az objektumok és események megfigyelését aktiválja, továbbá megadja a CHGSECAUD parancsban az alapértelmezésben megfigyelt tevékenységeket is.

A program testreszabása

Ha a beállítások valamelyike nem megfelelő az adott környezet számára, akkor létrehozhat saját programot a parancs feldolgozására. Tegye a következőket:

__ Lépés 1. A CL forrás visszakeresése (RTVCLSRC) parancs segítségével másolja le a CFGSYSSEC parancs használatakor futó program forrását. A visszakeresendő program a QSYS/QSECCFGS. A visszakeresés után adjon neki *eltérő nevet*.

__ Lépés 2. Végezze el a megfelelő módosításokat a programban. Ezután fordítsa le. A fordítás során győződjön meg róla, hogy *nem* írja felül az IBM által szállított QSYS/QSECCFGS programot. A programnak eltérő névvel kell rendelkeznie.

__ Lépés 3. A Parancs módosítása (CHGCMD) parancs segítségével módosítsa a CFGSYSSEC parancs Feldolgozandó program (PGM) paraméterét. A PGM paraméternek az egyéni program nevét adja meg. Ha például a programot a QGPL könyvtárban hozta létre MYSECCFG néven, akkor írja be a következő parancsot:

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

Megjegyzés: A QSYS/QSECCFGS program módosítása esetén az IBM nem tudja garantálni a program megbízhatóságát, javíthatóságát, teljesítményét és funkcionalitását. A kereskedelmi értékesíthetőségre és az adott célra való alkalmasságra vonatkozó vélelmezett garanciát az IBM ugyancsak kifejezetten elutasítja.

A Nyilvános jogosultság visszavonása parancs funkciói

A Nyilvános jogosultság visszavonása (RVKPUBAUT) paranccsal állíthatja be egy sor parancs és program nyilvános jogosultságát az *EXCLUDE értékre. A RVKPUBAUT parancs a QSYS/QSECRVKP programot futtatja. Eredeti formájában a QSECRVKP program a 11. táblázat: helyen felsorolt parancsok, illetve a 12. táblázat: helyen felsorolt alkalmazásprogram illesztők (API) nyilvános jogosultságait vonja vissza a nyilvános jogosultság *EXCLUDE értékre állításával. A rendszer megérkezésekor ezen programok és API-k nyilvános jogosultsága a *USE értékre van állítva.

A 11. táblázat: helyen felsorolt parancsok és a 12. táblázat: helyen felsorolt API-k mindegyike olyan funkciókat végez a rendszeren, amely lehetőséget nyújthat helytelen felhasználásra. A biztonsági adminisztrátornak a nyilvános jogosultság biztosítása helyett kifejezetten fel kell jogosítania a megfelelő felhasználókat ezen parancsok és programok futtatására.

A RVKPUBAUT parancs futtatásakor meg kell adni a parancsokat tartalmazó könyvtárat. Az alapértelmezés a QSYS könyvtár. Ha a rendszeren egynél több nemzeti nyelv van telepítve, akkor a parancsot minden egyes QSYSxxx könyvtárra le kell futtatni.

11. táblázat: A RVKPUBAUT parancs által beállított nyilvános jogosultságú parancsok

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

A 12. táblázat: helyen megadott összes API a QSYS könyvtárban található:

12. táblázat: A RVKPUBAUT parancs által beállított nyilvános jogosultságú programok

QTIENDSUP
QTISTRSUP
QWTCTLTR
QWTSETTR
QY2FTML

A RVKPUBAUT parancs futtatásakor a rendszer a gyökér katalógus nyilvános jogosultságát a *USE értékre állítja (kivéve ha már *USE vagy annál korlátozóbb).

A program testreszabása

Ha a beállítások valamelyike nem megfelelő az adott környezet számára, akkor létrehozhat saját programot a parancs feldolgozására. Tegye a következőket:

__ Lépés 1. A CL forrás visszakeresése (RTVCLSRC) parancs segítségével másolja le a RVKPUBAUT parancs használatakor futó program forrását. A visszakeresendő program a QSYS/QSECRVKP. A visszakeresés után adjon neki *eltérő nevet*.

__ Lépés 2. Végezze el a megfelelő módosításokat a programban. Ezután fordítsa le. A fordítás során győződjön meg róla, hogy *nem* írja felül az IBM által szállított QSYS/QSECRVKP programot. A programnak eltérő névvel kell rendelkeznie.

__ Lépés 3. A Parancs módosítása (CHGCMD) parancs segítségével módosítsa a RVKPUBAUT parancs Feldolgozandó program (PGM) paraméterét. A PGM paraméternek az egyéni program nevét adja meg. Ha például a programot a QGPL könyvtárban hozta létre MYRVKPGM néven, akkor írja be a következő parancsot:

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

Megjegyzés: A QSYS/QSECRVKP program módosítása esetén az IBM nem tudja garantálni a program megbízhatóságát, javíthatóságát, teljesítményét és funkcionalitását. A kereskedelmi értékesíthetőségre és az adott célra való alkalmasságra vonatkozó vélelmezett garanciát az IBM ugyancsak kifejezetten elutasítja.

2. rész iSeries biztonság speciális funkciói

5. fejezet Információs tulajdon védelme objektum jogosultságokkal

A biztonsági adminisztrátorok számára a legnagyobb kihívást az jelenti, hogy a vállalati információs tulajdon védelmét a rendszer felhasználóinak frusztrálása nélkül biztosítsák. Meg kell győződni arról, hogy a felhasználók elegendő jogosultsággal rendelkeznek a munkájuk elvégzéséhez, egyszersmind nincs jogosultságuk a teljes rendszer böngészésére és nem kívánt módosítások végrehajtására.

Biztonsági tipp

A túl szoros biztonság gyakran visszafelé sülhet el. A felhasználók a túlságosan korlátozó jogosultságokat gyakran ellentételezik jelszavaik megosztásával.

Az OS/400 operációs rendszer integrált objektum biztonságot nyújt. A felhasználóknak a rendszer által nyújtott felületeket kell használniuk az objektumok elérésére. Ha például egy adatbázisfájlhoz szeretnének hozzáférni, akkor egy adatbázisfájlok kezelésére szolgáló paranccsal vagy programmal kell ezt megtenniük. Az üzenetsorok vagy munkanaplók kezelésére szolgáló parancsokkal végzett kísérletek nem vezetnek eredményre.

Amikor a felhasználó egy felület segítségével objektum hozzáférésre tesz kísérletet, a rendszer minden egyes alkalommal ellenőrzi, hogy a felhasználó rendelkezik-e az objektumra vonatkozó jogosultságokkal, amelyeket megkövetel az adott felület. Az objektum jogosultság hatékony, egyszersmind rugalmas eszköz a rendszeren tárolt információtulajdon védelmére. A biztonsági adminisztrátorok feladata, hogy olyan objektum biztonsági sémát alakítsanak ki, amely kezelhető és karbantartható.

Objektum jogosultságok foganatosítása

Minden egyes alkalommal, amikor egy objektumhoz hozzá próbál férni, a rendszer ellenőrzi az adott objektumra vonatkozó jogosultságait. Ha azonban a rendszer biztonsági szintje (vagyis a QSECURITY rendszerváltozó értéke) 10 vagy 20, akkor minden felhasználó automatikusan jogosult minden objektum elérésére, mivel minden felhasználói profil rendelkezik az *ALLOBJ speciális jogosultsággal.

Objektum jogosultsági tipp: Ha nem biztos az objektum jogosultság foganatosításában, akkor ellenőrizze a QSECURITY (biztonsági szint) rendszerváltozó értékét. Ha a QSECURITY értéke 10 vagy 20, akkor a rendszer nem alkalmaz objektum biztonságot.

A biztonsági szint 30-ra vagy magasabb értékre állítása előtt körültekintően tervezze meg és készítse elő az áttérést. Ellenkező esetben elképzelhető, hogy a felhasználók nem férnek hozzá a szükséges információkhoz.

Az Információs központ **Alapvető rendszerbiztonság és tervezés** című témaköre bemutat egy módszert az alkalmazások elemzésére és az objektum biztonság beállítási módjának meghatározására. Ha nem használ objektum biztonságot, vagy az objektum biztonsági sémája elavult vagy szövevényes, akkor mielőtt bármit tenne, olvassa tovább ezt a témakört.

Menü biztonság

Az iSeries szerver eredetileg az S/36 és S/38 termékek felváltását szolgálta. Az iSeries környezetek tekintélyes része korábban S/36 vagy S/38 környezet volt. A felhasználók által végrehajtható tevékenységek felügyelete érdekében a hőskor biztonsági adminisztrátorai gyakran alkalmazták a **menü biztonság** vagy **menü hozzáférés felügyelet** technikáját.

A menü hozzáférés felügyelet azt jelenti, hogy a felhasználónak a bejelentkezés után megjelenik egy menü. A felhasználó csak a menüben megjelenő funkciókat hajthatja végre. Nem juthat parancssorhoz sem, nehogy a menüben nem szereplő tevékenységet hajtson végre. Elvileg a biztonsági adminisztrátoroknak nem kell aggódniuk az objektumok biztonsága miatt, hiszen a menük és programok felügyelik a felhasználó által végezhető tevékenységeket.

Az iSeries szerver több felhasználói profil beállítást is biztosít a menü hozzáférés felügyelethez; ezek a következők:

- A **Kezdeti menü** (INLMNU) paraméter határozza meg a felhasználó számára a bejelentkezés után megjelenő menüt.
- A **Kezdeti program** (INLPGM) paraméterrel határozható meg egy program, amely még a menü megjelenése előtt lefut. Az INLPGM paraméter segítségével a felhasználó egyetlen program futtatására is korlátozható.
- A **Képességek korlátozása** (LMTCPB) paraméter korlátozhatja a felhasználót egy szűkített parancskészletre. Ez akadályozza meg továbbá a felhasználót abban, hogy eltérő kezdeti programot vagy menüt állítson be magának. (A LMTCPB paraméter csak a parancssorban beírt parancsokra vonatkozik.)

A menü hozzáférés felügyelet korlátai

Az elmúlt néhány évben a számítógépek és a számítógépek felhasználói is jelentős változásokon estek át. Egyre több az olyan eszköz, gondoljunk csak a lekérdezési és táblázatkezelő programokra, amelyek segítségével a felhasználók saját programokat is írhatnak. Bizonyos eszközök, például az SQL vagy az ODBC az információk megtekintése mellett az információk módosítására is lehetőséget nyújt. Az ilyen és ehhez hasonló eszközök menüszerkezeten keresztüli engedélyezése láthatóan igen bonyolult.

A rögzített funkciós (“zöld képernyős”) munkaállomások helyét egyre gyorsuló ütemben veszik át a személyi számítógépek és a számítógépes hálózatok. Ha a rendszer hálózat tagja, akkor a felhasználók anélkül léphetnek be a rendszerre, hogy akár egyszer is találkoznának bejelentkezési képernyővel vagy menüvel.

A menü hozzáférés felügyelet foganatosítására törekvő biztonsági adminisztrátor alapvetően két problémával fog szembesülni:

- Ha sikeresen korlátozza a felhasználókat a megfelelő menükre, akkor a felhasználók csalódottak lesznek, mivel nem használhatják a rendelkezésre álló modernebb eszközöket.
- Ha a korlátozás nem sikeres, akkor ez veszélyeztetheti a menü hozzáférés felügyelet által védeni szándékozott kritikus információk biztonságát. Ha a rendszer emellett hálózatnak is tagja, akkor a menü hozzáférés felügyelet sikeres kialakításának esélye még tovább csökken. A LMTCPB paraméter például csak az interaktív szekciók parancssorában megadott parancsokra vonatkozik. A kommunikációs szekciókon, például PC fájlátvitelen, FTP protokollon vagy távoli parancsokon keresztül érkező kérésekre a LMTCPB paraméter semmilyen hatással nincs.

Menü hozzáférés felügyelet kiegészítése objektum biztonsággal

A rendszerek összekapcsolásához rendelkezésre álló lehetőségek széles skálája miatt a jövő iSeries szerverének biztonsági sémája nem épülhet kizárólag a menü hozzáférés felügyeletre.

Ez témakör ad néhány tanácsot, hogyan egészíthető ki fokozatosan a menü hozzáférés felügyeleti séma objektum biztonsági elemekkel.

Az Információs központ *Alapvető rendszerbiztonság és tervezés* című témaköre bemutat egy technikát, hogyan határozhatók meg a felhasználóknak az aktuális alkalmazások futtatásához minimálisan szükséges objektum jogosultságai. A felhasználókat ezután csoportokhoz kell rendelni, és a csoportoknak meg kell adni a megfelelő jogosultságokat. Ez a megközelítés logikus és vállalható. Ha azonban a rendszer már évek óta működik, és sok alkalmazás fut rajta, akkor az alkalmazások elemzése és az objektum jogosultságok beállítása nyomasztó feladatnak tűnhet.

Objektum jogosultsági tipp: Az aktuális menük a tulajdonosuk jogosultságait átvevő programokkal kombinálva megteremthetik az alapot a menü hozzáférés felügyeleten túli biztonsági funkciók bevezetéséhez. Győződjön meg róla, hogy a jogosultságot átvevő programok és az ezeket birtokló felhasználói profilok is védettek.

Elképzelhető, hogy az aktuális menük segítségével összeállítható egy átmeneti környezet, amelyben az áttérés során folyamatosan végzi az alkalmazások és objektumok elemzését. A következőkben egy példát mutatunk be egy Rendelés (OEMENU) menüre és a hozzá tartozó fájlokra és programokra.

Példa: Átmeneti környezet beállítása

A példa következő feltételezésekre és szükségletekre épül:

- Az összes fájl az ORDERLIB könyvtárban található.
- Nem ismeri az összes fájl nevét. Emellett azt sem tudja, hogy a különféle menüpontok milyen jogosultságokat igényelnek a különféle fájlokhoz.
- A menü és az általa hívott programok az ORDERPGM könyvtárban találhatók.
- A kívánt eredmény, hogy a rendszerre bejelentkező összes felhasználó meg tudja jeleníteni a rendelési fájlok, ügyfél fájlok és tétel fájlok információit (lekérdezésekkel, táblázatokkal vagy bármilyen más módon).
- A fájlok módosítására csak azok a felhasználók lehetnek jogosultak, akiknek az OEMENU a bejelentkezés menüjük. Emellett ehhez a menü programjait kell használniuk.
- A biztonsági adminisztrátorokon kívüli felhasználók nem rendelkeznek *ALLOBJ vagy *SECADM speciális jogosultsággal.

A menü hozzáférés felügyeletet alkalmazó környezetet a következő lépések végrehajtásával egészítheti ki a lekérdezések által támasztott igényeknek megfelelően.

__ Lépés 1. Jegyezze fel azon felhasználók listáját, akiknek kezdeti menüje az OEMENU.

A rendszeren található felhasználói profilok környezetnek kilistázásához használja a Felhasználói profil kinyomtatása (PRTUSRPRF *ENVINFO) parancsot. Ez a jelentés tartalmazza a felhasználói profilok kezdeti menüjét, kezdeti programját és aktuális könyvtárát. A jelentésre az 7. ábra: oldalszám: 62 mutat be egy példát.

__ Lépés 2. Győződjön meg róla, hogy az OEMENU objektumot (legyen az akár *PGM, akár *MENU objektum) bejelentkezéshez nem használt felhasználói profil birtokolja. A felhasználói profilt le kell tiltani, vagy *NONE jelszót kell beállítani számára. A példában feltesszük, hogy az OEMENU program objektumot az OEOWNER birtokolja.

__ Lépés 3. Győződjön meg róla, hogy az OEMENU program objektumot birtokló profil nem csoport profil. Ehhez használja a következő parancsot.

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

__ Lépés 4. Módosítsa az OEMENU programot, hogy az átvegye az OEOWNER felhasználói profil jogosultságát. (A CHGPGM paranccsal módosítsa az USRPRF paramétert az *OWNER értékre.)

Megjegyzés: A *MENU objektumok nem képesek jogosultság átvételére. Ha az OEMENU egy *MENU objektum, akkor a példát a következő módszerek valamelyikével adaptálhatja:

- Hozzon létre egy programot a menü megjelenítéséhez.
- Az OEMENU menüpontjainak kiválasztásakor futó programokat állítsa be a felhasználó jogosultságainak átvételére.

__ Lépés 5. Az ORDERLIB könyvtárban valamennyi fájl nyilvános jogosultságát állítsa a *USE értékre a következő két paranccsal:

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

Ne feledje, hogy a *USE jogosultsággal a felhasználók PC fájlátvitel vagy FTP segítségével képesek a fájlok másolására.

__ Lépés 6. A menü programját birtokló profilnak adjon *ALL jogosultságot a fájlokhoz a következő parancscsal:

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

A legtöbb alkalmazásnál a *CHANGE jogosultság elegendő. Az alkalmazások viszont végrehajthatnak például fizikai fájl member törléseket is, amelyhez a *CHANGE jogosultságnál magasabb jogosultsági szint szükséges. Végső soron elemezni kell az alkalmazásokat, és meg kell adni a működésükhöz szükséges minimális jogosultságokat. Az átmeneti időszak során azonban az *ALL jogosultság átvételével elkerülheti a jogosultságok hiányából származó alkalmazás hibákat.

__ Lépés 7. Korlátozza a rendelési könyvtár programjaira vonatkozó jogosultságokat a következő paranccsal:

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

__ Lépés 8. Adjon az OEOWNER profilnak jogosultságot a a könyvtár programjaihoz a következő parancs beírásával:

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

__ Lépés 9. A lépés: 1 helyen azonosított felhasználóknak adjon jogosultságot a menü programjához a következő parancs felhasználónkénti megadásával:

```
GRTOBJAUT OBJ(ORDERPGM/OEMENU) OBJTYPE(*PGM)
     USER(felhasználói_profil_neve) AUT(*USE)
```

A lépések befejezése után a rendszer valamennyi kifejezetten nem tiltott felhasználója hozzáférhet az ORDERLIB könyvtár fájljaihoz, de nem módosíthatja azokat. Az OEMENU programhoz jogosultsággal rendelkező felhasználók a menüből elérhető programok használatával frissíthetik is az ORDERLIB könyvtár fájljait. A könyvtárban található fájlok módosítására csak az OEMENU programjára is jogosult felhasználók jogosultak. A fájlokat az objektum biztonság és a menü hozzáférés felügyelet kombinációja védi.

Ha a megfelelően alkalmazott lépéseket végrehajtja a felhasználói adatokat tartalmazó összes könyvtáron, akkor ennek befejezésekor létrehozott egy egyszerű sémát az adatbázisok frissítéseinek felügyeletére. A módszer megakadályozza a felhasználókat az adatbázisfájlok

frissítésében, az elfogadott menük és programok használatának kivételével. Ugyanakkor biztosította, hogy a más rendszerekről vagy személyi számítógépről csatlakozó felhasználók megjelenítési, elemzési és másolási céllal hozzáférjenek az adatbázisfájlokhoz.

Objektum jogosultsági tipp: Ha a rendszer hálózat tagja, akkor a *USE jogosultság a vártnál több jogot biztosíthat. Ha például rendelkezik *USE jogosultsággal a fájlhoz, akkor FTP segítségével másolatot készíthet arról egy másik rendszeren.

Menü biztonság kiegészítése könyvtár biztonsággal

Könyvtárakban található objektumok eléréséhez jogosultnak kell lennie mind a könyvtár, mind az objektum használatára. A legtöbb műveletnél a könyvtárhoz *EXECUTE vagy *USE jogosultságra van szükség.

Az adott helyzettől függően elképzelhető, hogy az objektumok védelmére szolgáló egyszerű módszerként könyvtár jogosultságokat is alkalmazhat. A Rendelési menüvel kapcsolatos helyzetnél maradva tegyük fel például, hogy a Rendelés menühöz hozzáférő összes felhasználó jogosult az ORDERPGM könyvtár összes programjának használatára. Az egyedi programok védelme helyett beállíthatja az ORDERPGM könyvtár nyilvános jogosultságát az *EXCLUDE értékre. Ezután *USE jogosultságot adhat a könyvtárra vonatkozóan az egyes felhasználói profiloknak, amely lehetővé teszi számukra a könyvtárban található programok használatát. (Ez feltételezi, hogy a könyvtár programjainak nyilvános jogosultsága legalább *USE.)

A könyvtár jogosultság egyszerű és hatékony módszert biztosít az objektum jogosultságok felügyeletére. A nem szándékolt hozzáférések biztosításának elkerülése érdekében azonban meg kell győződni róla, hogy ismeri a védeni kívánt könyvtárak tartalmát.

Objektum tulajdonjog beállítása

A rendszer objektumainak tulajdonosa fontos része az objektum jogosultsági sémának. Az objektum tulajdonosa alapértelmezésben *ALL jogosultsággal rendelkezik az objektumhoz. Az objektum tulajdonjog tervezéséhez az *iSeries biztonsági összefoglaló* 5. fejezete ad tanácsokat és példákat. Néhány tipp:

- A csoportprofilok általában ne birtokoljanak objektumokat. Ha egy csoportprofil birtokol egy objektumot, akkor a kifejezett tiltás esetét kivéve a csoport valamennyi tagja *ALL jogosultsággal rendelkezik az objektumhoz.
- Átvett jogosultság használatakor fontolja meg, hogy a programokat birtokló felhasználói profiloknak kell-e birtokolniuk alkalmazás objektumokat, például fájlokat is. Valószínűleg nem jó ötlet, hogy a jogosultságokat átvevő programokat futtató felhasználók *ALL jogosultsággal rendelkeznek a fájlokhoz.

Az iSeries navigátor használatakor ezt a **Biztonsági stratégiák** funkcióban a megfelelő módosítások elvégzésével érheti el. További információkat az iSeries Információs központban talál. Az elérésével kapcsolatos részleteket lásd: “Előfeltétel és kapcsolódó információk” oldalszám: xii.

Rendszer parancsokra és programokra vonatkozó objektum jogosultságok

Az IBM által szállított objektumok jogosultságainak korlátozásakor tartsa szem előtt a következőket:

- Több nemzeti nyelv telepítésekor a rendszeren egynél több rendszerkönyvtár (QSYS) található. A rendszer minden egyes nemzeti nyelvéhez létezik egy QSYSxxxx könyvtár. Ha

a rendszer parancsok elérését objektum jogosultságokkal biztosítja, akkor ne feledje el, hogy a korlátozásokat a QSYS könyvtáron kívül minden egyes QSYSxxxx könyvtárban is foganatosítani kell.

- A System/38 könyvtár bizonyos esetekben biztosíthat olyan parancsokat, amelyek funkciója megegyezik azokkal, amelyeket korlátozni kíván. Ne feledkezzen el a QSYS38 könyvtár megfelelő parancsának korlátozásáról sem.
- Ha rendelkezik System/36 környezettel, akkor további programokat is korlátoznia kell. Ilyen például a QY2FTML program, amely a System/36 fájlátvitelt biztosítja.

Biztonsági megfigyelési funkciók

Ez a fejezet írja le a rendszerbiztonság hatékonyságának megfigyelésére szolgáló technikákat. A rendszerbiztonság megfigyelését több ok is indokolhatja:

- A biztonsági terv teljességének ellenőrzése.
- A tervezett biztonsági elemek meglétének és megfelelő működésének ellenőrzése. Az ilyen jellegű megfigyelést általában az adatvédelmi megbízott végzi a napi biztonsági adminisztráció részeként. Emellett - gyakran részletesebben is - végezheti egy belső vagy külső auditor a rendszeres biztonsági felülvizsgálat során.
- Annak megállapítása, hogy a rendszer biztonsága lépést tart a rendszer környezetének változásával. Néhány változás, amely hatással lehet a biztonságra:
  - Rendszer felhasználók által létrehozott új objektumok
  - Új felhasználók a rendszeren
  - Objektum tulajdonjog változása (jogosultság változása nélkül)
  - Felelősségi kör változása (felhasználói csoport változása)
  - Ideiglenes jogosultság (visszavonásának elfelejtése)
  - Újonnan telepített termékek
- Jövőbeni eseményekre, például új alkalmazás telepítésére, magasabb biztonsági szint beállítására vagy kommunikációs hálózat kialakulására való felkészülés.

A szakaszban leírt technikák az összes ilyen szituációra alkalmazhatók. A megfigyelendő dolgok és a megfigyelés gyakorisága a szervezet méretétől és biztonsági igényeitől függ. A fejezet célja a rendelkezésre álló információk bemutatása; ezek megszerzési módjának leírása, a gyűjtésükre irányuló igény lehetséges okainak feltárása illetve a megfigyelések gyakoriságára vonatkozó irányvonalak felvázolása.

A szakasz három részből áll:

- A tervezhető és megfigyelhető biztonsági elemek ellenőrzőlistája.
- A rendszer által biztosított megfigyelési napló beállítására és használatára vonatkozó információk.
- További technikák a rendszer biztonságára vonatkozó információk összegyűjtéséhez.

A biztonsági megfigyelés iSeries parancsok kiadásával, illetve naplóinformációk elérésével és megtekintésével jár. Érdemes létrehozni egy speciális profilt, amelyet a rendszer biztonsági megfigyelését végző személy használ. A megfigyeléshez használt profil rendelkezzen *AUDIT speciális jogosultsággal, hogy módosíthassa a rendszer megfigyelési jellemzőit. A fejezetben megadott megfigyelési feladatok némelyike *ALLOBJ és *SECADM speciális jogosultságot is igényel. A megfigyelési időszak végén a megfigyelési profil jelszavát ne felejtse el visszaállítani a *NONE értékre.

A biztonsági megfigyelésről további információkat a *Security Reference* című kiadvány 9. fejezetében talál.

Felhasználói profilok elemzése

A Jogosult felhasználók megjelenítése (DSPAUTUSR) paranccsal a rendszer valamennyi felhasználójáról összefoglaló listát jeleníthet meg vagy nyomtathat ki. A lista profilnév vagy csoportprofil név alapján rendezhető. Az alábbi a csoportprofil sorrendre mutat be egy példát:

```
                          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
```

Kijelölt felhasználói profilok kinyomtatása

A Felhasználói profil megjelenítése (DSPUSRPRF) paranccsal hozhat létre lekérdezési eszközzel feldolgozható kimeneti fájlt.

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

A kimeneti fájlból egy lekérdezési eszközzel többféle elemzési jelentést is létrehozhat, például:

- Az összes olyan felhasználó listája, aki *ALLOBJ és *SPLCTL speciális jogosultsággal is rendelkezik.
- Az összes felhasználónak a felhasználói profil egy adott mezője, például a kezdeti program vagy a felhasználói osztály szerint rendezett listája.

Saját lekérdezési programokat is írhat, amelyek különféle jelentéseket állítanak elő a kimeneti fájlból. Például:

- A speciális jogosultságokkal rendelkező összes felhasználói profil listája az olyan rekordok kiválasztásával, amelyben az UPSPAU mező értéke nem *NONE.
- Az összes olyan felhasználó listája, aki képes parancsok beírására az olyan rekordok kiválasztásával, amelyekben a *Képességek korlátozása* mező (a modell adatbázis kimeneti fájlban UPLTCP) értéke *NO vagy *PARTIAL.
- Egy adott kezdeti menüvel vagy kezdeti programmal rendelkező összes felhasználó listája.
- Az inaktív felhasználók listája a legutóbbi bejelentkezés mező vizsgálatával.

Nagy felhasználói profilok vizsgálata

A rendszer különböző részein elszórt nagy mennyiségű jogosultsággal rendelkező felhasználói profilok hiányos biztonsági tervezésre utalhatnak. Egy módszer a nagy felhasználói profilok megkeresésére és kiértékelésére:

1. Az Objektumleírás megjelenítése (DSPOBJD) paranccsal hozzon létre egy kimeneti fájlt a rendszer összes felhasználói profiljára vonatkozó információkkal:

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

2. Hozzon létre egy lekérdezési programot minden egyes felhasználói profil nevének és méretének méret szerinti csökkenő sorrendű kilistázására.
3. A legnagyobb méretű felhasználói profilokra vonatkozóan nyomtassa ki a részleteket is a jogosultságok és birtokolt objektumok helyénvalóságának vizsgálatához:

   ```
   DSPUSRPRF USRPRF(felhasználói_profil_neve) +
             TYPE(*OBJAUT) OUTPUT(*PRINT)
   DSPUSRPRF USRPRF(felhasználói_profil_neve) +
             TYPE(*OBJOWN) OUTPUT(*PRINT)
   ```

   Bizonyos IBM által szállított felhasználói profilok rendkívül nagyok a birtokolt objektumok nagy száma miatt. Ezek kilistázása és elemzése általában nem szükséges. Érdemes viszont ellenőrizni az *ALLOBJ jogosultsággal rendelkező IBM által szállított felhasználói profilok, például a QSECOFR vagy QSYS jogosultságát átvevő programokat.

A biztonsági megfigyelésről további információkat a *Security Reference* című kiadvány 9. fejezetében talál.

Objektum jogosultságok elemzése

Az alábbi módszerrel állapíthatja meg, hogy kik rendelkeznek jogosultságokkal a rendszer könyvtáraihoz:

1. A DSPOBJD paranccsal listázza ki a rendszer összes könyvtárát:

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

   Megjegyzés: A parancs nem jeleníti meg a nem elérhető független háttértárakban található könyvtárakat.
2. Az Objektum jogosultság megjelenítése (DSPOBJAUT) paranccsal jelenítse meg az adott könyvtárra vonatkozó jogosultságok listáját:

   ```
   DSPOBJAUT OBJ(QSYS/könyvtárnév) OBJTYPE(*LIB) +
             ASPDEV(ASP_eszköz_neve) OUTPUT(*PRINT)
   ```
3. A Könyvtár megjelenítése (DSPLIB) paranccsal listázza ki a könyvtárban található objektumokat:

   ```
   DSPLIB LIB(QSYS/könyvtárnév) ASPDEV(ASP_eszköz_neve) OUTPUT(*PRINT)
   ```

Ezen jelentésekkel meghatározhatja, hogy mi található a könyvtárban, és ki fér hozzá a könyvtárhoz. Ha szükséges, akkor a DSPOBJAUT parancs segítségével megjelenítheti a könyvtár kijelölt objektumaira vonatkozó jogosultságokat is.

Megváltozott objektumok keresése

Az Objektum integritás ellenőrzése (CHKOBJITG) paranccsal keresheti meg a megváltozott objektumokat. A megváltozott objektumok általában annak jelei, hogy valaki megpróbált belepiszkálni a rendszerbe. A parancsot érdemes lefuttatni, miután valaki:

- programokat állított vissza a rendszerre
- a Kijelölt szervizeszközöket (DST) használta

A parancs futtatásakor a rendszer létrehoz egy adatbázisfájlt, benne a lehetséges integritási problémákra vonatkozó információkkal. Az objektumok keresését végezheti egyetlen tulajdonos profil, több különböző profil vagy minden profil szerint. Lehetőség van olyan objektumok keresésére is, amelyeknek megváltozott a tartománya. Emellett a megváltozott *PGM, *SRVPGM, *MODULE és *SQLPKG objektumok megtalálása érdekében ismételten kiszámíttathatja a program ellenőrzési értékeket.

A CHKOBJITG program futtatásához *AUDIT speciális jogosultság szükséges. A parancs futása a végrehajtott keresések és számítások miatt hosszú ideig is tarthat. Érdemes ezért olyankor futtatni, amikor a rendszer nincs túlterhelve.

Megjegyzés: A sok objektumot birtokló és sok magánjogosultsággal rendelkező profilok rendkívül nagyra nőhetnek. A tulajdonos profilok mérete hatással lehet a teljesítményre a birtokolt objektumok megjelenítésekor és kezelésekor, illetve a profilok mentésekor és visszaállításakor. Hatással lehetnek tovább a rendszer működésére is. A teljesítményre és a rendszer működésére gyakorolt káros hatások megakadályozása érdekében az objektumok tulajdonjogát érdemes megosztani több profil között. **Ne rendelje hozzá az összes (vagy majdnem az összes) objektum tulajdonjogát egyetlen tulajdonos profilhoz.**

Jogosultságot átvevő programok elemzése

Az *ALLOBJ speciális jogosultsággal rendelkező felhasználó jogosultságait átvevő programok biztonsági kockázatot jelentenek. Az ilyen programok megkeresésére és vizsgálatára a következő módszer alkalmazható:

1. Az *ALLOBJ speciális jogosultsággal rendelkező összes felhasználóra vonatkozóan hívja meg az Átvevő programok megjelenítése (DSPPGMADP) parancsot a felhasználó jogosultságait átvevő programok felsorolásához:

   ```
   DSPPGMADP USRPRF(felhasználói_profil_neve) +
             OUTPUT(*PRINT)
   ```

   Megjegyzés: Az *ALLOBJ jogosultsággal rendelkező felhasználók listájának megszerzését a “Kijelölt felhasználói profilok kinyomtatása” oldalszám: 51 témakör írja le.
2. A DSPOBJAUT parancs segítségével határozza meg, hogy kik jogosultak a jogosultságot átvevő programok használatára, és nézze meg a programok nyilvános jogosultságait:

   ```
   DSPOBJAUT OBJ(könyvtárnév/programnév) +
             OBJTYPE(*PGM) ASPDEV(könyvtárnév/programnév) +
             OUTPUT(*PRINT)
   ```
3. A program forráskódjának és leírásának vizsgálatával határozza meg a következőket:
   - A program felhasználóit az átvett profil alatti működés során megakadályozza-e valami többletfunkciók, például egy parancssor használatában.
   - A program a szándékolt funkció eléréséhez minimálisan szükséges jogosultságot veszi-e át. A programhibákat használó alkalmazások tervezhetők oly módon, hogy azonos profilt használjanak az objektumokhoz és a programokhoz. A program tulajdonos jogosultságainak átvételekor a felhasználó *ALL jogosultsággal rendelkezik az alkalmazás objektumaihoz. A legtöbb esetben a tulajdonos profil számára nincs szükség speciális jogosultságokra.
4. A DSPOBJD paranccsal ellenőrizze a program legutóbbi módosításának időpontját:

   ```
   DSPOBJD OBJ(könyvtárnév/programnév) +
           OBJTYPE(*PGM) ASPDEV(könyvtárnév/programnév) +
           DETAIL(*FULL)
   ```

A megfigyelési napló és fogadóinak kezelése

A QSYS/QAUDJRN megfigyelési napló kizárólag biztonsági megfigyelési célokat szolgál. Objektumok naplózását nem szabad végezni a megfigyelési naplóba. A megfigyelési naplót nem használhatja végrehajtás felügyelet sem. A naplóba felhasználói bejegyzéseket sem lehet küldeni a Naplóbejegyzés küldése (SNDJRNE) paranccsal vagy a Naplóbejegyzés küldése (QJOSJRNE) API segítségével.

Speciális zárolási mechanizmus gondoskodik arról, hogy a rendszer írhassa a megfigyelési napló bejegyzéseit. A megfigyelés aktív állapotában (vagyis ha QAUDCTL rendszerváltozó

értéke nem *NONE) a rendszer egyeztető job (QSYSARB) zárolást jegyez be a QSYS/QAUDJRN naplón. A megfigyelés aktív állapotában bizonyos tevékenységek nem végezhetők el a megfigyelési naplón, például:

- DLTJRN parancs
- ENDJRNxxx parancs
- APYJRNCHG parancs
- RMVJRNCHG parancs
- DMPOBJ vagy DMPSYSOBJ parancs
- Napló áthelyezése
- Napló visszaállítása
- Jogosultságokat kezelő műveletek, például GRTOBJAUT parancs
- WRKJRN parancs

A biztonsági naplóbejegyzésekben feljegyzett információkat a *Security Reference* című kiadvány írja le. A megfigyelési napló valamennyi biztonsággal kapcsolatos bejegyzése T naplókóddal rendelkezik. A biztonsági bejegyzések mellett a QAUDJRN naplóban rendszer bejegyzések is szerepelhetnek. Ezen bejegyzések naplókódja J, és egyebek között rendszerindító programbetöltésekre (IPL) vagy naplófogadó műveletekre (mentés, visszaállítás, stb.) utalhatnak.

Ha a napló vagy az aktuális fogadója megsérül, és a megfigyelési bejegyzések naplózása a továbbiakban nem lehetséges, akkor a rendszer a QAUDENDACN rendszerváltozó által meghatározott tevékenységgel reagál. A sérült napló vagy naplófogadó helyreállítása megegyezik a többi naplófogadónál megszokottal.

A naplófogadók cseréjét érdemes a rendszerre bízni. A QAUDJRN napló létrehozásakor adja meg a MNGRCV(*SYSTEM) paramétert, vagy módosítsa a naplót erre az értékre. A MNGRCV(*SYSTEM) megadása esetén a rendszer a küszöbérték elérésekor automatikusan leválasztja a fogadót, és új naplófogadót hoz létre és csatol. Ezt **Rendszer által vezérelt naplókezelésnek** hívjuk. További információkat az iSeries Információs központ Rendszerfelügyelet → Naplókezelés → Helyi naplók kezelése → Naplók kezelése című témakörében talál. Az iSeries Információs központ elérésével kapcsolatban nézze meg az “Előfeltétel és kapcsolódó információk” oldalszám: xii szakaszt.

6. fejezet Jogosultságok kezelése

A rendszer jogosultsági beállításainak nyomon követéséhez több biztonsági jelentés is segítséget nyújt. A jelentések első használatakor érdemes mindent (például az összes fájlra vagy programra vonatkozó jogosultságokat) kinyomtatni.

A kiindulási információk rögzítése után elegendő a változásokat rögzítő változatok rendszeres időközönkénti lefuttatása. A változásokat rögzítő változatok segítséget nyújtanak a rendszeren bekövetkezett biztonsággal kapcsolatos figyelmet érdemlő változások azonosításához. Lefuttathat például minden héten egy olyan jelentést, amely a fájlok nyilvános jogosultságait jeleníti meg. A jelentésből kérhető olyan változat, amely csak a változásokat tartalmazza. A jelentésben megjelennek azok az új fájlok, amelyek mindenki számára elérhetők, illetve azok a meglévő fájlok, amelyeknek nyilvános jogosultsága megváltozott a jelentés legutóbbi lefuttatása óta.

A biztonsági eszközökhöz két menü áll rendelkezésre:

- A SECTOOLS menü használható a programok interaktív futtatására.
- A SECBATCH menü segítségével futtathatja a programokat kötegelt módban. A SECBATCH menü két részből áll, az egyik segítségével a jobokat azonnal elküldheti a jobsorba, a másikkal a jobokat elhelyezheti a job ütemezőben.

Az iSeries navigátor használatakor a biztonsági eszközök futtatásához tegye a következőket:

1. Az iSeries navigátorban bontsa ki a szervert, majd a **Biztonság** kategóriát.
2. Kattintson a jobb egérgombbal a **Stratégiák** elemre, majd válassza az előugró menü **Intéző** menüpontját a kezelhető stratégiák listájának megjelenítéséhez.

Objektumok nyilvános jogosultságának megfigyelése

Az egyszerűség és teljesítmény kedvéért a legtöbb rendszer úgy van beállítva, hogy az objektumok többsége a felhasználók nagy része számára elérhető. Minden egyes objektum jogosultságának kifejezett megadása helyett a felhasználók jogosultságai egyes bizalmas, biztonsági szempontból érzékeny objektumoknál kifejezetten le vannak tiltva. A magas biztonsági követelményekkel rendelkező rendszereken követhető az ellenkező megközelítés is, amelynek lényege, hogy minden objektum jogosultságot külön kell indokolni és megadni. Ez utóbbi rendszereken a legtöbb objektum *EXCLUDE nyilvános jogosultsággal jön létre.

Az iSeries objektum alapú rendszer, amelyen sokféle objektumtípus található. A legtöbb objektumtípus nem tartalmaz érzékeny információkat és nem vesz részt biztonsággal kapcsolatos funkciókban. Az általános biztonsági igényeket támasztó iSeries rendszereken a biztonsági adminisztrátornak inkább a védelmet igénylő objektumokra, például adatbázisfájlokra és programokra kell összpontosítania. A többi objektumtípus esetén általában elegendő, ha egyszerűen megad egy olyan nyilvános jogosultságot, amely megfelelő az alkalmazások számára; a legtöbb objektumtípus esetén ez a *USE jogosultság.

A Nyilvános jogosultságok kinyomtatása (PRTPUBAUT) parancs segítségével nyomtathatja ki a nyilvános felhasználók által elérhető objektumokra vonatkozó információkat. (A **nyilvános felhasználók** olyan felhasználók, akik bejelentkezhetnek a rendszerbe, de egy objektumra vonatkozóan sem rendelkeznek kifejezett jogosultságokkal.) A PRTPUBAUT parancs használatakor megadhatja megvizsgálni kívánt objektumtípusokat, könyvtárakat vagy katalógusokat. A SECBATCH és SECTOOLS menükből kinyomtathat egy jelentést azon objektumtípusok nyilvános jogosultságaira vonatkozóan, amelyekkel kapcsolatban a

leggyakrabban merülnek fel biztonsági következmények. A jelentés változásokat feltüntető változatát rendszeres időközönként kinyomtatva képet kap az esetleges odafigyelést igénylő objektumokról.

Új objektumok jogosultságainak kezelése

Az OS/400 többféle funkciót is biztosít a rendszer új objektumaira vonatkozó jogosultságok és tulajdonjog kezelésének megkönnyítéséhez. Amikor egy felhasználó létrehoz egy objektumot, akkor a rendszer meghatározza a következőket:

- Ki lesz az objektum tulajdonosa
- Mi lesz az objektum nyilvános jogosultsága
- Rendelkezik-e az objektum magánjogosultságokkal
- Hova kerül az objektum (melyik könyvtár vagy katalógus)
- Végez-e a rendszer megfigyelést az objektum elérésével kapcsolatban

A meghatározáshoz a rendszer különféle rendszerváltozókat, könyvtár paramétereket és felhasználói profil paramétereket használ fel. A rendelkezésre álló tekintélyes számú lehetőség közül néhányat az *iSeries biztonsági összefoglaló* című kiadvány 5. fejezete mutat be példaként az "Új objektumok jogosultságainak és tulajdonosának hozzárendelése" című szakaszban.

Az új objektumok tulajdonjogát és jogosultságait meghatározó felhasználói profil paraméterek kinyomtatására a PRTUSRPRF parancsot használhatja. A jelentésre az 5. ábra: oldalszám: 61 mutat be egy példát.

Jogosultsági listák megfigyelése

A hasonló biztonsági követelményeket támasztó objektumokat jogosultsági listák felhasználásával csoportosíthatja. A jogosultsági listák nagy vonalakban a lista által védett objektumra vonatkozóan jogosultsággal rendelkező felhasználókat sorolják fel ezek jogosultságaival együtt. A jogosultsági listák hatékony módszert biztosítanak a rendszer hasonló objektumainak kezeléséhez. Bizonyos esetekben azonban használatuk megnehezítheti az objektum jogosultságok nyomon követését.

A jogosultsági listák által biztosított jogosultságokra vonatkozó információkat a Magánjogosultságok kinyomtatása (PRTPVTAUT) paranccsal nyomtathatja ki. A jelentésre az 3. ábra: mutat be egy példát.

```
                        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
```

3. ábra: Jogosultsági listák magánjogosultságai jelentés

A jelentés a Jogosultsági lista szerkesztése (EDTAUTL) képernyőn láthatóakkal megegyező információkat tartalmaz. A jelentés előnye, hogy valamennyi jogosultsági listát egy helyre gyűjt össze. Új objektumcsoport biztonságának beállítása esetén például egyszerűen átfuthatja a jelentést annak megállapításához, hogy van-e olyan meglévő jogosultsági lista, amely megfelel az objektumok által támasztott biztonsági követelményeknek.

A jelentésnek a változásokat tartalmazó változata is kinyomtatható, amelyen nyomon követhetők a jelentés legutóbbi kinyomtatása óta megváltozott jogosultsági listák. Emellett lehetőség van az egyes jogosultsági listák által védett objektumok listájának kinyomtatására is. Egy jogosultsági lista ilyen jelentését mutatja be az 4. ábra:.

```
                    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
```

4. ábra: Jogosultsági lista objektumok megjelenítése jelentés

Ezzel a jelentéssel határozhatja meg például annak következményeit, hogy a jogosultsági listához új felhasználót ad hozzá (milyen jogosultságokhoz jut ezzel a felhasználó).

Jogosultsági listák használata

Az iSeries navigátor biztonsági szolgáltatásai úgy kerültek kialakításra, hogy segítséget nyújtsanak a biztonsági tervek és stratégiák kialakításához, illetve a rendszernek a vállalat által támasztott igényeknek megfelelő beállításához. A rendelkezésre álló funkciók egyike a jogosultsági listák használata.

A jogosultsági listák jellemzői a következők.

- A jogosultsági listák hasonló biztonsági igényekkel rendelkező objektumokat csoportosítanak.
- A jogosultsági listák felhasználók és csoportok listáit, illetve ezeknek a lista által védett objektumokra vonatkozó jogosultságait tartalmazzák.
- A lista által védett objektumra vonatkozóan valamennyi felhasználó és csoport eltérő jogosultságokkal rendelkezhet.
- A jogosultságok a felhasználónkénti vagy csoportonkénti megoldás helyett a lista útján adományozhatók.

A jogosultsági listákon végrehajtható feladatok például a következők.

- Jogosultsági lista létrehozása
- Jogosultsági lista módosítása
- Felhasználók és csoportok hozzáadása
- Felhasználói engedélyek módosítása
- Védett objektumok megjelenítése

A funkció használatához tegye a következőket:

1. Az iSeries navigátorban bontsa ki a Szerver —> Biztonság kategóriát. Megjelennek a **Jogosultsági listák** és **Stratégiák**.
2. Kattintson a jobb egérgombbal a **Jogosultsági listák** elemre, majd válassza az előugró menü **Új jogosultsági lista** menüpontját. A megjelenő **Új jogosultsági lista** párbeszédablakban az alábbi engedélyek állíthatók be.
   - **Használat:** Lehetővé teszi az objektum attribútumainak elérését és az objektum használatát. A nyilvánosság megtekintheti, de nem módosíthatja az objektumot.
   - **Módosítás:** Néhány kivételtől eltekintve lehetővé teszi az objektum tartalmának módosítását.

- **Mind:** A tulajdonosra korlátozott funkciókon kívül valamennyi tevékenység végrehajtását engedélyezi az objektumon. A felhasználó vagy csoport felügyelheti az objektum létezését, beállíthatja az objektum biztonságát, módosíthatja az objektumot, és végrehajthatja rajta az alapvető műveleteket is. A felhasználó vagy csoport módosíthatja az objektum tulajdonjogát is.
- **Kizárás:** Az objektumon minden művelet tiltott. Ezzel az ″engedéllyel″ rendelkező felhasználók és csoportok semmilyen műveletet nem hajthatnak végre az objektumon. Megadja, hogy az objektumot a nyilvánosság sem használhatja.

Jogosultsági listák kezelésekor bizonyos esetekben szükség lehet objektumokra és adatokra vonatkozó engedélyek beállítására is. A választható objektum engedélyek a következők.

- **Működtetés:** Engedélyt ad az objektumok leírásának megtekintésére, és az objektumnak a felhasználó vagy csoport adat engedélyei által meghatározott mértékű használatára.
- **Kezelés:** Engedélyt ad az objektum biztonságának beállítására, az objektum átnevezésére vagy áthelyezésére, illetve adatbázisfájl memberek felvételére.
- **Létezés:** Engedélyt ad az objektum létezésének és tulajdonjogának felügyeletére. Az engedéllyel rendelkező felhasználó vagy csoport törölheti az objektumot, felszabadíthatja az objektum tárterületét, mentési és visszaállítási műveleteket hajthat végre az objektumon, és átadhatja az objektum tulajdonjogát. Ha egy felhasználó vagy csoport rendelkezik speciális mentési engedéllyel, akkor a mentéshez nincs szükség létezési engedélyre.
- **Módosítás:** Engedélyt ad az objektum attribútumainak módosítására (csak adatbázisfájlok és SQL csomagok használják). Az engedéllyel adatbázisfájl vonatkozásában rendelkező felhasználók vagy csoportok hozzáadhatnak és eltávolíthatnak triggereket és hivatkozási vagy egyedi megszorításokat, illetve módosíthatják az adatbázisfájl attribútumait. Ha egy felhasználó vagy csoport SQL csomagra vonatkozóan rendelkezik ilyen engedéllyel, akkor módosíthatja az SQL csomag attribútumait. Az engedélyt jelenleg csak adatbázisfájlok és SQL csomagok használják.
- **Hivatkozás:** Engedélyt ad az objektum hivatkozására más objektumokból, ily módon az objektumokon végzett műveleteket más objektumok korlátozhatják. Csak adatbázisfájlok és SQL csomagok használják. Az engedéllyel fizikai fájlokra vonatkozóan rendelkező felhasználók és csoportok hozzáadhatnak olyan hivatkozási megszorításokat, amelyben a fizikai fájl a szülő. A rendszer ezt az engedélyt jelenleg csak adatbázisfájlokhoz használja.

A választható adat engedélyek a következők.

- **Olvasás:** Engedélyt ad az objektum tartalmának, például egy fájl rekordjainak lekérdezésére és megjelenítésére.
- **Hozzáadás:** Engedélyt ad objektum bejegyzések felvételére, például üzenetek hozzáadására egy üzenetsorhoz vagy fájl rekordok felvételére.
- **Frissítés:** Engedélyt ad az objektum bejegyzéseinek módosítására, például egy fájl rekordjainak módosítására.
- **Törlés:** Engedélyt ad egy objektum bejegyzéseinek törlésére, például egy üzenetsor üzeneteinek eltávolítására vagy egy fájl rekordjainak törlésére.
- **Végrehajtás:** Engedélyt ad egy program, szervizprogram vagy SQL csomag futtatására. Ez az engedély teszi lehetővé az objektum keresését is a könyvtárban vagy katalógusban.

A jogosultsági listák létrehozásával és szerkesztésével kapcsolatos feladatokra vonatkozó részleteket az iSeries navigátor online súgójában találja.

Stratégiák kezelése az iSeries navigátorban

Az iSeries navigátor segítségével lehetősége van az iSeries szerver stratégiáinak megjelenítésére és kezelésére. Az iSeries navigátor ötféle stratégia kezelését támogatja:

- **Megfigyelési stratégia**
  Lehetővé teszi a különféle tevékenységek elvégzésére, illetve a rendszererőforrások használatára vonatkozó megfigyelés beállítását.

- **Biztonsági stratégia**
  Lehetővé teszi a biztonsági szint meghatározását, és a rendszer biztonságával kapcsolatos további lehetőségek beállítását.
- **Jelszó stratégia**
  Lehetővé teszi a rendszer jelszó szintjének meghatározását.
- **Visszaállítási stratégia**
  Lehetővé teszi az objektumok visszaállítási módjának meghatározását.
- **Bejelentkezési stratégia**
  Lehetővé teszi a felhasználói bejelentkezés felügyeletét.

A stratégiák megtekintéséhez vagy módosításához az iSeries navigátorban tegye a következőket:

1. Az iSeries navigátorban bontsa ki a szervert, majd a **Biztonság** kategóriát.
2. Kattintson a jobb egérgombbal a **Stratégiák** elemre, majd válassza az előugró menü **Intéző** menüpontját a kezelhető stratégiák listájának megjelenítéséhez. A stratégiákra vonatkozó részleteket az iSeries navigátor súgójából ismerheti meg.

Objektumok magánjogosultságainak megfigyelése

SECBATCH menü menüpontjai:
12 - *azonnali elküldés* **41** - *job ütemező használata*

A megadott könyvtárban található adott típusú objektumokra vonatkozó magánjogosultságok listáját a Magánjogosultságok kinyomtatása (PRTPVTAUT) paranccsal nyomtathatja ki.

Ezzel a jelentéssel derítheti fel az objektumokra vonatkozó új jogosultságokat. Segítséget nyújt továbbá a magánjogosultságoknál alkalmazott séma ésszerű keretek között tartására.

Kimeneti- és jobsorokra vonatkozó hozzáférés megfigyelése

Bizonyos helyzetekben előfordul, hogy az adminisztrátornak sikerül jó megvalósítást kialakítania a fájl hozzáférésre, viszont megfeledkezik arról, hogy mi történik a fájlok tartalmának nyomtatásakor. Az iSeries szerverek több funkciót is biztosítanak a biztonsági szempontból érzékeny kimeneti sorok és jobsorok védelmére. A kimeneti sorok védelmére azért van szükség, nehogy a jogosulatlan felhasználók megtekinthessék vagy lemásolhassák a nyomtatásra várakozó bizalmas információkat tartalmazó spoolfájlokat. A jobsorok védelme megakadályozza, hogy a jogosulatlan felhasználók az egyébként bizalmas információkat tartalmazó kimenetet előállító jobokat általános kimeneti sorba helyezzék át, vagy teljes egészében visszavonják a jobot.

SECBATCH menü menüpontjai:
24 - azonnali elküldés 63 - *job ütemező használata*

A kimeneti sorok és jobsorok védelmét az Információs központ *Alapvető rendszerbiztonság és tervezés* című témaköre, illetve az *iSeries biztonsági összefoglaló* című kiadvány írja le.

A Sor jogosultságok kinyomtatása (PRTQAUT) paranccsal nyomtathatja ki a rendszer jobsoraira és kimeneti soraira vonatkozó biztonsági beállításokat. Ezután a bizalmas információkat tartalmazó kimeneteket előállító jobokat elkülönítheti védett jobsorokban és kimeneti sorokban.

A biztonsági szempontból érzékenynek tekintett kimeneti sorok és jobsorok esetén hasonlítsa össze ezek beállításait az *iSeries biztonsági összefoglaló* D függelékében megadott biztonsági beállításokkal. A D függelék táblázatai adják meg a kimeneti sorokon és jobsorokon elvégezhető műveletekhez szükséges beállításokat.

Speciális jogosultságok megfigyelése

Ha a rendszer felhasználói feleslegesen rendelkeznek speciális jogosultságokkal, akkor az objektum jogosultsági séma kialakítására tett erőfeszítések akár elpocsékoltnak is tekinthetők. Az objektum jogosultságnak semmi értelme, ha egy felhasználói profil rendelkezik az *ALLOBJ speciális jogosultsággal. A *SPLCTL speciális jogosultsággal rendelkező felhasználók pedig a rendszer összes spoolfájlját megtekinthetik, függetlenül attól, hogy mennyi energiát fektetett a kimeneti sorok védelmének kialakítására. A *JOBCTL speciális jogosultság birtokában lévő felhasználók befolyásolhatják a rendszer működését, és átirányíthatják a jobokat. A *SERVICE speciális jogosultsággal rendelkező felhasználók a szervizeszközök felhasználásával az operációs rendszer megkerülésével férhetnek hozzá az adatokhoz.

SECBATCH menü menüpontjai:
29 - azonnali elküldés 68 - *job ütemező használata*

A Felhasználói profil kinyomtatása (PRTUSRPRF) paranccsal nyomtathatja ki a rendszeren található felhasználói profilok speciális jogosultságait és felhasználó osztályát. A jelentés futtatása többféle beállítás mellett is történhet:
- Minden felhasználói profil
- Adott speciális jogosultságokkal rendelkező felhasználói profilok
- Adott felhasználói osztályhoz tartozó felhasználói profilok
- A felhasználói osztály és a birtokolt speciális jogosultságok között eltéréseket mutató felhasználói profilok.

Az összes felhasználói profil speciális jogosultságait tartalmazó jelentésre az 5. ábra: oldalszám: 61 mutat be egy példát:

```
                                        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
```

5. ábra: Felhasználói információs jelentés: 1. példa

A speciális jogosultságok mellett a jelentéseken a következők láthatók:

- A felhasználói profil képességei korlátozottak-e.
- A felhasználó vagy a felhasználó csoportja birtokolja-e a felhasználó által létrehozott új objektumokat.
- A felhasználó által létrehozott új objektumokra vonatkozóan a felhasználó csoportja által automatikusan megkapott jogosultságok.

Az 6. ábra: a felhasználói osztályok és a speciális jogosultságok közötti eltérésekre vonatkozó jelentésre mutat be egy példát:

```
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
```

6. ábra: Felhasználói információs jelentés: 2. példa

Az 6. ábra: ismételt áttekintése után érdemes megfigyelni a következőket:

- Az USERX rendszeroperátor (*SYSOPR) felhasználói osztályhoz tartozik, de rendelkezik *ALLOBJ és *SPLCTL speciális jogosultságokkal.
- Az USERY felhasználó (*USER) felhasználói osztályba tartozik, ennek ellenére *SECADM speciális jogosultsága van.
- Az USERZ szintén felhasználó (*USER) osztályba tartozik, és neki is van *SECADM speciális jogosultsága. Könnyű észrevenni továbbá, hogy az USERZ a QPGMR csoport tagjakén *JOBCTL és *SAVSYS speciális jogosultságokkal is rendelkezik.

A jelentéseket a felhasználói profilok felügyeletének megkönnyítése érdekében érdemes rendszeres időközönként lefuttatni.

Felhasználói környezetek megfigyelése

A felhasználói profil egyik célja, hogy meghatározza a felhasználó környezetét, beleértve a kimeneti sort, a kezdeti menüt és a jobleírást. A felhasználó környezete határozza meg, hogy a felhasználó hogyan látja a rendszert, és milyen feladatokat végezhet el rajta. A felhasználónak jogosultsággal kell rendelkeznie a profiljában megadott objektumokhoz. Ha viszont a jogosultsági séma kialakítása még folyamatban van, vagy nem túl korlátozó, akkor felhasználói profilban megadott felhasználói környezet váratlan eredményeket produkálhat. Erre az alábbiakban sorolunk fel néhány példát.

SECBATCH menü menüpontjai:

29 - *azonnali elküldés* **68** - *job ütemező használata*

- A felhasználó jobleírása megadhat olyan felhasználói profilt, amely több jogosultsággal rendelkezik a felhasználónál.
- Elképzelhető, hogy a felhasználónak parancssor nélküli kezdeti menüje van. Az Attn billentyűt kezelő program azonban szintén biztosíthat parancssort a felhasználónak.
- Elképzelhető, hogy a felhasználó jogosult bizalmas jelentések előállítására. A felhasználó kimenete viszont csak olyan kimeneti sorra irányítható, ahol más felhasználók is szabadon megtekinthetik a bizalmas információkat tartalmazó spoolfájlokat.

A rendszer felhasználói számára beállított környezetek megfigyeléséhez használja a Felhasználó profil kinyomtatása (PRTUSRPRF) parancs *ENVINFO paraméterét. A jelentésre az 7. ábra: mutat be egy példát:

```
                                    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
```

7. ábra: Példa a felhasználói profil környezetének kinyomtatására

Szervizeszközök kezelése

A szervizeszközök használhatók a szerver konfigurálására, kezelésére és szervizfunkcióinak elvégzésére. A szervizeszközök a Kijelölt szervizeszközök (DST) és Rendszer szervizeszközök (SST) menüből érhetők el. A DST, SST, valamint az iSeries navigátor logikai partíciókkal (LPAR) és lemezkezeléssel kapcsolatos funkciónak eléréséhez szervizeszköz felhasználói azonosítóra van szükség.

A DST a Licensed Internal Code elindítása után, még az OS/400 betöltése előtt érhető el. Az SST az OS/400 operációs rendszerből indítható. A DST és SST közötti alapvető különbségeket az alábbi táblázat foglalja össze.

Jellemző	DST	SST
Elérés módja	Fizikai konzol hozzáférés szükséges kézi IPL során, vagy ki kell választani a vezérlőpanel 21. lehetőségét.	QSRV bejelentkezés képességével vagy a következő jogosultságokkal rendelkező interaktív jobon keresztül érhető el: • Jogosultság az STRSST (SST indítása) CL parancshoz • Szerviz (*SERVICE) és Minden objektum (*ALLOBJ) speciális jogosultság • Funkcionális jogosultság az SST használatára.

Rendelkezésre állás	A szerver korlátozott állapotában is rendelkezésre áll. A DST eléréséhez az OS/400 nem szükséges.	Az OS/400 indítása után érhető el. Az SST eléréshez szükség van az OS/400 operációs rendszerre.
Hitelesítés módja	Szervizeszköz felhasználói azonosítót és jelszót igényel.	Szervizeszköz felhasználói azonosítót és jelszót igényel.

Az iSeries Információs központ Biztonság → Szervizeszközök témakörében szerezhet további információkat a szervizeszközöknek az alábbi feladatokra való felhasználásáról:

- Szervizeszközök elérése a DST segítségével
- Szervizeszközök elérése az SST segítségével
- Szervizeszközök elérése az iSeries navigátorból
- Szervizeszköz felhasználói azonosítók létrehozása
- Szervizeszköz felhasználói azonosítók funkcionális jogosultságainak módosítása
- Szervizeszköz felhasználói azonosítók leírásának módosítása
- Szervizeszköz felhasználói azonosítók megjelenítése
- Szervizeszköz felhasználói azonosítók engedélyezése és letiltása
- szervizeszköz felhasználói azonosítók törlése
- Szervizeszköz felhasználói azonosítók és jelszavak módosítása az SST vagy DST segítségével
- Saját szervizeszköz felhasználói azonosító jelszavának lecserélése az STRSST paranccsal
- Szervizeszköz felhasználói azonosítók és jelszavak módosítása
- Szervizeszköz felhasználói azonosítók módosítása (QSYCHGDS) API
- A QSECOFR OS/400 felhasználói profil jelszavának alaphelyzetbe állítása
- A QSECOFR szervizeszköz felhasználói azonosító és jelszó alaphelyzetbe állítása
- Szervizeszköz biztonsági adatok mentése és visszaállítása
- A QSECOFR szervizeszköz felhasználói azonosító saját változatának létrehozása
- Szervizeszköz szerver beállítása a DST-hez
- Szervizeszköz szerver beállítása az OS/400-hoz
- Szervizfunkciók használatának megfigyelése a DST segítségével
- Szervizeszközök használatának megfigyelése az OS/400 biztonsági megfigyelési naplójával

Az iSeries Információs központ elérésével kapcsolatban nézze meg az “Előfeltétel és kapcsolódó információk” oldalszám: xii szakaszt.

7. fejezet Logikai partíciók (LPAR) biztonsága

Az iSeries szervereken kialakítható önálló logikai partíciók az alábbi helyzetekben bizonyulhatnak hasznosnak.

- **Független rendszerek fenntartása:** Az erőforrások (lemezes tároló, processzor, memória és I/O eszközök) egy részének dedikálásával a partíciók megoldást nyújtanak a szoftverek logikai elkülönítésére. Megfelelő beállításuk esetén a logikai partíciók biztosítanak bizonyos szintű hardver hibatűrést is. Az önálló rendszeren csak problémásan együtt futó interaktív és kötegelt terhelés logikai partíciók felhasználásával elkülöníthető és hatékonyan futtatható.
- **Egyesítés:** A logikai partíciókkal rendelkező rendszerek csökkentik a vállalat által igényelt iSeries szerver rendszerek számát. Egyetlen, logikai partíciókkal rendelkező rendszerben több rendszer is egyesíthető. Ez kiküszöböli a további berendezésekre vonatkozó igényeket, és ezek költségvonzatát. Az igények változásával a logikai partíciók között az erőforrások áthelyezhetők.
- **Vegyes termelési és tesztkörnyezet létrehozása:** Logikai partíciókkal lehetőség van termelési és tesztelési környezetek kombinációjának létrehozására. Az elsődleges partíción belül létrehozható egy termelési partíció. Több termelési partíció kialakításával kapcsolatban nézze meg az alábbi *Több termelési partíciót tartalmazó környezet kialakítása* szakaszt.

  A logikai partíciók tesztelési vagy termelési partíciók lehetnek. A termelési partíciókon futnak az üzleti alkalmazások. A termelési partíció meghibásodása jelentősen visszaveti az üzletmenetet, ezért ez költséges és időveszteséget is okoz. A tesztelési partíción szoftverek tesztelése folyik. A tesztelési partíció meghibásodása bár nem feltétlenül van betervezve, nincs különösebb hatással a szokásos üzletmenetre.
- **Több termelési partíciót tartalmazó környezet kialakítása:** Több termelési partíciót csak a másodlagos partíciókban érdemes kialakítani. Az ilyen esetekben az elsődleges partíció partíciókezelési célokat szolgál.
- **Azonnal rendelkezésre álló tartalék:** Ha egy másodlagos partíció az adatait ugyanazon a rendszeren belül egy másik logikai partícióra többszörözi, akkor partíció meghibásodás esetén át lehet kapcsolni a tartalékra, amely így csak minimális kényelmetlenséget okoz. Ez az összeállítás emellett minimálisra csökkenti a hosszú mentési ablakok hatásait is. A tartalékpartíció ilyenkor offline állapotba helyezhető, és elindítható rajta a mentés, míg a másik logikai partíció folytatja a tevékenységét. A felvázolt azonnal rendelkezésre álló tartalék összeállítás speciális szoftvert igényel.
- **Integrált fürtözés:** Az OptiConnect/400 és egy magasszintű elérhetőséget kialakító szoftver segítségével a partíciókkal rendelkező rendszer integrált fürtként futhat. Az integrált fürtök segítségével bebiztosíthatja a rendszert a másodlagos partíciók legtöbb meghibásodása ellen.

Megjegyzés: Másodlagos partíciók beállításakor a kártyák elhelyezése külön megfontolást igényel. Ha a konzol funkcióhoz kiválasztott I/O processzor (IOP) LAN kártyával is rendelkezik, és a LAN kártyát nem kívánja felhasználni a Műveleti konzolhoz, akkor ez konzol felhasználásra lesz aktiválva, és elképzelhető, hogy a tervezett módon nem fogja tudni használni. A Műveleti konzol használatával kapcsolatban további információkat a 8. fejezet, “iSeries Műveleti konzol”, oldalszám: 67 szakaszban talál.

A témakörben felvázoltakról további részleteket az iSeries Információs központ Logikai partíciók című témaköréből tudhat meg.

Logikai partíciók biztonságának kezelése

A partíciókkal rendelkező rendszereken végrehajtott biztonsággal kapcsolatos feladatok megegyeznek a logikai partíciókat nem tartalmazó rendszereken végzett feladatokkal. Ne feledje viszont, hogy logikai partíciók létrehozásakor egynél több független rendszer kezeléséről van szó. Ennek megfelelően a feladatokat minden egyes logikai partíción el kell végezni.

A logikai partíciók biztonságával kapcsolatban érdemes szem előtt tartani a következőket:

- A felhasználók hozzáadása logikai partíciónként történik. A felhasználókat külön fel kell venni minden egyes logikai partíción, amelyhez hozzá kell férniük.
- Korlátozza azon személyek számát, akik az elsődleges partíció Kijelölt szervizeszközeit (DST) vagy Rendszer szervizeszközeit (SST) elérhetik. A DST-ről és SST-ről további információkhoz az iSeries Információs központ ″Logikai partíciók kezelése az iSeries navigátorral a DST-n vagy SST-n keresztül″ című témaköréből juthat. A “Szervizeszközök kezelése” oldalszám: 62 szakaszban talál információkat arról, hogyan használhatók a szervizeszköz felhasználói profilok a partíciókkal kapcsolatos tevékenységek elérésének felügyeletére.

  Megjegyzés: Mielőtt az iSeries navigátor használható lenne az LPAR funkciók elérésére, be kell állítani a szervizeszköz szervert (STS). A kapcsolódó információkat az iSeries Információs központ —> Biztonság —> Szervizeszközök témakörében találja. Az iSeries Információs központ elérésével kapcsolatban nézze meg az “Előfeltétel és kapcsolódó információk” oldalszám: xii szakaszt.
- A másodlagos partíciók nem látják és használhatják a többi logikai partíció főtárát és lemezegységeit.
- A másodlagos partíciók csak a saját hardvererőforrásaikat látják.
- Az elsődleges partíció a DST vagy SST Rendszer partíciók kezelése képernyőjén az összes hardvererőforrást láthatja.
- Az elsődleges partíció operációs rendszere még mindig csak a rendelkezésre álló erőforrásait látja.
- A rendszer vezérlőpanel az elsődleges partíciót vezérli. Ha a panel üzemmódját biztonságosra állítja, akkor az SST Partíció állapotának kezelése képernyőjén semmilyen tevékenység nem végezhető. Ha ki kívánja kényszeríteni a DST használatát a rendszer vezérlőpanelről, akkor módosítani kell az üzemmódját kézire.
- Ha egy másodlagos partíció működési módját állítja biztonságosra, akkor a Partíció állapotának kezelése képernyő használatát az alábbi módokon korlátozza:
  - A partíció állapotának módosítására csak a másodlagos partíció DST menüje használható, az SST nem.
  - A másodlagos partíció DST menüjének kikényszerítését csak az elsődleges partíció DST vagy SST menüjéből elindított Partíció állapotának kezelése képernyőn teheti meg.
  - A másodlagos partíció biztonságostól eltérő működési módjának beállítására csak az elsődleges partíció DST menüjéből van lehetőség.

Ha a másodlagos partíció kikerült a biztonságos üzemmódból, akkor a partíció állapotának módosításához használhatja a másodlagos partíció DST vagy SST menüjét is.

Az iSeries szerver biztonságával kapcsolatosan további információkat a Security Reference című kiadványból és az iSeries Információs központ Alapvető rendszer biztonság és tervezés témaköréből szerezhet.

8. fejezet iSeries Műveleti konzol

A Műveleti konzol lehetővé teszi, hogy egy személyi számítógép segítségével érje el és irányítsa az iSeries szervert. A Műveleti konzol lehetővé teszi távoli számítógépek számára, hogy felhívják a konzol eszközzel nem rendelkező iSeries szervereket, és konzol eszközzé váljanak. A Műveleti konzol használata során ne feledkezzen meg a következőkről:

- A Műveleti konzol segítségével minden olyan feladat elvégezhető, amelyet a hagyományos konzolok is biztosítanak. A *SERVICE vagy *ALLOBJ speciális jogosultsággal rendelkező felhasználói profilok például akkor is indíthatnak Műveleti konzol szekciót, ha egyébként le vannak tiltva.
- A Műveleti konzol az iSeries szerver kapcsolatának létesítéséhez szervizeszköz felhasználói profilokat és jelszavakat használ. Ezért különösen fontos a szervizeszköz felhasználói profilok és jelszavak lecserélése. A betörők valószínűleg tisztában vannak az alapértelmezett szervizeszköz felhasználói profilokkal és jelszavakkal, és ezek segítségével távoli konzol szekció kialakítását kísérelhetik meg az iSeries szerverrel. Jelszavak beállítására vonatkozó tanácsokat az “Ismert jelszavak módosítása” oldalszám: 20 és “Alapértelmezett jelszavak elkerülése” oldalszám: 26 szakaszok tartalmaznak.
- Távoli konzol használata esetén az információk védelme érdekében használja a Windows Telefonos hálózatok visszahívás támogatását.
- Másodlagos partíciók beállításakor a kártyák elhelyezése külön megfontolást igényel. Ha a konzol funkcióhoz kiválasztott I/O processzor (IOP) LAN kártyával is rendelkezik, és a LAN kártyát nem kívánja felhasználni a Műveleti konzolhoz, akkor ez konzol felhasználásra lesz aktiválva, és elképzelhető, hogy a tervezett módon nem fogja tudni használni.

A V5R1 kiadásban a Műveleti konzol kibővült, és a konzol tevékenységek végrehajtását helyi hálózaton (LAN) keresztül is biztosíthatja. A konzol eljárások biztonságát kiterjesztetthitelesítés és adattitkosítás védi. LAN csatlakozással rendelkező Műveleti konzol használata esetén erősen javallt az alábbi termékek telepítése:

- Cryptographic Access Provider (5722–AC2 vagy 5722–AC3) az iSeries szerveren
- Client Encryption (5722–CE2 vagy 5722–CE3) a Műveleti konzol számítógépen

A konzol adatok titkosításához az iSeries szerveren telepíteni kell valamelyik Cryptographic Access Provider terméket **és** a számítógépen is telepíteni kell a Client Encryption termékek valamelyikét.

Megjegyzés: Kriptográfiai termékek telepítésének hiányában adattitkosításra nem kerül sor.

A rendelkezésre álló termékek különféle kombinációi esetén nyújtott titkosítási szintet az alábbi táblázat foglalja össze.

13. táblázat: Titkosítás eredményei

iSeries szerverre telepített Cryptographic Access Provider termék	Műveleti konzol számítógépre telepített Client Encryption termék	Eredményül kapott adattitkosítási szint
Nincs	Nincs	Nincs
5722–AC2	5722–CE2	56 bites
5722–AC2	5722–CE3	56 bites
5722–AC3	5722–CE2	56 bites
5722–AC3	5722–CE3	128 bites

Az iSeries Műveleti konzol beállításával és felügyeletével kapcsolatban további információkat az iSeries Információs központban talál.

Műveleti konzol biztonság áttekintése

Az Műveleti konzol biztonságot a következők biztosítják:

- konzol eszköz hitelesítés
- felhasználói hitelesítés
- adatok bizalmassága
- adatok integritása

A közvetlen csatlakozással rendelkező Műveleti konzol a pont-pont kapcsolat miatt implicit eszköz hitelesítést, bizalmasságot és integritást nyújt. A konzol képernyőre való bejelentkezéshez felhasználói hitelesítés szükséges.

Konzol eszköz hitelesítés

A konzol eszköz hitelesítés segítségével lehet meggyőződni arról, hogy melyik fizikai eszköz a konzol. A közvetlen csatlakozású Műveleti konzol a twinaxiális konzolokhoz hasonló fizikai kapcsolattal rendelkezik. A közvetlen csatlakozású Műveleti konzol esetén a fizikai hozzáférés korlátozásának érdekében a twinaxiális konzolokhoz hasonló fizikai biztonsági intézkedések alkalmazhatók.

A LAN csatlakozással rendelkező Műveleti konzol a Védett socket réteg (SSL) egy olyan változatát használja, amely igazolások nélkül biztosítja az eszköz és a felhasználó hitelesítését. Az ilyen kapcsolatoknál az eszköz hitelesítés alapját a szervizeszköz eszközprofil képezi. További részletek a 69. oldalon.

Felhasználó hitelesítés

A felhasználó hitelesítés nyújt bizonyságot a konzol eszközt használó személlyel kapcsolatban. A felhasználói hitelesítésre vonatkozó szempontok a konzol típusára való tekintet nélkül minden esetben ugyanazok.

Adatbizalmasság

Az adatbizalmasság biztosítja, hogy a konzol adatok csak a szándékolt fogadó számára olvashatók. A konzol adatok védelme érdekében a közvetlen csatlakozású Műveleti konzol a twinaxiális konzolokhoz hasonló fizikai kapcsolattal vagy LAN csatlakozás esetén biztonságos hálózati kapcsolattal rendelkezik. A közvetlen csatlakozású Műveleti konzol a twinaxiális kapcsolattal megegyező bizalmasságot nyújt. Ha a fizikai kapcsolat biztonságos, akkor a konzol adatok is védettek.

A LAN csatlakozással rendelkező Műveleti konzol a megfelelő kriptográfiai termékek (ACx és CEx) telepítése esetén biztonságos hálózati kapcsolatot használ. A konzol szekció az iSeries szerverre és a Műveleti konzol számítógépre telepített kriptográfiai termékek kombinációjával elérhető legmagasabb szintű titkosítást használja.

Megjegyzés: Kriptográfiai termékek telepítésének hiányában adattitkosításra nem kerül sor.

Integritás

Az integritás biztosítja, hogy a konzol adatokat ne módosíthassák az átvitel során. A konzol adatok védelme érdekében a közvetlen csatlakozású Műveleti konzol a twinaxiális konzolokhoz hasonló fizikai kapcsolattal vagy LAN csatlakozás esetén biztonságos hálózati

kapcsolattal rendelkezik. A közvetlen csatlakozású Műveleti konzol a twinaxiális kapcsolattal megegyező integritást nyújt. Ha a fizikai kapcsolat biztonságos, akkor a konzol adatok is védettek.

A LAN csatlakozással rendelkező Műveleti konzol a megfelelő kriptográfiai termékek (ACx és CEx) telepítése esetén biztonságos hálózati kapcsolatot használ. A konzol szekció az iSeries szerverre és a Műveleti konzol számítógépre telepített kriptográfiai termékek kombinációjával elérhető legmagasabb szintű titkosítást használja.

Megjegyzés: Kriptográfiai termékek telepítésének hiányában adattitkosításra nem kerül sor.

LAN csatlakozással rendelkező Műveleti konzol használata

Megjegyzés: Bármilyen Műveleti konzol eszköz lehet konzol, de csak a LAN alapú összeállítások használják a szervizeszköz felhasználói profilt.

Az iSeries szerver alapértelmezett szervizeszköz eszközprofilja a QCONSOLE, amelynek alapértelmezett jelszava szintén QCONSOLE. A LAN csatlakozással rendelkező Műveleti konzol minden egyes sikeres csatlakozásnál lecseréli a jelszót. További információk: "Műveleti konzol beállítási varázsló használata".

Az iSeries LAN csatlakozással rendelkező Műveleti konzol funkcióról további részleteket az Információs központ Műveleti konzol beállítása LAN csatlakozásra című témakörből tudhat meg.

LAN csatlakozással rendelkező Műveleti konzol védelme

LAN csatlakozással rendelkező Műveleti konzol használata esetén javasoljuk a következőket:

- Hozzon létre egy másik szervizeszköz eszközprofilt konzol attribútumokkal, és tárolja a profil információkat biztonságos helyen.
- Telepítse a Cryptographic Access Provider (5722–AC2 vagy 5722–AC3) terméket az iSeries szerverre, és a Client Encryption (5722–CE2 vagy 5722–CE3) terméket a Műveleti konzol számítógépre.
- Válasszon nemtriviális eszközinformációs jelszót.
- A Műveleti konzol számítógépet védje ugyanúgy, mintha egy twinaxiális vagy közvetlenül csatlakozó Műveleti konzolról lenne szó.

Műveleti konzol beállítási varázsló használata

LAN csatlakozással rendelkező Műveleti konzol használata esetén a szükséges információkat a beállítási varázsló hozza létre a számítógépen. A beállítási varázsló megkérdezi a szervizeszköz eszközprofilt, a szervizeszköz eszközprofil jelszót, és a szervizeszköz eszközprofil információk védelmére szolgáló jelszót.

Megjegyzés: A szervizeszköz eszközprofil információs jelszó a szervizeszköz eszközprofil információk (szervizeszköz eszközprofil és jelszó) zárolásának feloldására szolgál a számítógépen.

Hálózati kapcsolat kialakításakor a Műveleti konzol beállítási varázsló a titkosított szervizeszköz eszközprofil és jelszó megszerzése érdekében megkérdezi az eszközinformációs jelszót. Emellett meg kell adni egy érvényes szervizeszköz felhasználói azonosítást és jelszót is.

9. fejezet Gyanús programok felismerése

A számítógépek felhasználásának legújabb irányvonalai arra engednek következtetni, hogy nőtt annak a valószínűsége, hogy rendszeren megbízhatatlan forrásból származó vagy ismeretlen funkciókat végrehajtó programok találhatók. Néhány példa:

- A személyi számítógépes felhasználók gyakran cserélnek egymás között programokat. Ha a számítógép csatlakozik az iSeries rendszerre, akkor a program hatással lehet az iSeries szerverre is.
- A hálózatokhoz csatlakozó felhasználóknak további lehetőségeik is vannak programok beszerzésére, például különféle információs szolgáltatásoktól.
- A crackerek szintén egyre aktívabbak és hírhedtebbek. Gyakran közzéteszik a módszereiket és eredményeiket is. Ezeket az egyébként törvénytisztelő programozók is átvehetik.

Mindezen irányzatok vezettek el a számítástechnikai ipar **számítógépvírusnak** nevezett problémájához. A vírusok olyan programok, amelyek képesek más programok módosítására oly módon, hogy tartalmazzák a vírus egy példányát. Az ily módon érintett programokról azt mondjuk, hogy a vírus megfertőzte azokat. A vírusok emellett más tevékenységeket is végezhetnek, amelyek a rendszererőforrások elfogyásához vagy az adatok megsemmisüléséhez vezethetnek.

Az iSeries architektúra biztosít bizonyos szintű védelmet a számítógépvírusok fertőző jellemzőivel szemben. Ezt a “Védelem a számítógépvírusok ellen” szakasz részletezi. Az iSeries szerverek biztonsági adminisztrátorainak inkább a jogosulatlan funkciókat végrehajtó programok miatt kell aggódniuk. A fejezet további témakörei bemutatnak néhány módszert rossz szándékú programok futtatására a rendszeren. Ezzel együtt természetesen leírjuk a jogosulatlan funkciókat végrehajtó programok futásának megakadályozására szolgáló módszereket is.

Biztonsági tipp

Az első védelmi vonalnak mindig az objektum jogosultságnak kell lennie. Ha nincs egy jó terve az objektumok védelmének biztosítására, akkor a rendszer védtelen. Az információk bemutatnak különböző módszereket, amelyekkel a jogosult felhasználók kihasználhatják az objektum jogosultsági séma kibúvóit.

Védelem a számítógépvírusok ellen

A vírussal fertőzött számítógépen található egy olyan program, amely képes más programok módosítására. Az iSeries objektum alapú architektúrája a többi számítógépes architektúrához képest megnehezíti a bajkeverők dolgát az ilyen jellegű vírusok előállításakor és terjesztésekor. Az iSeries szerveren a különféle objektumtípusokon a típusra jellemző parancsok és utasítások használhatók. Fájlra vonatkozó utasítás nem használható például futtatható program objektumok módosítására (a legtöbb víruskészítő ezt a módszert követi). A más program objektumokat módosító programok létrehozása sem egyszerű feladat. Jelentős mennyiségű időt, erőfeszítést és gyakorlatot igényel, az általánosan nem hozzáférhető eszközök és dokumentációk igényéről nem is beszélve.

Az iSeries szerver azonban folyamatosan bővül olyan funkciókkal, amely lehetővé teszi számára a nyílt rendszerekből álló környezetekben való részvételt, amelynek eredményeként az iSeries szerverek néhány objektum alapú védelmi funkciója már nem alkalmazható. Az

integrált fájlrendszer (IFS) segítségével például lehetőség van bizonyos katalógus objektumok, például folyamfájlok közvetlen kezelésére.

Emellett bár az iSeries szerver architektúrája megnehezíti a vírusok szaporodását az iSeries szerver programok között, nem akadályozza meg azt, hogy az iSeries szerver vírushordozó legyen. Fájlszerverként az iSeries tárolhat olyan programokat, amelyeket több PC felhasználó is használ. Ezen programok bármelyike fertőzött lehet anélkül, hogy az iSeries szerver észlelné ezt. Az ilyen jellegű vírusfertőzések megakadályozása érdekében az iSeries szerverhez csatlakozó számítógépeken használni kell valamilyen vírusellenőrző programot.

Az iSeries szerverek több funkciót is biztosítanak a mutatók használatát támogató alacsonyszintű nyelvek segítségével végzett program módosítások megakadályozására:

- Ha a rendszer 40-es vagy magasabb biztonsági szinten fut, akkor az integritásvédelem védelmet nyújt a program objektumok módosítása ellen is. Nem futtathatók például az olyan programok, amelyek blokkolt (védett) gépi utasításokat használnak.
- A program ellenőrzési érték szintén a védelmet szolgálja a a más rendszereken mentett (és potenciálisan módosított) programok visszaállításakor. A 40-es vagy magasabb biztonsági szinteken alkalmazott integritásvédelmi funkciókat a program ellenőrzési értékekkel együtt az *iSeries biztonsági összefoglaló* 2. fejezete tárgyalja.

  Megjegyzés: A program ellenőrzési érték nem bolondbiztos, és nem helyettesíti a rendszeren visszaállított programokkal szembeni óvatosságot.

A rendszeren emellett többféle eszköz is rendelkezésre áll a módosított programok felismerésére:

- Az Objektum integritás ellenőrzése (CHKOBJITG) paranccsal keresheti meg a keresési feltételeknek megfelelő objektumokat (végrehajtható objektumokat), és győződhet meg ezek érintetlenségéről. Ez hasonló a vírusellenőrzési funkcióhoz.
- A biztonsági megfigyelési funkcióval megfigyelheti a megváltozott vagy visszaállított programokat. A jogosultsági szint rendszerváltozó *PGMFAIL, *SAVRST és *SECURITY értékeinek beállításakor olyan megfigyelési feljegyzések jönnek létre, amelyek segítségével felismerheti a vírushoz hasonló programok behozatalára irányuló kísérleteket. A megfigyelési értékeket és a megfigyelési napló bejegyzéseit részletekbe menően az *iSeries biztonsági összefoglaló* 9. fejezete és F függeléke tárgyalja.
- A Létrehozás kényszerítése (FRCCRT) paraméter használatával megadhatja a Program módosítása (CHGPGM) parancsnak, hogy hozza létre ismét a rendszerre visszaállított valamennyi programot. A rendszer a program ismételt létrehozásához a program sablont használja. Ha a program objektum megváltozott a fordítás után, akkor a rendszer ismét létrehozza és lecseréli a megváltozott objektumot. Ha a program sablonja blokkolt (védett) utasításokat tartalmaz, akkor rendszer nem tudja újból létrehozni a programot.
- A QFRCCVNRST (átalakítás kényszerítése a visszaállítás során) rendszerváltozóval írhatja elő a rendszerre visszaállított összes program ismételt létrehozását. A program ismételt létrehozásához a rendszer a program sablont használja. A rendszerváltozó többféle választási lehetőséget is nyújt az újból létrehozandó programok meghatározásához.
- A QVFYOBJRST (objektumok ellenőrzése a visszaállítás során) rendszerváltozó segítségével akadályozhatja meg a digitális aláírással nem rendelkező vagy érvénytelen digitális aláírással rendelkező programok visszaállítását. A digitális aláírások érvénytelensége azt jelenti, hogy a program megváltozott, amióta a fejlesztője aláírta. Saját programok, mentési fájlok és folyamfájlok aláírásához különféle API-k használhatók.

Az objektum aláírásról és ezeknek a rendszert ért támadások elleni védekezésben való felhasználásáról az “Objektum aláírás” oldalszám: 84 szakaszban olvashat.

Átvett jogosultság használatának megfigyelése

Az iSeries szerveren lehetőség van olyan programok létrehozására, amelyek átveszik a tulajdonosuk jogosultságait. Ez azt jelenti, hogy a programot futtató valamennyi felhasználó ugyanazokkal a jogosultságokkal (magánjogosultságok és speciális jogosultságok) rendelkezik, mint a program tulajdonos felhasználói profilja.

Az átvett jogosultság megfelelő felhasználás esetén értékes biztonsági eszköz. A “Menü hozzáférés felügyelet kiegészítése objektum biztonsággal” oldalszám: 46 szakasz bemutat például egy példát, amely menük és átvett jogosultságok kombinációjával terjeszti ki a menü hozzáférés felügyeletet. Az átvett jogosultságok segítségével például megvédheti a fontos fájlokat az erre célra szolgáló alkalmazáson kívüli módosítástól, miközben továbbra is lehetőség van a fájlok lekérdezésére.

A biztonsági adminisztrátornak meg kell győződnie az átvett jogosultságok megfelelő használatáról:

- A programoknak csak olyan felhasználói profilok jogosultságait szabad átvenniük, amelyek a funkciók használatához minimálisan szükséges jogosultságokkal rendelkeznek, és nincsenek extra jogosultságaik. Különösképp oda kell figyelni az *ALLOBJ speciális jogosultsággal rendelkező vagy fontos objektumokat birtokló felhasználói profil jogosultságait átvevő programokra.
- A jogosultságot átvevő programoknak egy adott funkcióra kell szolgálniuk, és nem biztosíthatnak parancsbeviteli lehetőségeket.
- A jogosultságot átvevő programokat megfelelően védeni kell.
- Az átvett jogosultságok túlzásba vitt használata negatív hatással lehet a rendszer teljesítményére. A teljesítménnyel kapcsolatos problémák elkerülése érdekében tekintse át az *iSeries biztonsági összefoglaló* 5. fejezetében található jogosultság ellenőrzési folyamatábrákat és az átvett jogosultságok használatára vonatkozó információkat.

SECBATCH menü menüpontjai:
1 - *azonnali elküldés* **40 - job ütemező használata**

Az Átvevő objektumok kinyomtatása (PRTADPOBJ) paranccsal (a SECTOOLS menü 21. menüpontja) figyelheti meg az átvett jogosultságok használatát a rendszeren.

A jelentésben szerepelnek a megadott felhasználói profil speciális jogosultságai, a felhasználói profil jogosultságait átvevő programok, illetve a profil jogosultságait használó ASP eszközök. A kiindulási információk rögzítése után elegendő a változásokat rögzítő változatok rendszeres időközönkénti lefuttatása. Ebben azok a programok szerepelnek, amelyek a jelentés legutóbbi futtatásakor még nem használtak átvett jogosultságokat, illetve amelyek átvett jogosultságai megváltoztak.

Ha visszaéléseket gyanít az átvett jogosultságok használatának kapcsán, akkor a QAUDLVL rendszerváltozó beállításai közé vegye fel a *PGMADP értéket. Ha az érték aktív, akkor a rendszer minden egyes jogosultságot átvevő program indításakor és befejezésekor bejegyzést ír a megfigyelési naplóba. A bejegyzés a programot indító felhasználó illetve a program nevét tartalmazza.

Átvett jogosultságok használatának korlátozása

Amikor egy iSeries program fut, akkor kétféleképpen használhat átvett jogosultságot az objektumok elérése érdekében:

- Maga a program képes a tulajdonos jogosultságának átvételére. Ezt a program vagy szervizprogram felhasználói profil (USRPRF) paraméterében lehet megadni.
- A program használhatja (örökölheti) egy olyan korábbi program átvett jogosultságait, amely még a job hívási vermében van. A program akkor is örökölheti a korábbi program átvett jogosultságait, ha a program maga nem vesz át jogosultságokat. Az Átvett jogosultság használata (USEADPAUT) határozza meg, hogy a program vagy szervizprogram örököl-e átvett jogosultságokat a hívási veremben található korábbi programoktól.

A korábbi programoktól örökölt átvett jogosultságok használatára az alábbiakban mutatunk be egy példát.

Tegyük fel, hogy az ICOWNER felhasználói profil *CHANGE jogosultsággal rendelkezik az ITEM fájlhoz, az ITEM fájl nyilvános jogosultsága pedig *USE. Az ITEM fájlra vonatkozóan más felhasználói profilok nem rendelkeznek kifejezett jogosultsággal. A 14. táblázat: három olyan programot tartalmaz, amelyek az ITEM fájlt használják:

14. táblázat: Átvett jogosultság használata (USEADPAUT) - Példa

Program neve	Program tulajdonosa	USRPRF érték	USEADPAUT érték
PGMA	ICOWNER	*OWNER	*YES
PGMB	ICOWNER	*USER	*YES
PGMC	ICOWNER	*USER	*NO

1. példa – Jogosultság átvétele:
1. A USERA futtatja a PGMA programot.
2. A PGMA program megkísérli az ITEM fájl megnyitását frissítésre.

Eredmény: A kísérlet sikerül. A USERA *CHANGE hozzáféréssel rendelkezik az ITEM fájlhoz, mivel a PGMA átveszi az ICOWNER profil jogosultságát.

2. példa – Átvett jogosultság használata:
1. A USERA futtatja a PGMA programot.
2. A PGMA program meghívja a PGMB programot.
3. A PGMB program megkísérli az ITEM fájl megnyitását frissítésre.

Eredmény: A kísérlet sikerül. Bár a PGMB program nem vesz át jogosultságot (a *USRPRF értéke *USER), lehetővé teszi a korábban átvett jogosultság használatát (a *USEADPAUT *YES értéke miatt). A PGMA program még mindig megtalálható a hívási veremben. Ennek megfelelően a USERA felhasználó *CHANGE jogosultsághoz jut az ITEM fájlhoz az ICOWNER jogosultsága miatt.

3. példa – Nincs átvett jogosultság használat:
1. A USERA futtatja a PGMA programot.
2. A PGMA program meghívja a PGMC programot.
3. A PGMC program megkísérli az ITEM fájl megnyitását frissítésre.

Eredmény: Jogosultsági hiba. A PGMC program nem vesz át jogosultságot. Emellett a PGMC program nem engedélyezi a korábbi programok átvett jogosultságainak használatát sem. Bár a PGMA még mindig megtalálható a hívási veremben, átvett jogosultság használatára nem kerül sor.

Új programok megakadályozása átvett jogosultságok használatában

Az átvett jogosultság átadása a verem későbbi programjainak lehetővé teheti egy hozzáértő programozó számára trójai program létrehozását. A trójai program a verem korábbi programjainak átvett jogosultságaiból megszerezheti a kártékony tevékenységéhez szükséges jogosultságokat. Ennek megakadályozása érdekében korlátozni kell azokat a felhasználókat, akik létrehozhatnak korábbi programok átvett jogosultságait öröklő programokat.

Új program létrehozásakor a rendszer a USEADPAUT paramétert automatikusan a *YES értékre állítja. Ha nem kívánja, hogy a program örökölje az átvett jogosultságokat, akkor a Program módosítása (CHGPGM) vagy a Szervizprogram módosítása (CHGSRVPGM) paranccsal állítsa a USEADPAUT paramétert *NO-ra.

Az átvett jogosultságokat öröklő programok létrehozására jogosult felhasználókat jogosultsági listákkal vagy az átvett jogosultság használata (QUSEADPAUT) rendszerváltozóval felügyelheti. Ha a QUSEADPAUT rendszerváltozóban jogosultsági listát ad meg, akkor a rendszer ezt a jogosultsági listát használja az új programok létrehozási módjának meghatározására.

Amikor egy felhasználó programot vagy szervizprogramot hoz létre, akkor a rendszer ellenőrzi a felhasználónak a jogosultsági listára vonatkozó jogosultságát. Ha a felhasználó rendelkezik *USE jogosultsággal, akkor az új program USEADPAUT paraméterének értéke *YES lesz. Ha a felhasználónak nincs *USE jogosultsága, akkor a USEADPAUT paraméter a *NO értéket kapja. A felhasználónak a jogosultsági listára vonatkozó jogosultsága nem származhat átvett jogosultságból.

A QUSEADPAUT rendszerváltozóban megadott jogosultsági lista felügyeli emellett azt is, hogy a felhasználó jogosult-e a programok vagy szervizprogramok USEADPAUT paraméterének módosítására a CHGxxx paranccsal.

Megjegyzések:

1. A jogosultsági listát nem kell QUSEADPAUT-nak nevezni. Eltérő nevű jogosultsági lista is létrehozható. Ezután adja meg a jogosultsági lista nevét a QUSEADPAUT rendszerváltozóban. A példában megadott parancsokban a megfelelő helyre helyettesítse be a jogosultsági lista nevét.
2. A QUSEADPAUT rendszerváltozó nem érinti a rendszer meglévő programjait. Az USEADPAUT paraméter meglévő programokra vonatkozó beállításhoz használja a CHGPGM vagy a CHGSRVPGM parancsot.

Korlátozóbb környezet: Ha a felhasználók többségének nem kívánja engedélyezni átvett jogosultságokat öröklő programok létrehozását, akkor tegye a következőket:

1. Írja be a következő parancsot a jogosultsági lista nyilvános jogosultságának *EXCLUDE-ra állításához:

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

2. A korábbi programok átvett jogosultságait öröklő programok létrehozására jogosult egyedi felhasználók megadásához írja be a következő parancsot:

   ```
   ADDAUTLE AUTL(QUSEADPAUT) USER(felhasználónév)
      AUT(*USE)
   ```

Kevésbé korlátozó környezet: Ha a felhasználók többségének engedélyezni kívánja átvett jogosultságokat öröklő programok létrehozását, akkor tegye a következőket:

1. Hagyja meg a jogosultsági lista nyilvános jogosultságának *USE értékét.

2. A korábbi programok átvett jogosultságait öröklő programok létrehozásában megakadályozott egyedi felhasználók megadásához írja be a következő parancsot:

```
ADDAUTLE AUTL(QUSEADPAUT)
   USER(felhasználónév) AUT(*EXCLUDE)
```

Trigger programok használatának megfigyelése

A DB2 UDB lehetővé teszi trigger programok társítását az adatbázisfájlokhoz. A trigger programok kezelésének képessége általános dolog a magas szintű funkciókat biztosító adatbáziskezelőknél.

Amikor trigger programot társít egy adatbázisfájlhoz, akkor meg kell adni a trigger program futásának idejét. Beállítható például olyan trigger program az ügyfelek megrendeléseit tartalmazó fájlhoz, amely új rekordok hozzáadásakor fut le. Amikor az ügyfél egyenlege túllépi a hitelkeretet, akkor a trigger program kinyomtathat egy figyelmeztető levelet az ügyfélnek, és üzenetet küldhet a hitelügyletekért felelős személynek.

A trigger programok hatékony lehetőséget nyújtanak mind alkalmazás funkciók biztosítására, mind az információk kezelésére. A trigger programok emellett lehetőséget nyújtanak a rossz szándékú felhasználóknak “Trójai programok” bevezetésére a rendszerre. Elképzelhető, hogy a rendszeren van valahol egy kártékony program, amely csak a rendszer egyik adatbázisfájljában bekövetkező bizonyos eseményre várakozik.

Megjegyzés: A Trójai faló története jól ismert a történelemből: Az ókori görögök Trója ostromlásakor egy katonákkal megtöltött hatalmas falovat készítettek. Miután elhitették a trójaiakkal, hogy a faló egy istenszobor, a trójaiak bevitték a falovat a várba, amelyből éjszaka kimásztak a katonák, és kinyitották Trója kapuit a többi görög harcos számára. A számítógépes világban emiatt nevezik a rejtett destruktív funkciókat tartalmazó programokat trójai programnak.

SECBATCH menü menüpontjai:
27 - *azonnali elküldés* **66** - *job ütemező használata*

A rendszer alapértelmezett beállításai korlátozzák a trigger programok hozzáadását az adatbázisfájlokhoz. Az objektum jogosultság körültekintő kezelése esetén a tipikus felhasználóknak általában nincs jogosultsága trigger program adatbázisfájlhoz társítására. (A parancsok futtatásához szükséges jogosultságok felsorolása az *iSeries biztonsági összefoglaló* című kiadvány D függelékében található.)

A Trigger programok kinyomtatása (PRTTRGPGM) paranccsal nyomtathatja ki egy adott könyvtár vagy minden könyvtár összes trigger programját.

Ezen kezdeti jelentés alapján értékelheti ki a rendszeren található trigger programokat. Ezután a változásokat tartalmazó jelentés rendszeres időközönkénti kinyomtatásával követheti nyomon a rendszer új trigger programjait.

A trigger programok kiértékelése során a következőket kell szem előtt tartani:

- Ki hozta létre a trigger programot? Ennek meghatározásához használja az Objektumleírás megjelenítése (DSPOBJD) parancsot.
- Mit tesz a program? Ennek megállapításához nézze át a program forrását, vagy konzultáljon a program szerzőjével. Ellenőrzi például a trigger program, hogy milyen

felhasználó futtatja? Elképzelhető például, hogy a trigger program egy adott felhasználóra (például QSECOFR) várakozik, hogy a kártékony funkcióját ne akadályozzák jogosultsági korlátozások.

A kezdeti információk rögzítése után a változásokat tartalmazó jelentés rendszeres időközönkénti kinyomtatásával követheti nyomon a rendszer új trigger programjait.

Rejtett programok keresése

A rendszerbe nemcsak trigger programok útján vihetők be trójai programok. A trigger programok a **végprogramok** egy bizonyos formái. Bizonyos események bekövetkezésekor, például trigger program esetén egy fájl frissítésekor, a rendszer lefuttatja az eseményhez társított végprogramot.

A rendszeren található további lehetséges végprogramokat a 15. táblázat: írja le. A végprogramok használatának és tartalmának kiértékelésére ugyanaz a módszer használható, mint a trigger programok esetében.

Megjegyzés: A 15. táblázat: nem sorolja fel az összes lehetséges végprogramot.

.

15. táblázat: Rendszer által biztosított végprogramok

Program neve	**Program futásának bekövetkezése**
A DDMACC hálózati attribútum felhasználó által megadott neve.	Amikor a felhasználó DDM fájlt próbál megnyitni a rendszeren, vagy DRDA kapcsolatot alakít ki.
A PCSACC hálózati attribútum felhasználó által megadott neve.	Amikor a felhasználó az eredeti kliensek használatakor Client Access funkciók segítségével próbál rendszerobjektumokhoz hozzáférni.
A QPWDVLDPGM rendszerváltozó felhasználó által megadott neve.	Amikor egy felhasználó a Jelszócsere funkciót futtatja.
A QRMTSIGN rendszerváltozó felhasználó által megadott értéke.	Amikor egy felhasználó interaktív bejelentkezésre tesz kísérletet távoli rendszerről.
QSYS/QEZUSRCLNP	Az automatikus tisztítási funkció futásakor.
A CHGBCKUP parancs EXITPGM paraméterének felhasználó által megadott értéke.	A Műveleti segédlet mentési funkció használatakor.
A CRTPRDLOD parancsban a felhasználó által megadott nevek.	A paranccsal létrehozott termék mentése és visszaállítása előtt és után, illetve törlésekor.
A CHGMSGD parancs DFTPGM paraméterének felhasználó által megadott értéke.	Ha egy üzenetnek van megadott alapértelmezett programja, akkor a rendszer az adott üzenet küldésekor lefuttatja a programot. A tipikus rendszereken található üzenetleírások nagy száma miatt az alapértelmezett programok használatának megfigyelése nehézkes lehet. alapértelmezett programok hozzáadásának megakadályozásához az üzenetfájlok (*MSGF objektumok) nyilvános jogosultságát javasolt a *USE értékben megállapítani.
A STREML3270 parancs FKEYPGM paraméterének felhasználó által megadott értéke.	Amikor egy felhasználó megnyom egy funkcióbillentyűt a 3270 eszköz emulációs szekcióban. A rendszer a végprogram lefutása után adja vissza a vezérlést a 3270 eszköz emulációs szekciónak.
A teljesítményfigyelő parancsok EXITPGM paraméterének felhasználó által megadott értéke.	Az STRPFRMON, ENDPFRMON, ADDPFRCOL és CHGPFRCOL parancsok által végzett adatfeldolgozáskor. A program az adatgyűjtés befejezésekor fut le.
A RCVJRNE parancs EXITPGM paraméterének felhasználó által megadott értéke.	A megadott naplóból és naplófogadóból kiolvasott valamennyi naplóbejegyzésen vagy naplóbejegyzés csoporton.

15. táblázat: Rendszer által biztosított végprogramok (Folytatás)

Program neve	Program futásának bekövetkezése
A QTNADDCR API számára átadott felhasználó által megadott név.	Véglegesítés vagy visszagörgetés művelet során.
A QHFRGFS API számára átadott felhasználó által megadott nevek.	Fájlrendszer funkciók végrehajtásakor.
A nyomtató eszközleírások SEPPGM paraméterének felhasználó által megadott értéke.	A spoolfájlok vagy nyomtatási feladatok előtt vagy után nyomtatott elválasztó oldalak tartalmának meghatározásakor.
QGPL/QUSCLSXT	Adatbázisfájl bezárásakor a fájl használati információk begyűjtésnek biztosításához.
A logikai fájlok FMTSLR paraméterének felhasználó által megadott értéke.	Amikor egy rekord kerül az adatbázisfájlba, és a rekordformátum neve nincs megadva a magas szintű nyelven írt programban. A kiválasztási program bemenetként megkapja a rekordot, meghatározza a rekordformátumot, és visszaadja azt az adatbázisnak.
A QATNPGM rendszerváltozóban, a felhasználói profilok ATNPGM paraméterében, illetve a SETATNPGM parancs PGM paraméterében a felhasználó által megadott név.	Amikor egy felhasználó megnyomja az Attention billentyűt.
A TRCJOB parancs EXITPGM paraméterének felhasználó által megadott értéke.	A Job nyomkövetése eljárás indítása előtt.

A végprogramok használatát lehetővé tevő parancsok esetén meg kell győződni arról, hogy a parancs alapértelmezését nem módosították egy végprogram megadásával. Meg kell győződni emellett, hogy az ilyen parancsok nyilvános jogosultsága nem elegendő a parancs alapértelmezések módosításához. A CHGCMDDFT parancs *OBJMGT jogosultságot igényel a parancshoz. A parancs futtatása nem igényel *OBJMGT jogosultságot.

Bejegyzett végprogramok kiértékelése

A bizonyos események bekövetkezésekor futó végprogramok bejegyzéséhez a rendszer bejegyzési funkciója használható. A rendszeren megadott bejegyzési információk kinyomtatásához használja a WRKREGINF OUTPUT(*PRINT) parancsot. A jelentésre az 8. ábra: mutat be egy példát:

```
              Work with Registration Information
 Exit point . . . . . . . . . . . . . . . :   QIBM_QGW_NJEOUTBOUND
 Exit point format  . . . . . . . . . . . :   NJEO0100
 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  . . . . . . . . . . . . . . . :
```

8. ábra: Bejegyzési információk kezelése - Példa

A jelentés a rendszer valamennyi kilépési pontjának vonatkozásában megadja, hogy jelenleg van-e bejegyzett végprogram a ponton. Ha egy kilépési ponton van bejegyzett program, akkor a WRKREGINF képernyő 8. menüpontjának (Programok megjelenítése) kiválasztásával tekintheti meg a bejegyzett programra vonatkozó információkat:

```
                     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  NJEO0100     *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
```

Az ilyen végprogramok kiértékelésekor alkalmazza a trigger programoknál megadott módszereket.

Ütemezett programok ellenőrzése

Az iSeries többféle módszert is biztosít a jobok későbbi időpontban kezdeményezett futásának ütemezéséhez, az egyik ilyen a job ütemező. Ezek a módszerek általában nem képviselnek biztonsági kockázatot, mivel a jobokat ütemező felhasználóknak ugyanolyan jogosultságokkal kell rendelkezniük, mint a a jobok kötegelten való elküldése esetén.

Ettől függetlenül rendszeres időközönként ellenőrizni kell az ütemezett jobokat. A vállalattól már távozott, elégedetlen felhasználó például használhatja ezt a módszert egy katasztrófa beütemezésére.

Mentési és visszaállítási képesség korlátozása

A legtöbb felhasználónak nem szükséges objektumok mentését és visszaállítását végezni a rendszeren. A mentési parancsok lehetőséget nyújtanak a szervezet információs tulajdonának adathordozóra vagy másik rendszerre másolására. A legtöbb mentési parancs támogatja a mentési fájlokat is, amelyek adathordozó vagy mentési/visszaállítási eszközre vonatkozó hozzáférés nélkül is eljuttathatók másik rendszerre (a SNDNETF paranccsal).

A visszaállítási parancsok lehetőséget adnak jogosulatlan objektumok, például programok, parancsok és fájlok visszaállítására a rendszeren. Mentési fájlok használatával a visszaállítás elvégezhető adathordozó és mentés/visszaállítási eszköz nélkül is. A mentési fájlok származhatnak másik rendszerről is a SNDNETF parancs vagy FTP használatával.

A mentési és visszaállítási műveletek korlátozására a következőket javasoljuk:

- Ellenőrizze, hogy mely felhasználók rendelkeznek a *SAVSYS speciális jogosultsággal. A *SAVSYS speciális jogosultság lehetővé teszi a felhasználónak az objektumok mentését és visszaállítását abban az esetben is, ha a felhasználó egyébként nem rendelkezik az objektum eléréséhez szükséges jogosultságokkal.
- Felügyelje a mentési és helyreállítási eszközökhöz való fizikai hozzáférést.
- Korlátozza a mentési és visszaállítási parancsok elérését. Az OS/400 licencprogramok telepítésekor az RSTxxx parancsok nyilvános jogosultsága *EXCLUDE. A SAVxxx

parancsok nyilvános jogosultsága *USE. Fontolja meg a SAVxxx parancsok nyilvános jogosultságának *EXCLUDE beállítását. Gondosan korlátozza az RSTxxx parancsok használatára jogosult felhasználókat.

- A QALWOBJRST rendszerváltozóval korlátozza a rendszer állapotú programok, a jogosultságokat átvevő programok és az ellenőrzési hibákkal rendelkező objektumok visszaállítását.
- A QVFYOBJRST rendszerváltozóval felügyelje az aláírt objektumok visszaállítását a rendszeren.
- A QFRCCVNRST rendszerváltozóval felügyelje a rendszerre visszaállított egyes objektumok ismételt létrehozását.
- A visszaállítási műveleteken végezzen biztonsági megfigyelést. Vegye fel a *SAVRST paramétert a QAUDLVL rendszerváltozóba, és rendszeres időközönként nyomtassa ki a visszaállítási műveletek eredményeként létrejött megfigyelési feljegyzéseket. (A megfigyelési bejegyzésekkel kapcsolatos műveletekről további információkat az *iSeries biztonsági összefoglaló* 9. fejezetében és F függelékében talál.)

Védett könyvtárak felhasználói objektumainak ellenőrzése

Az iSeries szerver minden jobjának van egy könyvtárlistája. A könyvtárlista határozza meg, hogy a rendszer milyen sorrendben nézi végig a könyvtárakat egy objektum keresésekor abban az esetben, ha az objektum nevével a könyvtárnév nincs megadva. Amikor például egy felhasználó a program megadása nélkül futtat egy programot, akkor a rendszer a profil könyvtárlistáját keresi végig, és a program első megtalált változatát fogja futtatni.

A könyvtárlistából adódó biztonsági kockázatokról, illetve a könyvtárnév megadása nélkül meghívott (**minősítetlen hívás**) programokról az *iSeries biztonsági összefoglaló* című kiadványban talál további részleteket. Emellett javaslatokat tesz a a könyvtárlisták tartalmának, illetve a rendszer könyvtárlisták módosítási képességének felügyeletére vonatkozóan.

A rendszer megfelelő működéséhez bizonyos rendszerkönyvtáraknak (például QSYS és QGPL) minden job könyvtárlistájában benne kell lenniük. Az objektum jogosultság segítségével mindenképpen felügyelni kell, hogy ezekhez a könyvtárakhoz ki adhat hozzá programokat. Ez megakadályozza, hogy valaki olyan imposztor programot helyezzen ezen könyvtárak valamelyikébe, amely neve a könyvtárlista későbbi részében található valamelyik program nevével egyezik meg.

Meg kell vizsgálni, ki jogosult a CHGSYSLIBL parancs futtatására, és figyelni kell az SV rekordokat a biztonsági megfigyelési naplóban. Egy rossz szándékú felhasználó megteheti például, hogy hozzáad egy könyvtárat a rendszer könyvtárlistához a QSYS könyvtár előtt, amelyből az IBM parancsok nevével megegyező jogosulatlan programok futhatnak.

SECBATCH menü menüpontjai:
28 - *azonnali elküldés* **67** - *job ütemező használata*

A Felhasználói objektumok kinyomtatása (PRTUSROBJ) paranccsal nyomtathatja ki egy adott könyvtár felhasználói (nem IBM) objektumainak listáját. A listában szereplő programok kiértékelésével megállapíthatja, hogy ki hozta létre ezeket, és milyen funkciókat látnak el.

A programoktól eltérő felhasználói objektumok is jelenthetnek biztonsági kockázatot, amennyiben ezek rendszerkönyvtárakban találhatók. Ha például egy program nem teljes képzésű névvel megadott fájlba bizalmas adatokat ír, akkor egy egyszerű trükkel rávehető arra, hogy hamis fájlt nyisson meg, és abba írja az adatokat.

10. fejezet Betörési kísérletek felismerése és megakadályozása

Ez a fejezet különféle tippeket sorol fel a lehetséges biztonsági kockázatok és bajkeverők felismeréséhez.

Fizikai biztonság

A rendszeregység fontos üzleti tulajdon, egyszersmind potenciális rendszerbe jutási hely. A rendszeregységen belül több kicsi és értékes alkatrész is található. A rendszeregységet felügyelt helyre kell helyezni, nehogy a kicsi, de értékes alkatrészeket kilopják belőle.

A rendszeregységen található egy vezérlőpanel, amely különféle alapszintű műveleteket munkaállomás nélkül tesz lehetővé. A vezérlőpanelen a következő műveletek végezhetők el:

- Rendszer leállítása.
- Rendszer indítása.
- Operációs rendszer betöltése.
- Szervizfunkciók indítása.

A felsorolt tevékenységek mindegyike alkalmas a rendszer felhasználóinak félbeszakítására. Emellett potenciális biztonsági kockázatot is jelentenek a rendszerre. A tevékenységek korlátozásához használja a rendszerhez tartozó kulcsot. A vezérlőpanel használatának megakadályozásához helyezze a kulcsot Biztonságos pozícióba, távolítsa el a kulcsot, és tárolja biztonságos helyen.

Megjegyzések:

1. Ha a rendszeren távoli IPL-t vagy távoli diagnosztikai funkciókat kíván végrehajtani, akkor a kulcsot más pozícióba kell állítani. A kulcs beállításokról további részleteket az iSeries Információs központ Kezdeti lépések című témakörében talál (az elérésével kapcsolatos részleteket az “Előfeltétel és kapcsolódó információk” oldalszám: xii szakasz tartalmazza).
2. A kulcsot nem minden rendszeregység tartalmazza alapfelszereltségként.

Felhasználói profilokkal kapcsolatos tevékenységek megfigyelése

A felhasználói profilok biztosítják a rendszerre való bejutást. A felhasználói profil paraméterei határozzák meg a felhasználó környezetét és biztonsági jellemzőit. A biztonsági adminisztrátornak felügyelnie és követnie kell a rendszer felhasználói profiljaiban történt változásokat.

A biztonsági megfigyelés beállítható oly módon, hogy a felhasználói profilok változásai naplózásra kerüljenek. A változásokat tartalmazó jelentés kinyomtatására a DSPAUDJRNE parancs használható.

Létrehozhatók olyan végprogramok, amelyek kiértékelik a felhasználói profilokkal kapcsolatosan kért tevékenységeket. A felhasználói profil parancsok kilépési pontjait a 16. táblázat: sorolja fel.

16. táblázat: Felhasználói profil tevékenységek kilépési pontjai.

Felhasználói profil parancs	Kilépési pont neve
Felhasználói profil létrehozása (CRTUSRPRF)	QIBM_QSY_CRT_PROFILE
Felhasználói profil módosítása (CHGUSRPRF)	QIBM_QSY_CHG_PROFILE

16. táblázat: Felhasználói profil tevékenységek kilépési pontjai. (Folytatás)

Felhasználói profil parancs	Kilépési pont neve
Felhasználói profil törlése (DLTUSRPRF)	QIBM_QSY_DLT_PROFILE
Felhasználói profil visszaállítása (RSTUSRPRF)	QIBM_QSY_RST_PROFILE

A végprogram megvizsgálhatja például az olyan szándékolt módosításokat, amelyek hatására a felhasználó képes lesz egy program jogosulatlan változatának futtatására. Ilyenek például az eltérő jobleírást vagy új aktuális könyvtárat hozzárendelő módosítások. A végprogram az ilyen esetekben a kapott információk alapján értesítheti az üzenetsort, vagy eljárhat (például a felhasználói profil módosításával vagy letiltásával).

A felhasználói profilokkal kapcsolatos tevékenységek végprogramjairól további részleteket az *iSeries biztonsági összefoglaló* című kiadvány tartalmaz.

Objektum aláírás

Valamennyi biztonsági óvintézkedés hiábavaló, ha valaki megkerülheti ezeket azáltal, hogy megpiszkált adatokat hoz be a rendszerre. Az iSeries szerver rendelkezik olyan beépített szolgáltatásokkal, amelyek segítségével megakadályozhatja a megpiszkált szoftverek betöltését a rendszerre, illetve felismerheti a már betöltött ilyen jellegű szoftvereket. Az egyik ilyen technika a V5R1 kiadásban bevezetett objektum aláírás.

Az objektum aláírás az iSeries szerver implementációja a ″digitális aláírásként″ ismert kriptográfiai koncepcióra. Az ötlet viszonylag egyszerű: amikor a szoftver előállítója készen áll a szoftver szállítására, akkor ″aláírja″ a szoftvert. Ez az aláírás semmiféle garanciát nem nyújt a szoftver funkcióra vonatkozóan. Lehetőséget nyújt viszont annak hitelt érdemlő megállapítására, hogy a szoftver valóban az aláíró szállítótól származik-e, illetve hogy a szoftver megváltozott-e az aláírás óta. Ez különösen akkor fontos, ha a szoftver az Interneten keresztül került átvitelre, vagy olyan adathordozón található, amelyről gyanítja, hogy módosították.

A digitális aláírások szélesebb körű felügyeletet biztosítanak a rendszerre tölthető szoftverek felett, és lehetővé teszik a betöltés után történt változások felismerését. Az Objektum visszaállítás ellenőrzése (QVFYOBJRST) nevű új rendszerváltozó segítségével beállítható egy olyan korlátozó stratégia, amely megköveteli, hogy a rendszeren csak az ismert szoftverforrások aláírásával ellátott szoftver tölthető be. Nyíltabb stratégia szintén megvalósítható, például az aláírások megléte esetén ezek ellenőrzése.

Valamennyi OS/400 szoftvert, illetve az iSeries szerveren futó licencprogramokat és ezek opcióit aláírta egy olyan forrás, amelyben a rendszer megbízik. Az aláírások segítik a rendszer integritásának fenntartását, a javítások aláírása segítségével pedig meggyőződhet arról, hogy a javítás megbízható forrásból származik, és nem módosították az esetleges hálózati átvitel során. Az aláírások azután is ellenőrizhetők, hogy a szoftver bekerült a rendszerbe. A CHKOBJITG (Objektum integritásának ellenőrzése) parancs a meglévő integritási ellenőrzések mellett kibővült az aláírások ellenőrzésének képességével is. Emellett a Digitális igazolás kezelőbe is kerültek új panelek, amelyek segítségével ellenőrizheti a rendszeren található objektumok aláírásait, beleértve az operációs rendszer objektumait is.

Az operációs rendszer aláírásához hasonlóan a digitális aláírások felhasználhatók az üzletmenet szempontjából kritikus szoftverek integritásának védelmére is. Elképzelhető, hogy a szoftver szállítója már aláírta a szoftvert, de ha mégsem, akkor helyben is aláírható, sőt aláírhatók a saját fejlesztésű szoftverek is. Ezután a biztonsági stratégia kiegészíthető oly módon, hogy a CHKOBJITG parancs vagy a Digitális igazolás kezelő segítségével rendszeres időközönként ellenőrzi a szoftverek aláírásait, vagyis meggyőződhet arról, hogy az

objektumok nem változtak meg az aláírásuk óta. Emellett megkövetelhető, hogy a rendszerre csak olyan szoftvert lehessen visszaállítani, amelyet a rendszer vagy egy másik megbízhatónak tekintett forrás aláírt. Az IBM-en kívüli szállítóktól származó iSeries szoftverek aláírásának hiánya miatt ez azonban elképzelhető, hogy túl erős korlátozás. Az új digitális aláírás támogatás rugalmas eszközt biztosít a szoftverek integritásának lehető leghatékonyabb védelmére.

A szoftverek védelmét szolgáló digitális aláíráson kívül a digitális igazolások még számos módon felhasználhatók. A digitális igazolásokról további részleteket az Információs központ Digitális igazolás kezelő című témakörében talál (az elérésére vonatkozó részleteket az “Előfeltétel és kapcsolódó információk” oldalszám: xii szakasz írja le).

Alrendszerleírások megfigyelése

Amikor elindul egy alrendszer az iSeries szerveren, akkor a rendszer létrehoz egy környezetet a rendszerbe belépő és azon futó jobok számára. A környezet jellemzőit az alrendszerleírás határozza meg. Az alrendszerleírások ennek megfelelően különféle lehetőségeket nyújthatnak a rosszindulatú felhasználóknak. A bajkeverők egy alrendszerleírás segítségével megadhatják egy program automatikus indítását, vagy lehetővé tehetik a felhasználói profil nélküli bejelentkezést.

A Nyilvános jogosultságok visszavonása (RVKPUBAUT) parancs futtatásakor a rendszer *EXCLUDE értékre állítja az alrendszerleírásokkal kapcsolatos parancsok nyilvános jogosultságát. Ez megakadályozza az erre kifejezetten fel nem jogosított (és az *ALLOBJ speciális jogosultsággal nem rendelkező) felhasználókat az alrendszerleírások létrehozásában és módosításában.

Az alábbi témakörök a rendszer meglévő alrendszerleírásainak áttekintésére vonatkozóan adnak néhány tanácsot. Az összes alrendszerleírásról az Alrendszerleírások kezelése (WRKSBSD) paranccsal készíthet listát. Az 5. (Megjelenítés) menüpont kiválasztása esetén megjelenik a kijelölt leírásra vonatkozó menü. Ebben látható az alrendszer környezet részeinek listája.

A részekre vonatkozó részletek megjelenítéséhez használja a megfelelő menüpontokat. A menü első két elemének módosítására az Alrendszerleírás módosítása (CHGSBSD) parancsot használhatja. A további elemek módosításához használja a bejegyzés típusának megfelelő hozzáadási, módosítási vagy eltávolítási parancsot. A munkaállomás bejegyzések módosítására például használja a Munkaállomás bejegyzés módosítása (CHGWSE) parancsot.

Az alrendszerleírások kezeléséről további részleteket a *Work Management* című kiadvány tartalmaz. Itt találhatók az IBM által szállított alrendszerleírások alapértelmezett értékei is.

Automatikusan induló job bejegyzések

Az automatikusan induló job bejegyzések egy jobleírás nevét tartalmazzák. A jobleírás tartalmazhat olyan adatkérést (RQSDTA), amelynek hatására egy program vagy parancs fut le. Az RQSDTA lehet például CALL LIB1/PROGRAM1. Ebben az esetben az alrendszer minden indításakor lefut a LIB1 könyvtár PROGRAM1 programja.

Vizsgálja meg az automatikusan induló job bejegyzéseket és a hozzájuk társított jobleírásokat. Győződjön meg róla, hogy megértette az alrendszer indításakor automatikusan lefutó program funkcióját, és ennek szükségességét.

Munkaállomás nevek és típusok

Az alrendszerek az indulás során lefoglalják a munkaállomás név és munkaállomás típus bejegyzésekben (kifejezetten vagy általánosan) felsorolt valamennyi nem lefoglalt munkaállomást. Amikor egy felhasználó bejelentkezik, akkor arra az alrendszerre jelentkezik be, amely a munkaállomását lefoglalta.

A munkaállomás bejegyzés adja meg, hogy milyen jobleírás kerül felhasználásra a munkaállomáson indított jobokhoz. A jobleírás tartalmazhat olyan adatkérést, amelynek hatására egy program vagy parancs fut le. Az RQSDTA paraméter értéke lehet például CALL LIB1/PROGRAM1. Ilyenkor minden esetben, amikor egy felhasználó ezen alrendszer által lefoglalt munkaállomásra jelentkezik be, lefut a LIB1 könyvtár PROGRAM1 programja.

Nézze meg a munkaállomás bejegyzéseket és a társított jobleírásokat. Győződjön meg róla, hogy senki nem adott hozzá vagy módosított olyan bejegyzéseket, amelyek eredményeként ellenőrizetlen programok futnak le.

A munkaállomás bejegyzések megadhatnak alapértelmezett felhasználói profilt is. Bizonyos alrendszer konfigurációk esetében ez lehetővé teszi a bejelentkezést egyszerűen csak az Enter lenyomásával. Ha a rendszeren alkalmazott biztonsági szint (QSECURITY rendszerváltozó) 40-nél alacsonyabb, akkor érdemes átnézni a munkaállomás bejegyzéseket alapértelmezett felhasználók után kutatva.

Jobsor bejegyzések

Az alrendszerek az indulás során lefoglalják az alrendszer leírásában megadott nem lefoglalt jobsorokat. A jobsor bejegyzések nem képviselnek közvetlen biztonsági kockázatot. Segítségükkel azonban megbolygatható a rendszer teljesítménye a jobok nem megfelelő környezetben való futtatásával.

Az alrendszerleírások jobsor bejegyzéseit érdemes időről időre átnézni, és meggyőződni arról, hogy a kötegelt jobok valóban ott futnak, ahol az helyénvaló.

Továbbítási bejegyzések

A továbbítási bejegyzések határozzák meg, hogy mi történik a jobbal, amikor az belép az alrendszerbe. Az alrendszer az összes jobtípushoz (kötegelt, interaktív és kommunikációs) használ továbbítási bejegyzéseket. A továbbítási bejegyzések a következőket határozzák meg:

- A job osztálya. A jobsor bejegyzésekhez hasonlóan a jobokhoz társított osztály hatással lehet ugyan a teljesítményre, de biztonsági kockázatot nem jelent.
- A job indulásakor lefutó program. Nézze meg a továbbítási bejegyzéseket, és győződjön meg róla, hogy senki nem adott hozzá vagy módosított olyan bejegyzéseket, amelyek eredményeként ellenőrizetlen programok futnak le.

Kommunikációs bejegyzések és távoli hely nevek

Amikor egy kommunikációs job belép a rendszerbe, a rendszer az aktív alrendszer kommunikációs bejegyzései és a távoli hely név bejegyzések segítségével határozza meg a kommunikációs job futásának módját. A bejegyzésekben a következőket érdemes megnézni:

- Minden alrendszer képes kommunikációs jobok futtatására. Ha egy kommunikációs célt szolgáló alrendszer nem aktív, akkor a rendszerbe belépni szándékozó jobok elképzelhető, hogy egy másik alrendszerleírásban találnak olyan bejegyzést, amely megfelel az igényeiknek. Ennek megfelelően az összes alrendszerleírás bejegyzéseit érdemes megvizsgálni.

- A kommunikációs bejegyzések egy jobleírást tartalmaznak. A jobleírás tartalmazhat olyan adatkérést, amelynek hatására egy program vagy parancs fut le. A kommunikációs bejegyzések és a hozzájuk tartozó jobleírások áttekintésével győződjön meg róla, hogy érti a jobok indulásának módját.
- A kommunikációs bejegyzések megadnak egy alapértelmezett felhasználói profilt is, amelyet a rendszer különféle helyzetekben használhat fel. Vizsgálja meg az alapértelmezett profil szerepét. Ha a rendszeren vannak alapértelmezett profilok, akkor győződjön meg róla, hogy ezek jogosultsága minimális. Az alapértelmezett felhasználói profilokról további információkat a 12. fejezet, “Biztonságos APPC kommunikáció” szakasz tartalmaz.

  A felhasználói profilt meghatározó kommunikációs bejegyzések azonosításához használja az Alrendszerleírás kinyomtatása (PRTSBSDAUT) parancsot.

Előindított job bejegyzések

Az előindított job bejegyzések készíthetik fel az alrendszereket bizonyos típusú jobok fogadására, amelyek így gyorsabban indulhatnak el. Előindított jobok az alrendszer indulásakor vagy igény szerint futnak le. Az előindított jobok bejegyzései a következőket határozzák meg:

- Futtatandó program

  Alapértelmezett felhasználói profil

  Jobleírás

Ezek mindegyike hordozhat biztonsági kockázatokat. Meg kell győződni róla, hogy az előindított job bejegyzések csakis jogosult és szándékolt funkciókat hajtanak végre.

Jobok és jobleírások

A jobleírások olyan kérés adatokat és továbbítási adatokat tartalmaznak, amelyek hatására a jobleírás használatakor lefuthat egy adott program. Ha a jobleírás megad egy programot az adatkérés paraméterben, akkor a rendszer lefuttatja a programot. Ha a jobleírás továbbítási adatokat tartalmaz, akkor a rendszer lefuttatja a továbbítási adatoknak megfelelő továbbítási bejegyzésben megadott programot.

A rendszer a jobleírásokat az interaktív és a kötegelt jobokhoz is használja. Interaktív jobok esetén a jobleírást a munkaállomás bejegyzés határozza meg. A munkaállomás bejegyzés értéke jellemzően *USRPRF, vagyis a rendszer a felhasználói profilban megadott jobleírást használja. Kötegelt jobok esetén a jobleírást a jobok elküldésekor kell meghatározni.

A jobleírásokat érdemes rendszeres időközönként átnézni, és meggyőződni arról, hogy nem futtatnak nem szándékolt programokat. Emellett objektum jogosultságokkal biztosítani kell, hogy a jobleírásokat ne módosíthassák. A *USE jogosultság elég a jobleírással rendelkező jobok futtatásához. Az általános felhasználóknak nem szükséges *CHANGE jogosultságot adni a jobleírásokhoz.

SECBATCH menü menüpontjai:
15 - *azonnali elküldés* **54** - *job ütemező használata*

A jobleírások megadhatják azt is, hogy a jobnak milyen felhasználói profil alatt kell futnia. 40-es és magasabb biztonsági szinten a futtatáshoz a felhasználónak *USE jogosultsággal kell rendelkeznie a jobleíráshoz és a benne megadott felhasználói profilhoz is. A 40-nél alacsonyabb biztonsági szinteken elegendő, ha a felhasználó csak a jobleírás vonatkozásában rendelkezik *USE jogosultsággal.

A Jobleírás jogosultság kinyomtatása (PRTJOBDAUT) parancs segítségével nyomtathatja ki azon jobleírásokat, amelyek felhasználói profilt adnak meg, és nyilvános jogosultságuk *USE.

A jelentésben szerepelnek a jobleírásban megadott felhasználói profil speciális jogosultságai is. Emellett megtalálhatók benne a felhasználói profil csoportprofiljai által birtokolt speciális jogosultságok is. A felhasználói profil magánjogosultságainak megjelenítéséhez használja a következő parancsot:

```
DSPUSRPRF USRPRF(profilnév) TYPE(*OBJAUT)
```

A jobleírás megadja a job futásakor használandó könyvtárlistát. Ha valaki módosíthatja egy felhasználó könyvtárlistáját, akkor a felhasználó egy másik könyvtárból egy program jogosulatlan változatát futtathatja. Éppen ezért a rendszer jobleírásaiban megadott könyvtárlistákat rendszeres időközönként át kell tekinteni.

Végül a Job elküldése (SBMJOB) és a Felhasználói profil létrehozása (CRTUSRPRF) parancs alapértelmezett értékeinek ellenőrzésével meg kell győződni arról, hogy a parancsokat nem módosították más jobleírások megadásával.

Architekturális tranzakciós program nevek

Bizonyos kommunikációs kérések egy adott típusú jelzést küldenek a rendszerre. Ezt a kérést **architektúra tranzakciós program névnek (TPN)** hívjuk, mégpedig azért, mert a tranzakciós program a rendszer APPC architektúrájának része. Ilyen architektúra TPN például a terminál átjelentkezési kérés. Az architektúra tranzakciós program nevek a kommunikáció szokásos működésének részei, így nem feltétlenül képviselnek biztonsági kockázatot. Ettől függetlenül az architektúra TPN-ek nem tervezett lehetőségeket nyújthatnak a rendszerbe való belépésre.

Bizonyos TPN-ek a kérésben nem adnak át profilnevet. Ha a kérés olyan kommunikációs bejegyzéssel kerül társításra, amelynek alapértelmezett felhasználója a *SYS, akkor elképzelhető, hogy a kérés kezdeményezésre kerül a rendszeren. A *SYS profil azonban csak rendszerfunkciókat futtathat, felhasználói alkalmazásokat nem.

Ha az architektúra tranzakciós program neveket nem kívánja alapértelmezett profillal futtatni, akkor a kommunikációs bejegyzésekben módosítsa a *SYS felhasználót *NONE-ra. Az “Architekturális TPN kérések” oldalszám: 89 rész az architektúra tranzakciós program neveket és a hozzájuk társított felhasználói profilokat sorolja fel.

Ha egy adott TPN-t egyáltalán nem kíván futtatni a rendszeren, akkor tegye a következőket:

1. Hozzon létre egy több paramétert fogadó CL programot. A program ne végezzen semmilyen funkciót. Egyszerűen csak a paraméterek deklarációs (DCL) utasításait és a befejezést tartalmazza.

2. Vegyen fel egy továbbítási bejegyzést a TPN számára minden olyan alrendszerben, amelyben kommunikációs vagy távoli hely név bejegyzések találhatók. A továbbítási bejegyzésnek a következőket kell megadnia:
   - Egy *Összehasonlítási érték* (CMPVAL) paramétert, amely megegyezik a TPN programjának nevével (lásd: Architekturális TPN kérések), és kezdő pozíciója 37.
   - Egy *Meghívandó program* (PGM) paramétert, amely megegyezik a lépés: 1 oldalszám: 88 helyen létrehozott program nevével. Ez akadályozza meg, hogy a TPN másik továbbítási bejegyzést (például *ANY) találjon.

Több TPN már rendelkezik saját továbbítási bejegyzéssel a QCMN alrendszerben. Ezek teljesítményszempontok miatt kerültek hozzáadásra.

Architekturális TPN kérések

17. táblázat: TPN kérések programjai és felhasználói

TPN kérés	Program	Felhasználói profil	Leírás
X'30F0F8F1'	AMQCRC6A	*NONE	Üzenetsor kezelés
X'06F3F0F1'	QACSOTP	QUSER	APPC bejelentkezési tranzakciós program
X'30F0F2D1'	QANRTP	QADSM	ADSM/400 APPC konfiguráció
X'30F0F1F9'	QCNPCSUP	*NONE	Osztott mappák
X'07F0F0F1'	QCNTEDDM	QUSER	DDM
X'07F6C4C2'	QCNTEDDM	QUSER	Távoli SQL–DRDA1
X'30F0F7F7'	QCQNRBAS	QSVCCS	SNA CC_Server
X'30F0F1F4'	QDXPRCV	QUSER	DSNX–PC fogadó
X'30F0F1F3'	QDXPSEND	QUSER	DSNX–PC küldő
X'30F0F2C4'	QEVYMAIN	QUSER	ENVY**/400 szerver
X'30F0F6F0'	QHQTRGT	*NONE	PC adatsor
X'30F0F8F0'	QLZPSERV	*NONE	Client Access licenckezelő
X'30F0F1F7'	QMFRCVR	*NONE	PC üzenetfogadó
X'30F0F1F8'	QMFSNDR	*NONE	PC üzenetküldő
X'30F0F6F6'	QND5MAIN	QUSER	APPN 5394 munkaállomás vezérlő
DB2DRDA	QCNTEDDDM	QUSER	DB2DRDA
APINGD	QNMAPINGD	QUSER	APINGD
X'30F0F5F4'	QNMEVK	QUSER	Rendszerfelügyeleti segédprogramok
X'30F0F2C1'	QNPSERVR	*NONE	PWS-I hálózati nyomtatási szerver
X'30F0F7F9'	QOCEVOKE	*NONE	Rendszerközti naptár
X'30F0F6F1'	QOKCSUP	QDOC	Katalógus árnyékolás
X'20F0F0F7'	QOQSESRV	QUSER	DIA v2
X'20F0F0F8'	QOQSESRV	QUSER	DIA v2
X'30F0F5F1'	QOQSESRV	QUSER	DIA v2
X'20F0F0F0'	QOSAPPC	QUSER	DIA v1
X'30F0F0F5'	QPAPAST2	QUSER	S/36—S/38 átjelentkezés
X'30F0F0F9'	QPAPAST2	QUSER	Nyomtató átjelentkezés
X'30F0F4F6'	QPWFSTP0	*NONE	2-es típusú osztott mappák
X'30F0F2C8'	QPWFSTP1	*NONE	Client Access fájlszerver

17. táblázat: TPN kérések programjai és felhasználói (Folytatás)

TPN kérés	Program	Felhasználói profil	Leírás
X'30F0F2C9'	QPWFSTP2	*NONE	Windows** Client Access fájlszerver
X'30F0F6F9'	QRQSRVX	*NONE	Távoli SQL–összevont szerver
X'30F0F6F5'	QRQSRV0	*NONE	Véglegesítés nélküli távoli SQL
X'30F0F6F4'	QRQSRV1	*NONE	Véglegesítés nélküli távoli SQL
X'30F0F2D2'	QSVRCI	QUSER	SOC/CT
X'21F0F0F8'	QS2RCVR	QGATE	SNADS FS2 fogadó
X'21F0F0F7'	QS2STSND	QGATE	SNADS FS2 küldő
X'30F0F1F6'	QTFDWNLD	*NONE	PC átviteli funkció
X'30F0F2F4'	QTIHNPCS	QUSER	TIE funkció
X'30F0F1F5'	QVPPRINT	*NONE	PC virtuális nyomtatás
X'30F0F2D3'	QWGMTP	QWGM	Ultimedia Mail/400 szerver
X'30F0F8F3'	QZDAINIT	QUSER	PWS-I adathozzáférési szerver
X'21F0F0F2'	QZDRCVR	QSNADS	SNADS fogadó
X'21F0F0F1'	QZDSTSND	QSNADS	SNADS küldő
X'30F0F2C5'	QZHQTRG	*NONE	PWS-I adatsor szerver
X'30F0F2C6'	QZRCSRVR	*NONE	PWS-I távoli parancs szerver
X'30F0F2C7'	QZSCSRVR	*NONE	PWS-I központi szerver

Biztonsági események megfigyelésének módszerei

A biztonság beállítása nem egyszeri feladat. Folyamatosan követni kell a rendszer változásait és a biztonsági hibákat, majd el kell végezni a biztonsági környezet ezeknek megfelelő módosításait.

A biztonsági jelentések segítséget nyújtanak a rendszeren bekövetkezett biztonsággal kapcsolatos változások követéséhez. A biztonsági hibák és kockázatok felismeréséhez ezen kívül a következő rendszerfunkciók nyújthatnak segítséget:

- A biztonsági megfigyelés hatékony eszköz, amellyel többféle biztonsággal kapcsolatos eseményt is nyomon követhet a rendszeren. Beállítható például, hogy a rendszer megfigyelési feljegyzést írjon minden egyes alkalommal, amikor egy felhasználó megnyit egy adott adatbázisfájlt frissítésre. Lehetőség van a rendszerváltozókat ért összes módosítás megfigyelésére is. Megfigyelhetők a felhasználók által végzett objektum visszaállítás során bekövetkezett tevékenységek is.

  A biztonsági megfigyelési funkciót részletekbe menően az *iSeries biztonsági összefoglaló* 9. fejezete tárgyalja. A rendszer biztonsági megfigyelésének beállítására a Biztonsági megfigyelés módosítása (CHGSECAUD) parancs használható. A Megfigyelési napló bejegyzések megjelenítése (DSPAUDJRNE) paranccsal emellett kinyomtathatja a kijelölt információkat a biztonsági megfigyelési naplóból.
- Létrehozhatja a QSYSMSG üzenetsort a kritikus rendszeroperátori üzenetek fogadására. A QSYSOPR üzenetsorba egy átlagos munkanapon sok, vegyes fontosságú üzenet kerül. A QSYSOPR üzenetsorba küldött üzenetek nagy mennyisége miatt elképzelhető, hogy egy biztonsági szempontból kritikus üzenetet nem vesznek észre.

  Ha létrehoz a rendszer QSYS könyvtárában egy QSYSMSG üzenetsort, akkor a rendszer bizonyos kritikus üzeneteket automatikusan ide irányít az alapértelmezett QSYSOPR üzenetsor helyett.

Ezután létrehozhat egy programot a QSYSMSG üzenetsor figyelésére, vagy beállíthatja megszakítás módra saját maga vagy egy másik megbízható felhasználó számára.

3. rész Alkalmazások és hálózati kommunikáció

11. fejezet Integrált fájlrendszer használata a fájlok védelmére

Az integrált fájlrendszer több lehetőséget is biztosít az iSeries információk tárolására és megjelenítésére. Az integrált fájlrendszer az OS/400 operációs rendszernek az a része, amely támogatja a folyam bemeneti és kimeneti műveleteket is. Az általa biztosított tárterület kezelési módszerek rokonok (és kompatíbilisek) a személyi számítógépes és UNIX operációs rendszerek módszereivel.

Az integrált fájlrendszer segítségével a rendszer valamennyi objektuma egy hierarchikus katalógusszerkezet szemszögéből látható. A felhasználók ettől függetlenül az objektumokat a legtöbb esetben az adott fájlrendszerre jellemző módon látják. A ″hagyományos″ iSeries objektumok például a QSYS.LIB fájlrendszerben találhatók. A felhasználók ezeket az objektumokat jellemzően könyvtárak szemszögéből fogják látni. A QDLS fájlrendszerben található objektumokat általában mappákba rendezett dokumentumok módján látják. A gyökér (/), a QOpenSys és a felhasználói fájlrendszerek hierarchikus (egymásba ágyazott) katalógusszerkezetként láthatók.

A biztonsági adminisztrátornak meg kell ismernie a következőket:

- A rendszeren használt fájlrendszerek
- Az egyes fájlrendszerek egyedi biztonsági jellemzői

Az alábbi témakörök mutatnak be néhány általános szempontot az integrált fájlrendszer biztonságával kapcsolatban.

Az Integrált fájlrendszer biztonsági megközelítése

A gyökér fájlrendszer szolgál alapul az iSeries szerverek összes többi fájlrendszere számára. Magas szinten tekintve integrált nézetben egyesíti a rendszer összes objektumát. Az iSeries szerverek többi fájlrendszere a fájlrendszer céljától függően különböző objektumkezelési és integrációs megközelítést követ. A QOPT (optikai) fájlrendszer például lehetővé teszi az iSeries alkalmazások és szerverek (beleértve az iSeries Access for Windows fájlszervereket is) számára az iSeries szerver CD-ROM meghajtójának elérését. Hasonlóan, a QFileSvr.400 fájlrendszer lehetővé teszi az alkalmazásoknak a távoli iSeries szerverek integrált fájlrendszer adatainak elérését. A QLANSrv fájlrendszer az Integrated xSeries Server for iSeries szerveren és a hálózat többi szerverén tárolt fájlokhoz biztosít hozzáférést.

Minden egyes fájlrendszer biztonsági megközelítése a fájlrendszer által biztosított adatoktól függ. A QOPT fájlrendszer például nem biztosít objektumszintű biztonságot, mivel nincs olyan technológia, ami lehetővé tenné jogosultsági információk CD-ROM adathordozóra írását. A QFileSvr.400 fájlrendszer hozzáférés felügyelete a távoli rendszeren történik (ahol a fájlok fizikai tárolása és kezelése folyik). A QLANSrv és hasonló fájlrendszerek esetében a hozzáférés felügyeletet az Integrated xSeries Server for iSeries biztosítja. A különféle biztonsági modellek ellenére több fájlrendszer is támogatja a hozzáférés felügyelet konzisztens kezelését az integrált fájlrendszer parancsok, például a Jogosultság módosítása (CHGAUT) és a Tulajdonos módosítása (CHGOWN) parancs segítségével.

Az alábbiakban felsorolunk néhány tippet az integrált fájlrendszer biztonsággal kapcsolatban. Az integrált fájlrendszer kialakítása a POSIX szabványok lehető megközelítésének igényével került kialakításra. Ez néha érdekes viselkedést eredményez az iSeries jogosultságok és a POSIX jogosultságok ″keveredésekor″:

1. Ne szüntesse meg a felhasználók magánjogosultságait az általuk birtokolt katalógusokra vonatkozóan, még akkor sem, ha a felhasználó nyilvános jogosultságon, csoport

jogosultságon vagy jogosultsági listán keresztül rendelkezik jogosultsággal a katalógushoz. Az iSeries szerver biztonsági modelljében a könyvtárak és mappák kezelésekor a tulajdonos magánjogosultságának eltávolítása csökkenti a felhasználói profilban tárolt jogosultsági információk mennyiségét, és nincs hatással a többi műveletre. Viszont a katalógus jogosultságok öröklésének POSIX szabványos módja szerint az újonnan létrehozott katalógusok tulajdonosa ugyanazokkal az objektum jogosultságokkal rendelkezik a katalógushoz, mint amellyel a szülőkatalógus tulajdonosa rendelkezik a szülőkatalógushoz, még akkor is, ha az újonnan létrehozott katalógus tulajdonosa rendelkezik más magánjogosultságokkal a szülőkatalógushoz. Ez elsőre talán egy kicsit bonyolultnak hangzik, ezért lássunk egy példát: a USERA birtokolja a /DIRA katalógust, de a USERA magánjogosultságait eltávolították. A USERB magánjogosultsággal rendelkezik a /DIRA katalógushoz. A USERB létrehozza a /DIRA/DIRB katalógust. Mivel USERA nem rendelkezik objektum jogosultságokkal a /DIRA katalógushoz, a USERB sem fog objektum jogosultságokat kapni a /DIRA/DIRB katalógushoz. A USERB nem fogja tudni törölni vagy átnevezni a /DIRA/DIRB katalógust az objektum jogosultságainak beállításáig. Ez abban az esetben is szerephez jut, amikor az open() API O_INHERITMODE jelzőjének beállított állapotában hoznak létre fájlokat. Ha a USERB egy /DIRA/FILEB fájlt hozott volna létre, akkor sem objektum jogosultságokkal, sem adat jogosultságokkal nem rendelkezne hozzá. Még írni sem tudná az új fájlt.

2. A legtöbb fizikai fájlrendszer nem tartja tiszteletben az átvett jogosultságokat. Ebbe a gyökér (/), a QOpenSys, a QDLS és a felhasználói fájlrendszerek tartoznak bele.
3. Az objektumok tulajdonosa mindig az azokat létrehozó felhasználói profil, még akkor is, ha a felhasználói profil OWNER mezőjének értéke *GRPPRF.
4. A legtöbb fájlrendszer művelethez *RX adatjogosultság szükséges az elérési út minden összetevőjéhez, beleértve ebbe a gyökér (/) katalógust is. Jogosultsági problémák esetén győződjön meg róla, hogy a felhasználónak a gyökér katalógusra vonatkozó jogosultságai rendben vannak.
5. Az aktuális munkakatalógus megjelenítése vagy lekérdezése (DSPCURDIR, getcwd(), stb.) *RX adatjogosultságot igényel az elérési út valamennyi összetevőjéhez. Az aktuális munkakatalógus módosításához (CD, chdir(), stb.) azonban csak *X adatjogosultság szükséges minden összetevőhöz. Ennek megfelelően elképzelhető olyan eset, hogy a felhasználó be tud váltani egy adott munkakatalógusba, de annak tartalmát már nem tudja megjeleníteni.
6. A COPY parancs szándéka az objektumok többszörözése. Az új fájl jogosultságai a tulajdonost kivéve meg fognak egyezni az eredetivel. A CPYTOSTMF parancs viszont egyszerűen adatok másolására szolgál. Ilyenkor az új fájl jogosultsági beállításait a felhasználó nem tudja kontrollálni. A létrehozó/tulajdonos *RWX adatjogosultsággal fog rendelkezni, a csoport- és nyilvános jogosultság viszont *EXCLUDE lesz. A felhasználónak más módot kell használnia (CHGAUT, chmod(), stb.) a kívánt jogosultságok hozzárendelésére.
7. A felhasználónak az objektumokra vonatkozó jogosultsági információk lekérdezéséhez *OBJMGT objektum jogosultsággal kell rendelkeznie az objektumhoz, vagy az objektum tulajdonosának kell lennie. Ez néha váratlan problémákat okozhat, például a COPY parancsnál, amelynek a célobjektum jogosultságainak beállításához le kell kérdeznie a forrásobjektum jogosultsági információit.
8. Egy objektum tulajdonosának vagy csoportjának módosításakor a felhasználónak nemcsak rendelkeznie kell az objektumra vonatkozó megfelelő jogosultsággal, de rendelkeznie kell *ADD adatjogosultsággal is az új tulajdonos/csoport felhasználói profiljához, illetve *DELETE adatjogosultsággal a régi tulajdonos/csoport profilhoz. Ezek az adatjogosultságok nem kapcsolódnak a fájlrendszer adatjogosultságaihoz. Ezen adatjogosultságok a DSPOBJAUT paranccsal jeleníthetők meg, és az EDTOBJAUT paranccsal módosíthatók. Ebbe a problémába lehet például ütközni a COPY parancs használatakor az új objektum csoportazonosítójának beállításakor.

9. A MOV parancs igencsak hajlamos a különféle rejtélyes jogosultsági hibákra, különösen ha az áthelyezés két fizikai fájlrendszer között történik, vagy adatátalakítással jár együtt. Ezekben az esetekben az áthelyezés valójában egy másolás és törlési művelet lesz. Ennek megfelelően a MOV parancsra a rá egyébként is érvényes megfontolások mellett vonatkoznak a COPY parancsnál (a 7. és 8. pontban) már említett jogosultsági szempontok, illetve az RMVLNK parancs szempontjai is.

Az alábbi témakörök az említésre méltó fájlrendszerekkel kapcsolatos egyéni szempontokat tartalmazzák. Az iSeries szerver adott fájlrendszereire vonatkozó speciális részleteket a fájlrendszert használó licencprogram dokumentációjából tudhatja meg.

Gyökér (/), QOpenSys és felhasználói fájlrendszerek (UDFS)

Ez a szakasz foglalja össze a gyökér, a QOpenSys és a felhasználói fájlrendszerek (UDFS) biztonsági vonatkozásait.

Jogosultságok működése

A gyökér, a QOpenSys és a felhasználói fájlrendszerek az iSeries, a PC és a UNIX** platformok képességeinek speciális keverékét alkotják mind objektumkezelési, mind biztonsági szempontból. Ha az integrált fájlrendszer parancsokat iSeries szerver szekcióban használja (WRKAUT és CHGAUT), akkor az iSeries szerver szokásos objektum jogosultságainak beállítására van lehetősége. Ez magában foglalja a Spec 1170-kompatíbilis (UNIX típusú operációs rendszereken alkalmazott) *R, *W és *X jogosultságokat is.

Megjegyzés: A gyökér, a QOpenSys és a felhasználói fájlrendszerek működésükben egyenértékűek. A QOpenSys fájlrendszer megkülönbözteti a kis- és nagybetűket. A gyökér fájlrendszer nem. A felhasználói fájlrendszereknél beállítható a kis- és nagybetűk megkülönböztetése. Mivel ezek a fájlrendszerek azonos biztonsági jellemzőkkel rendelkeznek, a soron következő témakörökben feltételezheti, hogy a neveket felcserélhetően használjuk.

Ha a gyökér fájlrendszerhez PC szekcióból csatlakozik adminisztrátorként, akkor beállíthatja a PC által bizonyos hozzáférési típusok korlátozására használt objektum attribútumokat:
- Rendszer
- Rejtett
- Archiválandó
- Írásvédett

Ezek a PC attribútumok az iSeries szerver objektum jogosultsági értékeinek kiegészítései, nem pedig helyettesítői.

Amikor egy felhasználó megkísérli a gyökér fájlrendszer valamely objektumának elérését, akkor az OS/400 az objektumra vonatkozó valamennyi jogosultsági érték és attribútum használatát foganatosítja, függetlenül attól, hogy a felhasználó által használt felhasználói felület alkalmazza-e ezeket. Tegyük fel például, hogy egy objektumnak be van állítva az Írásvédett attribútuma. A PC felhasználók nem tudják törölni az objektumot az iSeries Access felületről. A rögzített funkciós munkaállomást használó iSeries szerver felhasználó szintén nem tudja törölni az objektumot, még akkor sem, ha az iSeries felhasználó történetesen *ALLOBJ speciális jogosultsággal rendelkezik. Mielőtt az objektumot törölni lehetne, egy jogosult felhasználónak egy PC funkció használatával törölnie kell az Írásvédett attribútumot (off). Hasonlóan elképzelhető, hogy egy PC felhasználó nem rendelkezik elegendő OS/400 jogosultságokkal egy objektum PC oldali biztonsági jellemzőinek módosításához.

Az iSeries szervereken futó UNIX jellegű alkalmazások UNIX jellegű alkalmazásprogram illesztőket (API) alkalmaznak a gyökér fájlrendszer adatainak eléréséhez. A UNIX jellegű API-k használatakor az alkalmazások a következő biztonsági információk felismerésére és kezelésére képesek:
- Objektum tulajdonos
- Csoport tulajdonos (az iSeries szerver elsődleges csoport jogosultsága)
- Olvasás (fájlok)
- Írás (tartalom módosítása)
- Végrehajtás (programok futtatása és katalógusok keresése)

A rendszer ezeket az adatjogosultságokat a következőképpen képezi le az iSeries szerver objektum- és adatjogosultságaira:
- Olvasás (*R) = *OBJOPR és *READ
- Írás (*W) = *OBJOPR, *ADD, *UPD és *DLT
- Végrehajtás (*X) = *OBJOPR és *EXECUTE

A UNIX típusú környezetek a többi objektum jogosultságot (*OBJMGT, *OBJEXIST, *OBJALTER és *OBJREF) nem definiálják.

Ettől függetlenül az objektum jogosultságok a gyökér fájlrendszer valamennyi objektumára érvényesülnek. Amikor egy objektum UNIX jellegű API használatának eredményeként jön létre, akkor az objektum örökli a szülőkatalógus jogosultságait, amely a következőket eredményezi:
- Az új objektum tulajdonosa ugyanazokkal az objektum jogosultságokkal fog rendelkezni, mint a szülőkatalógus tulajdonosa.
- Az új objektum elsődleges csoportja ugyanazokkal az objektum jogosultságokkal fog rendelkezni, mint a szülőkatalógus elsődleges csoportja.
- Az új objektum nyilvános felhasználói ugyanazokkal az objektum jogosultságokkal fognak rendelkezni, mint a szülőkatalógus nyilvános felhasználói.

Az új objektum tulajdonosának, elsődleges csoportjának és a nyilvánosságnak az adatjogosultságai az API mód paraméterében adhatók meg. Ha minden objektum jogosultság be van állítva, akkor jutunk el a UNIX környezetekben elvárt jogosultsági viselkedéshez. A legjobb megoldás ezeket bekapcsolva hagyni, kivéve ha nem szeretné a POSIX jellegű viselkedést.

UNIX jellegű alkalmazásprogram illesztőket (API) használó alkalmazások futtatásakor a rendszer valamennyi objektum jogosultságot foganatosít, függetlenül attól, hogy a UNIX jellegű alkalmazások ″látják-e″ ezeket vagy sem. A rendszer például betartatja a jogosultsági listák által megadott jogosultságokat, még akkor is, ha a jogosultsági listák fogalma nem is létezik a UNIX jellegű operációs rendszerekben.

Vegyes alkalmazási környezetben ügyeljen arra, hogy ne végezzen egy környezetben olyan jogosultsági módosításokat, amelyek miatt egy másik környezet alkalmazásai nem fognak működni.

A gyökér (/), a QOpenSys és a felhasználói fájlrendszerek biztonságának kezelése

Az integrált fájlrendszer bevezetésével az iSeries szervereken megjelentek a különféle fájlrendszerekben található objektumok kezelésére szolgáló parancsok is. A parancskészlet biztonság kezelésére használható parancsai a következők:
- Megfigyelés módosítása (CHGAUD)
- Jogosultság módosítása (CHGAUT)
- Tulajdonos módosítása (CHGOWN)
- Elsődleges csoport módosítása (CHGPGP)
- Jogosultság megjelenítése (DSPAUT)

- Jogosultság kezelése (WRKAUT)

A parancsok a fájlrendszer objektum- és adatjogosultságait a következő UNIX jellegű jogosultságkészletekbe rendezik:
***RWX** Olvasás/írás/végrehajtás
***RW** Olvasás/írás
***R** Olvasás
***WX** Írás/végrehajtás
***W** Írás
***X** Végrehajtás

Emellett a biztonság kezeléséhez UNIX jellegű API-k is rendelkezésre állnak.

Gyökér katalógus nyilvános jogosultsága

A rendszer alapértelmezett beállításai szerint a gyökér katalógusra vonatkozó nyilvános jogosultság *ALL (minden objektum jogosultság és minden adatjogosultság). Ez a beállítás rugalmasságot és kompatibilitást nyújt mind a UNIX jellegű alkalmazások, mind az iSeries szerver általános felhasználói által elvártaknak. Egy parancssort használó iSeries felhasználó egy új könyvtárat a QSYS.LIB fájlrendszerben egyszerűen a CRTLIB paranccsal hozhat létre. A tipikus iSeries szerverek jogosultságai ezt általában lehetővé teszik. Hasonlóan, a gyökér fájlrendszer alapértelmezett beállításai mellett az általános felhasználók létrehozhatnak új katalógusokat a gyökér fájlrendszerben (amint az a személyi számítógépeken is lehetséges).

A biztonsági adminisztrátornak ki kell oktatnia a felhasználókat az általuk létrehozott objektumok megfelelő védelméről. Amikor egy felhasználó létrehoz egy könyvtárat, akkor a könyvtár alapértelmezett *CHANGE nyilvános jogosultsága valószínűleg nem megfelelő. A felhasználónak a jogosultságot vagy *USE vagy *EXCLUDE értékre kell állítania a könyvtár tartalmától függően.

Ha a felhasználóknak új katalógusokat kell tudniuk létrehozni a gyökér (/), a QOpenSys vagy a felhasználói fájlrendszerekben, akkor több biztonsági lehetősége is van:

- El kell magyarázni a felhasználóknak az alapértelmezett jogosultságok módosítását az új katalógusok létrehozásakor. Az alapértelmezés a közvetlen szülőkatalógus jogosultságainak öröklése. A gyökér katalógus alatt létrehozott új katalógusok nyilvános jogosultsága *ALL lesz.
- Létrehozhat egy ″elsődleges″ alkatalógust a gyökér katalógus alatt. Az elsődleges katalógus nyilvános jogosultságát állítsa be egy megfelelő értékre. Ezután utasítsa a felhasználókat, hogy az új személyes katalógusokat ebben az elsődleges alkatalógusban hozzák létre. Az újonnan létrehozott katalógusok az elsődleges alkatalógus jogosultságait fogják örökölni.
- Megfontolhatja a gyökér katalógus nyilvános jogosultságának módosítását oly módon, hogy megakadályozza a felhasználókat abban, hogy objektumokat hozzanak benne létre. (Távolítsa el a *W, *OBJEXIST, *OBJALTER, *OBJREF és *OBJMGT jogosultságokat.) Ebben az esetben azonban át kell gondolni, hogy a módosítás milyen hatással lesz az alkalmazásokra. Elképzelhetők például olyan UNIX jellegű alkalmazások, amelyek feltételezik, hogy törölhetik a gyökér katalógus objektumait.

Magánjogosultságok kinyomtatása (PRTPVTAUT) parancs

A Magánjogosultságok kinyomtatása (PRTPVTAUT) paranccsal nyomtathatja ki a megadott könyvtárban, katalógusban vagy mappában található adott típusú objektumokra vonatkozó magánjogosultságok listáját. A jelentésben a megadott típusú objektumok, illetve a hozzájuk jogosultságokkal rendelkező felhasználók szerepelnek. Ez az egyik módszer az objektumokra vonatkozó jogosultságok különböző forrásainak ellenőrzésére.

A parancs a kijelölt objektumokról háromféle jelentést készíthet. Az első jelentésben (teljes jelentés) az összes kijelölt objektumra vonatkozó valamennyi magánjogosultság megtalálható. A második jelentés (változási jelentés) a kijelölt objektumokra vonatkozó magánjogosultságok eltéréseit tartalmazza a PRTPVTAUT parancsnak az adott objektumokra vonatkozó legutóbbi futtatásához képest. A változási jelentésben a megadott típusú új objektumok, a meglévő objektumok új jogosultságai, illetve a meglévő jogosultságokban történt változások szerepelnek. Ha a PRTPVTAUT parancs még nem futott le a megadott könyvtár, mappa vagy katalógus kijelölt objektumain, akkor nem készül változási jelentés. Ha a parancs már futott korábban, de az objektumok jogosultságaiban nem történt változás, akkor a változási jelentés nyomtatásra kerül ugyan, de nem tartalmaz objektumokat.

A harmadik jelentési típus (törlési jelentés) a PRTPVTAUT parancs legutóbbi futtatásához képest törölt magánjogosultságokat tartalmazza. A törlési jelentés a törölt objektumokat, illetve azokat a felhasználókat tartalmazza, amelyeknek az objektumokra vonatkozó magánjogosultságát visszavonták. Ha a PRTPVTAUT parancs a korábbiakban nem futott le, akkor nem készül törlési jelentés. Ha a parancs már futott korábban, de nem történtek objektum vagy jogosultság törlések, akkor a törlési jelentés nyomtatásra kerül ugyan, de nem tartalmaz objektumokat.

Korlátozás: A parancs használatához *ALLOBJ speciális jogosultság szükséges.

Példák:

A következő parancs a PAYROLLLIB összes objektumára vonatkozóan létrehozza a teljes, a változási és a törlési jelentéseket:

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

A következő parancs a garry nevű katalógus folyamfájl objektumaira vonatkozóan hozza létre a teljes, a változási és a törlési jelentéseket:

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

A következő parancs a garry nevű katalógussal kezdődő hierarchia folyamfájl objektumaira vonatkozóan hozza létre a teljes, a változási és a törlési jelentéseket:

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

Nyilvános jogosultsággal rendelkező objektumok kinyomtatása (PRTPUBAUT) parancs

A Nyilvános jogosultsággal rendelkező objektumok kinyomtatása (PRTPUBAUT) parancs lehetővé teszi egy jelentés kinyomtatását azon megadott objektumokról, amelyek nyilvános jogosultsága nem *EXCLUDE. *PGM objektumok esetén a jelentésben csak azok az *EXCLUDE-tól eltérő nyilvános jogosultsággal rendelkező programok fognak szerepelni, amelyeket egy felhasználó meghívhat (vagyis a program a felhasználói tartományban található, vagy a rendszer biztonsági szintje 30 vagy alacsonyabb). Ily módon kereshetők meg a rendszeren az olyan objektumok, amelyekhez minden felhasználó rendelkezik jogosultsággal.

A parancs kétféle jelentést készíthet. Az első jelentésben (teljes jelentés) az összes olyan megadott objektum szerepel, amelynek nyilvános jogosultsága nem *EXCLUDE. A második jelentés (változási jelentés) azokat az objektumokat tartalmazza, amelyek nem léteztek a PRTPUBAUT parancs előző futtatása alkalmával, vagy amelyek *EXCLUDE jogosultsága megszűnt a parancs előző futtatása óta. Ha a PRTPUBAUT parancs még nem futott le a megadott könyvtár, mappa vagy katalógus kijelölt objektumain, akkor nem készül változási jelentés. Ha a parancs már futott korábban, de nincsenek olyan objektumok, amelyek

*EXCLUDE nyilvános jogosultsága megszűnt volna a legutóbbi futtatás óta, akkor a változási jelentés nyomtatásra kerül ugyan, de nem tartalmaz objektumokat.

Korlátozás: A parancs használatához *ALLOBJ speciális jogosultság szükséges.

Példák:

A következő parancs a GARRY könyvtár azon objektumairól készít teljes és változási jelentést, amelyek nyilvános jogosultsága nem *EXCLUDE:

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

A következő parancs a GARRY nevű katalógussal kezdődő hierarchia nem *EXCLUDE nyilvános jogosultsággal rendelkező folyamfájl objektumaira vonatkozóan hozza létre a teljes, a változási és a törlési jelentéseket:

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

QSYS.LIB fájlrendszerre vonatkozó hozzáférés korlátozása

Mivel a gyökér fájlrendszer összefoglaló fájlrendszer, a QSYS.LIB fájlrendszer a gyökér katalógus alkatalógusaként jelenik meg. Ennek megfelelően az iSeries szerverhez hozzáférő bármely PC felhasználó hozzáfér az iSeries szerver könyvtáraihoz (a QSYS.LIB fájlrendszerhez) a szokásos PC parancsokkal és műveletekkel. Lehetősége van például egy QSYS.LIB objektum (például kritikus adatokat tartalmazó fájlok) behúzására a Lomtárba.

A “Gyökér (/), QOpenSys és felhasználói fájlrendszerek (UDFS)” oldalszám: 97 szakaszban leírtaknak megfelelően a rendszer az adott felületen vett láthatóságra való tekintet nélkül minden objektum jogosultságot betartat. Ennek megfelelően a felhasználók nem törölhetnek egy objektumot, csak akkor, ha rendelkeznek hozzá *OBJEXIST jogosultsággal. Ha azonban az iSeries menü hozzáférési biztonságra alapuló modellt alkalmaz objektum biztonság helyett, akkor a PC felhasználó szabadon barangolhat a QSYS.LIB fájlrendszerben, és találhat törölhető objektumokat.

A rendszer felhasználási körének és a biztosított hozzáférési módszerek bővülésével hamar rájöhet, hogy a menü hozzáférési biztonság nem elegendő. A menü hozzáférés felügyelet objektum biztonsággal való kiegészítését a 5. fejezet, “Információs tulajdon védelme objektum jogosultságokkal”, oldalszám: 45 szakasz tárgyalja. Az iSeries szerverek mindazonáltal biztosítanak egy egyszerű módszert a QSYS.LIB fájlrendszernek a gyökér fájlrendszer katalógusszerkezete felőli elérésének korlátozására. A QPWFSERVER jogosultsági listával felügyelheti, hogy mely felhasználók férhetnek hozzá a QSYS.LIB fájlrendszerhez a gyökér katalógus felől.

Ha egy felhasználó jogosultsága a QPWFSERVER jogosultsági listához *EXCLUDE, akkor a felhasználó nem léphet be a QSYS.LIB katalógusba a gyökér katalógusszerkezetből. *USE jogosultság esetén a felhasználó beléphet a katalógusba. Miután a felhasználó rendelkezik a katalógusba való belépés jogával, a QSYS.LIB fájlrendszer objektumain végrehajtani próbált tevékenységekre a szokásos objektum jogosultság vonatkozik. Más szavakkal a QPWFSERVER jogosultsági listára vonatkozó jogosultság a teljes QSYS.LIB fájlrendszerre nyíló ajtóként működik. Az *EXCLUDE jogosultságú felhasználók számára az ajtó zárva van. A *USE (vagy ennél magasabb) jogosultság birtokában lévő felhasználók számára az ajtó nyitva áll.

A legtöbb esetben a felhasználóknak nincs szükségük a katalógus felületre a QSYS.LIB fájlrendszer objektumainak eléréséhez. Éppen ezért valószínűleg érdemes a QPWFSERVER jogosultsági lista nyilvános jogosultságát *EXCLUDE-ra állítani. Ne feledje, hogy a jogosultsági listára vonatkozó jogosultság a QSYS.LIB fájlrendszer valamennyi könyvtárára vonatkozóan nyitja ki vagy zárja be az ajtót, és ebbe a felhasználói könyvtárak is

beletartoznak. Ha vannak olyan felhasználók, akiknek a kizárás gondot okoz, akkor az igényeiket egyéni alapon kell kiértékelni. Indokolt igény esetén kifejezetten jogosítsa fel az egyéni felhasználót a jogosultsági listára. Ettől függetlenül viszont győződjön meg róla, hogy a felhasználó megfelelő jogosultságokkal bír a QSYS.LIB fájlrendszer objektumait illetőleg. Ellenkező esetben elképzelhető, hogy a felhasználó véletlenül töröl néhány objektumot vagy egy teljes könyvtárat.

Megjegyzések:

1. A rendszer alapértelmezett beállításai szerint a QPWFSERVER jogosultsági lista nyilvános jogosultsága *USE.
2. Ha egy egyéni felhasználót kifejezetten feljogosít, akkor a jogosultsági lista csak az iSeries Access fájl kiszolgálásra, a hálózati szerver fájl kiszolgálásra és az iSeries szerverek közötti fájl kiszolgálásra vonatkozik. Nem akadályozza meg ugyanezen katalógusok FTP, ODBC vagy más módszerrel végzett elérését.

Védett katalógusok

A gyökér fájlrendszeren belül található objektumok elérésekor az objektumhoz vezető teljes elérési út végigolvasásra kerül. A katalógusok kereséséhez *X (*OBJOPR és *EXECUTE) jogosultság szükséges a katalógusra vonatkozóan. Tegyük fel például, hogy a következő objektumot szeretné elérni:

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

Ebben az esetben *X jogosultsággal kell rendelkeznie a companya katalógushoz és a customers katalógushoz is.

A gyökér fájlrendszerben lehetőség van objektumokra mutató szimbolikus hivatkozások létrehozására. A szimbolikus hivatkozások tulajdonképpen elérési út álnevek. Ezek általában rövidebbek a teljes elérési útnál, és könnyebb is őket megjegyezni. A szimbolikus hivatkozások viszont nem hoznak létre eltérő fizikai elérési útvonalat az objektumhoz. A felhasználónak továbbra is szüksége van *X jogosultságra az objektumhoz vezető fizikai elérési út valamennyi katalógusához és alkatalógusához.

A gyökér fájlrendszer objektumainál a katalógus biztonság ugyanúgy használható, mint a könyvtár biztonság a QSYS.LIB fájlrendszerben. Beállítható például *EXCLUDE jogosultság az olyan katalógusoknál, amelyek objektumaihoz a nyilvános felhasználók nem férhetnek hozzá.

Új objektumok biztonsága

Amikor egy új objektumot hoz létre a gyökér fájlrendszerben, akkor ennek jogosultságait a létrehozáshoz használt felhasználói felület dönti el. Ha például a CRTDIR parancsot és annak alapértelmezéseit használja, akkor az új katalógus örökli a szülőkatalógusának valamennyi jogosultsági jellemzőjét, beleértve a magánjogosultságokat, elsődleges csoport jogosultságokat és jogosultsági lista társítást. Az alábbi szakaszok írják le a jogosultságok meghatározását a különféle felületek alapján.

A jogosultságok a közvetlen szülőkatalógustól származnak, nem a fa magasabb katalógusaitól. Ennek megfelelően a biztonsági adminisztrátornak a hierarchiában lévő katalógusokhoz rendelt jogosultságokat a következő két szemszögből kell tekintenie:

- Ahogyan a jogosultság a fában található objektumokat érinti (a könyvtár jogosultságokhoz hasonlóan).
- Ahogyan a jogosultság az újonnan létrejött objektumokat érinti (hasonlóan a könyvtárak CRTAUT értékéhez).

Javaslat: Az integrált fájlrendszerben tevékenykedő felhasználóknak érdemes lehet kiosztani egy saját katalógust (például /home/usrxxx), amelynek biztonsága megfelelő módon beállítható (például PUBLIC *EXCLUDE). A felhasználók által a saját katalógusukban létrehozott további katalógusok öröklik ezeket a jogosultságokat.

A különféle felületeken alkalmazott jogosultság öröklések a következők:

Katalógus létrehozása parancs használata

Amikor egy új alkatalógust a CRTDIR paranccsal hoz létre, akkor a jogosultságok meghatározására két lehetőség áll rendelkezésére:

- Megadhatja a nyilvános jogosultságot (adatjogosultság, nyilvános jogosultság vagy mindkettő).
- Megadhatja az *INDIR értéket az adatjogosultságnak, objektum jogosultságnak vagy mindkettőnek. Ha az adatjogosultságnak és az objektum jogosultságnak is az *INDIR értéket adja meg, akkor a rendszer az új objektum jogosultsági információi számára pontos másolatot készít a szülőkatalógus jogosultsági információiról, beleértve a jogosultsági listát, az elsődleges csoportot, a nyilvános jogosultságot és a magánjogosultságokat. (A rendszer nem másolja le a QSYS és QSECOFR profilnak az objektumon birtokolt magánjogosultságait.)

Katalógus létrehozása API felhasználásával

Amikor egy katalógust az mkdir() API segítségével hoz létre, akkor megadja a tulajdonos, az elsődleges csoport és a nyilvánosság adatjogosultságait (az *R, *W és *X jogosultsági leképezéssel). A rendszer a szülőkatalógus információi alapján állítja be a tulajdonos, az elsődleges csoport és a nyilvánosság objektum jogosultságait.

Mivel a UNIX jellegű operációs rendszerek nem ismerik az objektum jogosultságok koncepcióját, az mkdir() API nem támogatja objektum jogosultságok meghatározását. Eltérő objektum jogosultságok meghatározásához használja az iSeries szerver CHGAUT parancsát. Bizonyos objektum jogosultságok eltávolítása esetén viszont elképzelhető, hogy a UNIX jellegű alkalmazás nem a várakozásnak megfelelően fog működni.

Folyamfájlok létrehozása az open() vagy creat() API felhasználásával

Amikor a creat() API segítségével hoz létre egy folyamfájlt, akkor megadhatja a tulajdonos, az elsődleges csoport és a nyilvánosság adatjogosultságait (a UNIX jellegű *R, *W és *X jogosultságokkal). A rendszer a szülőkatalógus információi alapján állítja be a tulajdonos, az elsődleges csoport és a nyilvánosság objektum jogosultságait.

Ezeket a jogosultságokat adhatja meg abban az esetben is, ha a folyamfájlt az open() API segítségével hozza létre. Ennek alternatívájaként az open() API használatakor megadhatja, hogy az objektum az összes jogosultságot a szülőkatalógustól örökölje. Ezt öröklési módnak nevezzük. Öröklési mód meghatározásakor a rendszer a szülőkatalógus jogosultságait teljes egészében lemásolja, beleértve a jogosultsági listát, az elsődleges csoportot, a nyilvános jogosultságot és a magánjogosultságokat. Ez hasonló a CRTDIR parancs *INDIR paraméterének használatához.

Objektumok létrehozása PC felületekről

Ha egy objektumot PC alkalmazás segítségével hoz létre a gyökér fájlrendszerben, akkor a rendszer automatikusan minden jogosultságot örökít a szülőkatalógustól. Ebbe beletartozik a jogosultsági lista, az elsődleges csoport, a nyilvános jogosultság és a magánjogosultságok. A PC alkalmazások nem rendelkeznek a jogosultságok meghatározásának megfelelő mechanizmussal az objektumok létrehozásához.

QFileSvr.400 fájlrendszer

A QFileSvr.400 fájlrendszer segítségével az egyik iSeries rendszer felhasználója hozzáférhet más csatlakozó iSeries rendszerek adataihoz. A felhasználónak ehhez egy Client Accesshez hasonló felület áll rendelkezésére. A távoli iSeries szerver katalógusként jelenik meg, amelyben minden fájlrendszer egy-egy alkatalógusnak felel meg.

Amikor a felhasználó ily módon próbál csatlakozni a távoli rendszerhez, akkor a helyi rendszer elküldi a felhasználó profilját és titkosított jelszavát a távoli rendszerre. A távoli rendszeren léteznie kell ugyanennek a felhasználói profilnak és jelszónak, ellenkező esetben a távoli rendszer visszautasítja a kérést.

Ha a távoli rendszer elfogadja a kérést, akkor a felhasználó a távoli rendszer szempontjából úgy fog kinézni, mind bármely más Client Access felhasználó. A felhasználó tevékenységeire is ugyanezek a jogosultság ellenőrzési szabályok vonatkoznak.

A biztonsági adminisztrátornak oda kell figyelnie arra, hogy a QFileSvr.400 fájlrendszer egy újabb potenciális ajtót jelent a rendszeren. Nem feltételezheti, hogy a távoli felhasználókat interaktív bejelentkezésre korlátozza a terminál átjelentkezéssel. Ha a szerveren fut a QSERVER alrendszer, és a szerver csatlakozik másik iSeries rendszerhez, akkor a távoli felhasználók ugyanúgy csatlakozhatnak a szerverre, mint a helyi számítógépek Client Access felhasználói. Több mint valószínű, hogy a rendszer rendelkezik olyan kapcsolattal, amely a QSERVER alrendszer futását igényli. Éppen ezért ez ismét egy jó indok a megfelelő objektum jogosultsági séma kialakítására.

Hálózati fájlrendszer

A Hálózati fájlrendszer (NFS) NFS támogatással rendelkező rendszerek hozzáférését biztosíthatja. Az NFS a hálózati rendszerek felhasználói közötti információmegosztás ipari szabvány módszere. A legtöbb nagyobb operációs rendszer (beleértve a PC operációs rendszereket is) biztosít NFS támogatást. UNIX rendszerek esetén az NFS az adatok elérésének elsődleges módszere. Az iSeries szerverek NFS kliensként és NFS szerverként is működhetnek.

Az NFS szerverként működő iSeries rendszerek biztonsági adminisztrátorának meg kell ismernie az NFS biztonsági jellemzőit. Néhány javaslat és szempont:

- Az NFS szerver funkciót kifejezetten el kell indítani az STRNFSSVR paranccsal. A parancs használatára vonatkozó jogosultságot érdemes felügyelni.
- A katalógusok vagy objektumok exportálással tehetők elérhetővé az NFS kliensek számára. Ez jól kézben tartható felügyeleti módszert biztosít a hálózat NFS kliensei számára elérhetővé tett rendszererőforrások felett.
- Az exportálásnál megadható, hogy milyen kliensek férhetnek hozzá az objektumokhoz. A kliensek rendszernév vagy IP cím alapján azonosíthatók. Kliensek lehetnek személyi számítógépek, iSeries szerverek vagy UNIX rendszerek. Az NFS szóhasználatában a klienseket (IP cím) számítógépnek hívjuk.
- Az exportálásnál minden egyes számítógép vonatkozásában megadhatja, hogy az az exportált katalógushoz vagy objektumhoz csak olvasási vagy olvasás/írási hozzáféréssel rendelkezik. A legtöbb esetben valószínűleg a csak olvasható hozzáférés a helyénvaló.
- Az NFS nem biztosít jelszóvédelmet. Kialakítása a megbízható hálózatok által támasztott igények szem előtt tartásával történt. Amikor egy felhasználó hozzáférést igényel, akkor a szerver megkapja a felhasználó uid számát. Néhány uid szempont:
  - Az iSeries szerver megpróbál találni egy azonos uid értékkel rendelkező felhasználói profilt. Ha talál egyező uid értéket, akkor az adott felhasználói profil meghatalmazásait

használja. A meghatalmazás a felhasználók jogosultságainak leírására használt NFS kifejezés. Ez hasonlít a más iSeries szerver alkalmazások által végzett profilcseréhez.

– Katalógus vagy objektum exportálásakor megadhatja, hogy engedélyezi-e root jogosultságú profilok számára a hozzáférést. Az iSeries rendszer NFS szervere a root jogosultságot az *ALLOBJ speciális jogosultságra képezi le. Ha nem engedélyezi a root hozzáférést, és egy NFS felhasználó uid értéke *ALLOBJ speciális jogosultsággal rendelkező felhasználói profilra képezhető le, akkor a felhasználónak az adott profil alatti hozzáférése nem lehetséges. Ehelyett, az anonim hozzáférés engedélyezésekor a kérő az anonim profilra kerül leképezésre.

– Katalógus vagy objektum exportálásakor megadhatja, hogy engedélyezi-e az anonim kéréseket. Az anonim kérések olyan uid értéket tartalmazó kérések, amelyek nem egyeznek meg a rendszer egyik uid értékével sem. Ha úgy dönt, hogy engedélyezi az anonim kéréseket, akkor a rendszer az anonim felhasználókat az IBM által szállított QNFSANON felhasználói profilra képezi le. Ez a felhasználói profil semmilyen speciális jogosultsággal és kifejezett jogosultsággal nem rendelkezik. (Az exportban igény szerint megadhat másik felhasználói profilt is az anonim kérésekhez.)

- Ha az iSeries szerver NFS (vagy uid értékektől függő UNIX) hálózat tagja, akkor az automatikus hozzárendelés helyett valószínűleg saját magának kell kezelnie az uid értékeket. Az uid értékeket össze kell hangolni a hálózat többi rendszerével.

  A hálózat többi rendszerével való kompatibilitás érdekében elképzelhető, hogy (még az IBM által szállított profilok esetén is) módosítani kell az uid értékeket. Rendelkezésre áll egy program, amely leegyszerűsíti a felhasználói profilok uid értékének módosítását. (Egy felhasználói profil uid értékének módosításakor módosítani kell a profil által a gyökér vagy a QOpenSrv katalógusban birtokolt objektumok uid értékét is.) A QSYCHGID program automatikusan lecseréli az uid értéket a felhasználói profilban és a birtokolt objektumokban is. A program használatáról további információkat az *iSeries System API Reference* című kiadványban talál.

12. fejezet Biztonságos APPC kommunikáció

Amikor a rendszer más rendszerekkel együtt hálózathoz csatlakozik, akkor a rendszeren új ajtók és ablakok válnak elérhetővé. A biztonsági adminisztrátornak tisztában kell lennie a rendszer bejáratait az APPC környezetben felügyelő lehetőségekkel.

Az APPC egy módszer a számítógépek, például személyi számítógépek egymással folytatott kommunikációjára. Az APPC kommunikációt a terminál átjelentkezés, az osztott adatkezelés és az iSeries Access for Windows funkciók használják.

Az alábbi témakörök az APPC kommunikáció működésére vonatkozó alapvető információkat, illetve a biztonságos beállításához szükséges tudnivalókat ismertetik. A kiadvány az APPC konfigurációknak elsősorban a biztonsággal kapcsolatos elemeire összpontosít. A példa adott helyzetre alkalmazásához együtt kell működnie a kommunikációs hálózat fenntartóival, illetve bizonyos esetekben az alkalmazás szállítójával. Az itt megadott információkat alapként használhatja fel az APPC funkció biztonsági kérdéseinek és lehetőségeinek megértéséhez.

A biztonság sohasem “ingyenes”. A hálózati biztonság megkönnyítését célzó javaslatok általában megnehezítik a hálózat felügyeletét. Ez a témakör nem hangsúlyozza például az APPN (Advanced Peer-to-Peer Networking) használatát, mivel a biztonsági szempontok könnyebben megérthetők és kezelhetők az APPN nélkül. Az APPN nélkül viszont a hálózati adminisztrátornak saját kezűleg kell létrehoznia azokat a konfigurációs információkat, amelyeket az APPN automatikusan létrehoz.

A személyi számítógépek is kommunikálnak

A személyi számítógépek és az iSeries szerverek közötti kapcsolat megteremtésére szolgáló módszerek nagy része függ a kommunikációtól (például APPC vagy TCP/IP). A soron következő szakaszok olvasásakor ne feledje számításba venni azt, hogy a biztonsági kérdések a rendszerekre és a személyi számítógépekre is vonatkoznak. A hálózat védelmének tervezésekor győződjön meg róla, hogy a kialakított intézkedések nem érintik hátrányosan a rendszerhez csatlakozó személyi számítógépeket.

APPC szakkifejezések

Az APPC képessé teszi a felhasználókat arra, hogy feladatokat végezzenek el más rendszereken. A kérés származási helyéül szolgáló rendszerek megnevezése a következők bármelyike lehet:

- **Forrásrendszer**
- **Helyi rendszer**
- **Kliens**

A kérést fogadó rendszerek elnevezései a következők lehetnek:

- **Célrendszer**
- **Távoli rendszer**
- **Szerver**

APPC kommunikáció alapelemei

A biztonsági adminisztrátor szemszögéből a következőknek kell megtörténniük, mielőtt egy rendszer (SYSTEMA) valamelyik felhasználója érdemi munkát tudna végezni egy másik rendszeren (SYSTEMB):

- A forrásrendszernek (SYSTEMA) biztosítania kell egy útvonalat a célrendszerhez (SYSTEMB). Ezt az útvonalat nevezzük **APPC szekciónak**.
- A célrendszernek azonosítania kell a felhasználót, és társítania kell hozzá egy felhasználói profilt. A célrendszernek támogatnia kell a forrásrendszer által használt titkosítási algoritmust (további információk: “Jelszó szintek” oldalszám: 16).
- A célrendszernek el kell indítania egy megfelelő környezettel (jobkezelési értékekkel) rendelkező jobot a felhasználó számára.

Az alábbi szakaszok ezeket az elemeket, illetve ezeknek a biztonsághoz való viszonyát veszik sorra. Elsősorban a célrendszer biztonsági adminisztrátorának feladata annak biztosítása, hogy az APPC felhasználók ne sértsék meg a biztonságot. Ha azonban a két rendszer biztonsági adminisztrátora együttműködik, akkor az APPC biztonság kezelésének feladata sokkal egyszerűbbé válik.

Példa: Alapvető APPC szekció

APPC környezetben amikor egy felhasználó vagy alkalmazás hozzáférést igényel egy másik rendszerhez, akkor a két rendszer felépít egy szekciót. A szekció kialakításához a rendszereknek két megfelelő APPC eszközleírást kell összekapcsolniuk. A SYSTEMA eszközleírásában található Távoli hely neve (RMTLOCNAME) paraméternek meg kell egyeznie a SYSTEMB eszközleírásának Helyi hely neve (LCLLOCNAME) paraméterével és viszont.

Az APPC szekció sikeres kialakításához a SYSTEMA és SYSTEMB rendszerek APPC eszközleírásaiban a hely jelszavaknak meg kell egyezniük. Vagy mindkét érték legyen *NONE, vagy azonos értéket kell megadniuk.

Ha a jelszavak értéke nem *NONE, akkor ezek tárolásra kerülnek, és titkosított formában kerülnek elküldésre a másik rendszernek. Ha a jelszavak megegyeznek, akkor a két rendszer kialakítja a szekciót. Ha a jelszavak nem egyeznek meg, akkor a távoli rendszer visszautasítja a felhasználó kérését. Amikor a rendszerek a szekció kialakításához kicserélik a hely jelszavakat, akkor ezt **védett kötésnek** hívjuk.

Megjegyzés: Nem minden számítógéprendszer támogatja a védett kötés funkciót.

APPC szekciók korlátozása

A forrásrendszer biztonsági adminisztrátorának kell meghatároznia objektum jogosultságok segítségével azon felhasználókat, kik jogosultak más rendszerek elérésére. Az APPC eszközleírások nyilvános jogosultságát állítsa *EXCLUDE-ra, és adjon *CHANGE jogosultságot az egyes felhasználóknak. A QLMTSECOFR rendszerváltozóval akadályozhatja meg az *ALLOBJ speciális jogosultsággal rendelkező felhasználóknak az APPC kommunikáció használatát.

A célrendszer biztonsági adminisztrátorának szintén az APPC eszközökre vonatkozó jogosultságokkal kell megakadályoznia, hogy jogosulatlan felhasználók APPC szekciókat indítsanak a rendszeren. Meg kell érteni viszont, hogy milyen felhasználói azonosító fogja megkísérelni az APPC eszközleírás elérését. Az “APPC felhasználói hozzáférés a célrendszerhez” oldalszám: 109 szakasz írja le, hogyan társít az iSeries szerver egy felhasználói azonosítót az APPC szekció kialakítási kéréshez.

Megjegyzés: A Nyilvános jogosultsággal rendelkező objektumok kinyomtatása (PRTPUBAUT *DEVD) és a Magánjogosultságok kinyomtatása (PRTPVTAUT *DEVD) parancsokkal határozhatja meg, hogy ki rendelkezik jogosultsággal a rendszer eszközleírásaihoz.

APPN használata esetén automatikusan létrejön egy új APPC eszköz, amennyiben a rendszer által kiválasztott útvonalhoz nincs létező eszköz. Az APPC eszközök korlátozására szolgáló egyik módszer az APPN funkciót használó rendszereken egy jogosultsági lista létrehozása. A jogosultsági lista tartalmazza az APPC eszközök használatára jogosult felhasználók listáját. Ezután a Parancs alapértelmezések módosítása (CHGCMDDFT) paranccsal módosítani kell a CRTDEVAPPC parancsot. A CRTDEVAPPC parancs jogosultság (AUT) paraméterében alapértelmezett értékként meg kell adni a létrehozott jogosultsági listát.

Megjegyzés: Ha a rendszeren több másodlagos nyelv is telepítve van, akkor parancs alapértelmezéseket az egyes nyelvek QSYSxxxx könyvtáraiban található parancsoknál is módosítani kell.

Az APPC eszköz hely jelszó (LOCPWD) paraméterével történik a szekciót (egy felhasználó vagy alkalmazás nevében) kérő rendszer azonosságának ellenőrzése. A hely jelszó segíthet az imposztor rendszerek felismerésében.

Hely jelszavak alkalmazása esetén a jelszavakat egyeztetni kell a hálózat többi rendszerének biztonsági adminisztrátorával. Emellett korlátozni kell az APPC eszközleírások és konfigurációs listák létrehozására és módosítására jogosult felhasználókat is. A rendszer *IOSYSCFG speciális jogosultságot igényel az APPC eszközök és konfigurációs listák kezelésére szolgáló parancsok használatához.

Megjegyzés: APPN használata esetén a hely jelszavak az eszközleírások helyett a QAPPNRMT konfigurációs listában találhatók.

APPC felhasználói hozzáférés a célrendszerhez

A rendszerek az APPC szekció kialakításakor létrehoznak egy útvonalat a kérést benyújtó felhasználó és a célrendszerbe nyíló ajtó között. Több más elem is hatással van arra, hogy a felhasználónak mit kell tennie ahhoz, hogy belépést nyerhessen a másik rendszerre.

Az alábbi témakörök mutatják be azon elemeket, amelyek meghatározzák, hogyan nyerhetnek belépést az APPC felhasználók a célrendszerre.

A rendszer módszerei a felhasználói információk küldésére

Az APPC architektúra három lehetőséget biztosít a felhasználókra vonatkozó biztonsági információk elküldéséhez a forrásrendszerről a célrendszerre. Ezeket a módszereket **architekturális biztonsági értékeknek** hívjuk. A módszereket a 18. táblázat: mutatja be:

Megjegyzés: Az architekturális biztonsági értékekről további információkat az *APPC Programming* című kiadványban talál.

18. táblázat: APPC architektúra biztonsági értékei

Architekturális biztonsági érték	Felhasználói azonosító elküldése	Jelszó elküldése
Nincs	Nem	Nem
Ugyanaz	Igen[1]	Lásd a 2. megjegyzést.
Program	Igen	Igen[3]

18. táblázat: APPC architektúra biztonsági értékei (Folytatás)

Architekturális biztonsági érték	Felhasználói azonosító elküldése	Jelszó elküldése

Megjegyzések:

1. A forrásrendszer akkor küldi el a felhasználói azonosítót, ha a célrendszer a SECURELOC(*YES) vagy a SECURELOC(*VFYENCPWD) paramétert adja meg.
2. A felhasználó nem ad meg jelszót a kérésben, mivel a jelszót a forrásrendszer már ellenőrizte. A SECURELOC(*YES) és a SECURELOC(*NO) beállítása esetén a forrásrendszer nem küldi el a jelszót. SECURELOC(*VFYENCPWD) esetén a forrásrendszer visszakeresi a titkosított formában tárolt jelszót és elküldi (titkosított formában).
3. A rendszer akkor küld titkosított jelszót, ha a forrás- és célrendszer is támogatja a jelszó titkosítást. Ellenkező esetben a jelszó nem kerül titkosításra.

Az architekturális biztonsági értéket a felhasználó által kért alkalmazás határozza meg. Az SNADS például mindig SECURITY(NONE) beállítást használ. A DDM SECURITY(SAME) értéket használ. Terminál átjelentkezés esetén a biztonsági értéket a felhasználó adja meg a STRPASTHR parancs paramétereiben.

A célrendszer minden esetben eldönti, hogy fogadja-e a kérést a forrásrendszertől kapott biztonsági érték mellett. Bizonyos esetekben elképzelhető, hogy a célrendszer teljesen visszautasítja a kérést. Olyan is történhet, hogy a célrendszer eltérő biztonsági értéket követel meg. Ha például a felhasználó a STRPASTHR parancsban felhasználói azonosítót és jelszót is megad, akkor a kérés SECURITY(PGM) beállítást használ. Ha azonban a célrendszeren a QRMTSIGN rendszerváltozó értéke *FRCSIGNON, akkor a felhasználónak ettől függetlenül megjelenik a bejelentkezés képernyő. Az *FRCSIGNON beállítással a rendszer mindig a SECURITY(NONE) beállítást használja, amely megegyezik azzal, ha a felhasználó nem ad meg felhasználói azonosítót és jelszót a STRPASTHR parancsban.

Megjegyzések:

1. A forrás- és célrendszer egyezteti a biztonsági értéket az adatforgalom megkezdése előtt. Az olyan helyzetekben, amikor a célrendszer SECURELOC(*NO) beállítást ad meg, és a kérés SECURITY(SAME), akkor a célrendszer megkéri a forrásrendszert a SECURITY(NONE) használatára. A forrásrendszer nem küldi el a felhasználói azonosítót.
2. A célrendszer visszautasítja a szekciókérést, amennyiben a felhasználó jelszava lejárt a célrendszeren. Ez a jelszót küldő kapcsolati kérésekre igaz, beleértve a következőket:
   - SECURITY(PROGRAM) típusú szekciókérések.
   - SECURITY(SAME) típusú szekciókérések a SECURELOC paraméter *VFYENCPWD beállításakor.

Lehetőségek a hálózati biztonsággal kapcsolatos felelősség megosztására

Amikor a rendszer hálózat tagja, akkor el kell dönteni, hogy megbízik-e a többi rendszerben a rendszerre belépni próbáló felhasználó azonosságának ellenőrzése szempontjából. Megbízik annyira a SYSTEMA rendszerben, hogy elhiggye neki, ha azt mondja a USERA felhasználóra, hogy USERA? Vagy ismét meg kell adnia a felhasználói azonosítót és jelszót?

A célrendszer APPC eszközleírásának védett hely (SECURELOC) paramétere határozza meg, hogy a forrásrendszer biztonságos (megbízható) hely-e.

Ha mindkét rendszeren olyan kiadás fut, amely támogatja a *VFYENCPWD beállítást, akkor a SECURELOC(*VFYENCPWD) további védelmet nyújt, amikor az alkalmazások SECURITY(SAME) beállítást használnak. Bár a kérő nem ad meg jelszót a kérésben, a

forrásrendszer visszakeresi a felhasználó jelszavát, és elküldi a kéréssel. Ahhoz, hogy a kérés sikeres legyen, a felhasználónak azonos felhasználói azonosítóval és jelszóval kell rendelkeznie mindkét rendszeren.

Ha a célrendszer SECURELOC(*VFYENCPWD) értéket ad meg, de a forrásrendszer ezt nem támogatja, akkor a célrendszer a kérést SECURITY(NONE) kérésként kezeli.

Az architekturális biztonsági érték és a SECURELOC érték együttműködését a 19. táblázat: mutatja be:

19. táblázat: Az APPC biztonsági érték és a SECURELOC érték együttműködése

Forrásrendszer	**Célrendszer**	
Architekturális biztonsági érték	**SECURELOC érték**	**Job felhasználói profilja**
Nincs	Tetszőleges	Alapértelmezett felhasználó[1]
Ugyanaz	*NO	Alapértelmezett felhasználó[1]
	*YES	A forrásrendszer kérőjével megegyező felhasználói profil
	*VFYENCPWD	A forrásrendszer kérőjével megegyező felhasználói profil. A felhasználónak azonos jelszóval kell rendelkeznie mindkét rendszeren.
Program	Tetszőleges	A forrásrendszer által a kérésben meghatározott felhasználói profilok.

Megjegyzések:

1. Az alapértelmezett felhasználót az alrendszerleírás kommunikációs bejegyzése határozza meg. Ezt a “Felhasználói profilok hozzárendelése a célrendszeren” szakasz részletezi.

Felhasználói profilok hozzárendelése a célrendszeren

Amikor egy felhasználó APPC jobot igényel egy másik rendszeren, akkor kéréshez tartozik egy társított módnév. A módnév származhat a felhasználói kérésből, illetve megadhatja a forrásrendszer hálózati attribútumainak alapértelmezett értéke is.

A célrendszer a módnév és az APPC eszköznév alapján határozza meg a job futásának módját. A célrendszer az aktív alrendszerekben keres egy olyan kommunikációs bejegyzést, amely a lehető leginkább megfelel az APPC eszköznévnek és a módnévnek.

A kommunikációs bejegyzés határozza meg, hogy a rendszer milyen felhasználói profilt használ a SECURITY(NONE) kérések esetén. Az alábbi példa egy alrendszerleírás kommunikációs bejegyzését mutatja be:

```
                        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
```

A kommunikációs bejegyzés alapértelmezett felhasználó paraméterének lehetséges értékeit a 20. táblázat: oldalszám: 112 mutatja be:

20. táblázat: Az alapértelmezett felhasználó paraméter lehetséges értékei

Érték	Eredmény
***NONE**	Nincs rendelkezésre álló alapértelmezett felhasználó. Ha a forrásrendszer nem ad meg felhasználói azonosítót a kérésben, akkor a job nem fut.
***SYS**	Csak IBM által szállított programok (rendszerjobok) futnak. Felhasználói alkalmazások futtatására nincs lehetőség.
felhasználónév	Ha a forrásrendszer nem küld felhasználói azonosítót, akkor a job ezen felhasználói profil alatt fut.

Az Alrendszerleírás kinyomtatása (PRTSBSDAUT) paranccsal nyomtathatja ki az összes olyan alrendszer listáját, amely alapértelmezett felhasználói profilt meghatározó kommunikációs bejegyzéssel rendelkezik.

Terminál átjelentkezés lehetőségek

A terminál átjelentkezés jó példa APPC kommunikációt használó alkalmazásra. A terminál átjelentkezés segítségével lehet bejelentkezni a hálózaton keresztül egy másik rendszerre.

Az átjelentkezési kérésekre (STRPASTHR parancs), illetve ezek kezelésére a célrendszeren a 21. táblázat: mutat be néhány példát. A terminál átjelentkezés esetén a rendszer az APPC kommunikáció alapelemeit és a távoli bejelentkezésre vonatkozó (QRMTSIGN) rendszerváltozókat használja.

Megjegyzés: A terminál átjelentkezési kérések a továbbiakban nem a QCMN és QBASE alrendszereken mennek keresztül. A V4R1 kiadással kezdődően ezek a QSYSWRK alrendszeren haladnak át. A V5R1 előtti kiadásokban a QCMD vagy QBASE alrendszerek elindításának elmaradása esetén feltételezni lehetett, hogy a terminál átjelentkezés nem működik. Ez már nem igaz. A QPASTHRSVR rendszerváltozó 0-ra állításával a terminál átjelentkezés kényszeríthető, hogy a QCMN (vagy QBASE) alrendszeren haladjon át.

21. táblázat: Példa átjelentkezés bejelentkezési kérések

STRPASTHR parancsban megadott értékek		**Célrendszer**		
Felhasználói azonosító	**Jelszó**	**SECURELOC érték**	**QRMTSIGN érték**	**Eredmény**
*NONE	*NONE	Tetszőleges	Tetszőleges	A felhasználónak be kell jelentkeznie a célrendszeren.
Felhasználói profil	Nincs megadva	Tetszőleges	Tetszőleges	A kérés meghiúsul.

21. táblázat: Példa átjelentkezés bejelentkezési kérések (Folytatás)

STRPASTHR parancsban megadott értékek		**Célrendszer**		
Felhasználói azonosító	**Jelszó**	**SECURELOC érték**	**QRMTSIGN érték**	**Eredmény**
*CURRENT	Nincs megadva	*NO	Tetszőleges	A kérés meghiúsul.
		*YES	*SAMEPRF	Elindul egy interaktív job ugyanazzal a felhasználói profil névvel, mint ami alatt a forrásrendszeren fut. A távoli rendszer számára jelszó nem kerül átadásra.A felhasználói profilnak léteznie kell a célrendszeren.
			*VERIFY	
			*FRCSIGNON	A felhasználónak be kell jelentkeznie a célrendszeren.
		*VFYENCPWD	*SAMEPRF	Elindul egy interaktív job ugyanazzal a felhasználói profil névvel, mint ami alatt a forrásrendszeren fut. A forrásrendszer visszakeresi a felhasználó jelszavát, és elküldi a távoli rendszerre. A felhasználói profilnak léteznie kell a célrendszeren.
			*VERIFY	
			*FRCSIGNON	A felhasználónak be kell jelentkeznie a célrendszeren.
*CURRENT (vagy a job aktuális felhasználói profiljának neve)	Meg van adva	Tetszőleges	*SAMEPRF	Elindul egy interaktív job ugyanazzal a felhasználói profil névvel, mint ami alatt a forrásrendszeren fut. A jelszó *elküldésre kerül* a távoli rendszerre.A felhasználói profilnak léteznie kell a célrendszeren.
			*VERIFY	
			*FRCSIGNON	A felhasználónak be kell jelentkeznie a célrendszeren.
Felhasználói profil (a job aktuális felhasználói profiljától különböző név)	Meg van adva	Tetszőleges	*SAMEPRF	A kérés meghiúsul.
			*VERIFY	Elindul egy interaktív job ugyanazzal a felhasználói profil névvel, mint ami alatt a forrásrendszeren fut. A jelszó *elküldésre kerül* a távoli rendszerre.A felhasználói profilnak léteznie kell a célrendszeren.
			*FRCSIGNON	Elindul egy interaktív job a megadott felhasználói profillal. A jelszó elküldésre kerül a célrendszernek. A felhasználói profilnak léteznie kell a célrendszeren.

Váratlan eszköz hozzárendelések elkerülése

Ha egy aktív eszközön hiba történik, akkor a rendszer megkísérli a helyreállítást. Bizonyos körülmények között a kapcsolat megszakadásakor egy másik felhasználó véletlenül újra kialakíthatja a hibás szekciót. Tegyük fel például, hogy a USERA felhasználó kijelentkezés nélkül kikapcsolta munkaállomását. A USERB bekapcsolhatja a munkaállomást, és bejelentkezés nélkül újraindíthatja a USERA felhasználó szekcióját.

Az említett lehetőség elkerülése érdekében az Eszköz I/O hiba tevékenység (QDEVRCYACN) rendszerváltozónak a *DSCMSG értéket kell beállítani. Ebben az esetben az eszközök meghibásodásakor a rendszer befejezi a felhasználó jobját.

Távoli parancsok és kötegelt jobok felügyelete

A rendszer több lehetőséget is biztosít a rendszeren futtatható távoli parancsok és jobok felügyeletére, például:

- Ha a rendszer használja a DDM funkciókat, akkor korlátozhatja a DDM fájlokra vonatkozó hozzáféréseket, így megakadályozhatja, hogy a felhasználók távoli rendszerről Távoli parancs elküldése (SBMRMTCMD) parancsot adjanak ki. A SBMRMTCMD használatához a felhasználónak képesnek kell lennie egy DDM fájl megnyitására. Emellett korlátozni kell a DDM fájlok létrehozásának képességét is.
- Megadhat egy végprogramot a DDM kérés hozzáférés (DDMACC) rendszerváltozónak. A végprogramban kiértékelheti az összes DDM kérést, mielőtt engedélyezné azokat.
- A hálózati job tevékenység (JOBACN) hálózati attribútummal megakadályozhatja hálózati jobok kiadását, illetve ezek automatikus futtatását.
- Megadhatja kifejezetten, hogy mely program kérések futhatnak egy adott kommunikációs környezetben a PGMEVOKE továbbítási bejegyzés eltávolításával az alrendszerleírásokból. A PGMEVOKE továbbítási bejegyzés lehetővé teszi a kérő számára a futtatandó program meghatározását. Ha eltávolítja ezt a továbbítási bejegyzést az alrendszerleírásokból, például a QCMN alrendszerből, akkor fel kell vennie azoknak a kommunikációs kéréseknek a továbbítási bejegyzéseit, amelyeknek sikeresen le kell futniuk.

  Az IBM által szállított alkalmazások által használt kommunikációs kérések programneveit az “Architekturális TPN kérések” oldalszám: 89 szakasz sorolja fel. Minden egyes engedélyezni kívánt kérésnél hozzáadhat egy olyan továbbítási bejegyzést, amelynek összehasonlítási értéke és programneve is megegyezik a program nevével.

  A módszer használatakor meg kell ismerni a rendszeren alkalmazott jobkezelési környezet működését, illetve a rendszeren bekövetkező kommunikációs kérések típusait. Ha lehetséges, akkor a kommunikációs kérések összes típusát le kell tesztelni annak biztosítása érdekében, hogy ezek a továbbítási bejegyzések módosítása után is megfelelően fognak működni. Ha egy kommunikációs kérés nem talál rendelkezésre álló továbbítási bejegyzést, akkor CPF1269 üzenet érkezik. Egy némileg kisebb hiba valószínűséggel rendelkező, viszont kevésbé hatékony másik alternatíva, hogy a rendszeren nem kívánt tranzakciós programok nyilvános jogosultságát az *EXCLUDE értékre állítja.

  Megjegyzés: A továbbítási bejegyzésekről, illetve a program indítási kérések kezeléséről további információkat a *Work Management* című kiadványban talál.

APPC konfiguráció kiértékelése

A Kommunikációs biztonság kinyomtatása (PRTCMNSEC) paranccsal vagy menüpontokkal nyomtathatja ki az APPC konfiguráció biztonsággal kapcsolatos értékeit. A következő szakaszok a jelentésekben megadott információkat írják le.

APPC eszközök kapcsolódó paraméterei

Az 9. ábra: mutat be egy példát az eszközleírásokra vonatkozó Kommunikációs információs jelentésre. A konfigurációs listákra vonatkozó jelentés mintája az 10. ábra: helyen látható. A jelentésekben szereplő mezők magyarázata a jelentések után következik.

```
                          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
```

9. ábra: APPC eszközleírások - Minta jelentés

```
                  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
```

10. ábra: Konfigurációs lista jelentés - Példa

Védett hely mező

A védett hely (SECURELOC) mező határozza meg, hogy a helyi rendszer megbízik-e a távoli rendszerben a jelszó ellenőrzés szempontjából. A SECURELOC mező csak a SECURITY(SAME) beállítást (például DDM) és a CPI-kommunikációs API-t használó alkalmazásokra vonatkozik.

A SECURELOC(*YES) érzékennyé teszi a helyi rendszert a távoli rendszer lehetséges gyengeségeire. Bármely mindkét rendszeren létező felhasználó meghívhat programokat a helyi rendszeren. Ez azért különösen veszélyes, mert a QSECOFR (adatvédelmi megbízott) felhasználói profil minden iSeries rendszeren létezik, és rendelkezik *ALLOBJ speciális jogosultsággal. Ha az egyik rendszer nem foganatosít kellő intézkedéseket a QSECOFR jelszavának védelmére, akkor a rendszert biztonságos helynek tekintő többi rendszer is veszélynek van kitéve.

A SECURELOC(*VFYENCPWD) használatakor a rendszer kevésbé érzékeny a jelszavak védelmét nem megfelelően biztosító rendszerekre. A SECURITY(SAME) alkalmazásokat kérő felhasználóknak azonos felhasználói azonosítóval és jelszóval kell rendelkezniük

mindkét rendszeren. A SECURELOC(*VFYENCPWD) teljes hálózatra kiterjedő jelszó felügyeleti stratégiákat igényel annak érdekében, hogy a felhasználók minden rendszeren azonos jelszóval rendelkezzenek.

Megjegyzés: A SECURELOC(*VFYENCPWD) csak V3R2, V3R7 és V4R1 rendszerek között támogatott. Ha a célrendszer SECURELOC(*VFYENCPWD) biztonságot igényel, de a forrásrendszer ezt nem támogatja, akkor a kérés SECURITY(NONE) kérésnek minősül.

Ha egy rendszer SECURELOC(*NO) értéket ad meg, akkor a SECURITY(SAME) alkalmazásoknak a programok futtatásához alapértelmezett felhasználóra van szükségük. Az alapértelmezett felhasználót az eszközleírás és a kéréshez társított mód együttesen határozza meg. (Lásd: “Felhasználói profilok hozzárendelése a célrendszeren” oldalszám: 111.)

Hely jelszó mező

A Hely jelszó mező határozza meg, hogy a két rendszer cserél-e jelszót egymás ellenőrzésének érdekében. A hely jelszavakról további információkat a “Példa: Alapvető APPC szekció” oldalszám: 108 szakasz tartalmaz.

APPN kezelésére képes mező

Az APPN kezelésére képes (APPN) mező határozza meg, hogy a távoli rendszer támogatja-e a fejlett hálózatkezelési funkciókat, vagy egyállomásos kapcsolatokra korlátozott. Az APPN(*YES) a következőket jelenti:

- Ha a távoli rendszer hálózati csomópont, akkor elképzelhető, hogy képes a helyi rendszer más rendszerekhez kapcsolására. Ezt **köztes csomópont továbbításnak** hívjuk. Ez azt jelenti, hogy a helyi rendszer felhasználói a távoli rendszert használhatják más hálózatokhoz vezető útvonalként.
- Ha a helyi rendszer hálózat csomópont, akkor a távoli rendszer használhatja a helyi rendszert más rendszerekhez csatlakozásra. A távoli rendszer felhasználói útválasztóként használhatják a helyi rendszert nagyobb hálózatok felé.

  Megjegyzés: A rendszer hálózati csomópont vagy végponti csomópont jellegének meghatározására a DSPNETA parancs használható.

Egyetlen szekció mező

Az egyetlen szekció (SNGSSN) mező határozza meg, hogy a távoli rendszer tud-e egynél több szekciót futtatni azonos APPC eszközleírás felhasználásával. Az általános beállítás a SNGSSN(*NO), mivel ilyenkor nincs szükség több eszközleírás létrehozására a távoli rendszerek számára. A PC felhasználók például általában egynél több 5250 emulációs szekciót használnak, emellett fájlszerver és nyomtatószerver funkciókra is szükségük van. A SNGSSN(*NO) beállítás esetén mindeme szolgáltatásokat az iSeries rendszer egyetlen eszközleírásával biztosíthatja a PC számára.

A SNGSSN(*NO) azt jelenti, hogy a PC felhasználók és más APPC felhasználók biztonságtudatos tevékenykedésére épít. A rendszer számára kockázatot jelent, ha a távoli rendszeren valaki jogosulatlan szekciót indít egy meglévő szekció eszközleírásának felhasználásával. (Ezt a módszert néha **egymásra ültetésnek** is hívják.)

Szekció előzetes kialakítása mező

Az egyetlen szekciós eszközöknél a szekció előzetes kialakítása (PREESTSSN) mező határozza meg, hogy a forrásrendszer indít-e szekciót a távoli rendszerrel, amikor a távoli rendszer először kapcsolatba lép a helyi rendszerrel. A PREESTSSN(*NO) azt jelenti, hogy a helyi rendszer várakozik a szekció indításával, amíg egy alkalmazás nem kéri egy szekció kialakítását. A PREESTSSN(*YES) beállítással minimálisra csökkenthető az alkalmazásprogram várakozása a szekció kialakítására.

A PREESTSSN(*YES) megakadályozza a rendszert a használaton kívüli kapcsolt (telefon-) vonal szétkapcsolásában. A szétkapcsoláshoz az alkalmazásnak vagy felhasználónak kifejezetten le kell kapcsolnia a vonalat. A PREESTSSN(*YES) meghosszabbíthatja az időszakot, amelynek során a helyi rendszer érzékeny az egymásra ültetett szekciókra.

SNUF program indítás mező

A SNUF program indítás mező határozza meg, hogy a távoli rendszer jogosult-e programok indítására a helyi rendszeren. A *YES azt jelenti, hogy a helyi rendszeren alkalmazott objektum jogosultsági sémának elegendő védelmet kell biztosítania az objektumok számára a távoli rendszer felhasználói által a helyi rendszeren elindított jobokkal és programokkal szemben.

APPC vezérlők paraméterei

Az 11. ábra: mutat be egy példát a vezérlőleírásokra vonatkozó Kommunikációs információs jelentésre. A jelentésben szereplő mezők leírása a jelentés után található.

```
                    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
```

11. ábra: APPC vezérlőleírások - Minta jelentés

Automatikus létrehozás mező

A vonalleírások automatikus létrehozás (AUTOCRTCTL) mezője határozza meg, hogy a helyi rendszer létrehoz-e automatikusan egy vezérlőleírást abban az esetben, amikor egy bejövő kérés nem talál megfelelő vezérlőleírást. A vezérlőleírások automatikus létrehozás (AUTOCRTDEV) mezője határozza meg, hogy a helyi rendszer létrehoz-e automatikusan egy eszközleírást abban az esetben, amikor egy bejövő kérés nem talál megfelelő eszközleírást.

APPN kezelésére képes vezérlők esetén az automatikus létrehozás mezőnek nincs hatása. A rendszer az automatikus létrehozás mező beállításától függetlenül szükség esetén automatikusan létrehozza az eszközleírásokat.

Ha egy vonalleírásnál értéke *YES, akkor a rendszerhez bárki csatlakozhat, aki hozzáfér a vonalhoz. Ebbe a hidakon és útválasztókon keresztül csatlakozó rendszerek felhasználói is beletartoznak.

Vezérlőpont szekciók mező

APPN használatára képes vezérlők esetén a vezérlőpont szekciók (CPSSN) mező határozza meg, hogy a rendszer alakít-e ki automatikusan APPC kapcsolatot a távoli rendszerrel. A rendszer a vezérlőpont szekciót használja a hálózati információk és az állapot adatcseréjére a távoli rendszerrel. A naprakész információk cseréje különösen APPN hálózati csomópontok között fontos, mivel ez biztosítja a hálózat zökkenőmentes működését.

*YES beállítása esetén a tétlen kapcsolt vonalak nem kerülnek automatikusan szétkapcsolásra. Ennek eredményeként a helyi rendszer érzékenyebb lesz az egymásra ületett szekciókra.

Szétkapcsolási időmérő mező

APPC vezérlők esetén a szétkapcsolási időmérő mező határozza meg, hogy a vezérlőnek milyen hosszú ideig kell használaton kívül lennie ahhoz, hogy a rendszer szétkapcsolja a távoli rendszerhez vezető vonalat. A mező két értéket tartalmaz. Az első érték határozza meg,

hogy a vezérlő mennyi ideig marad aktív a kezdeti kapcsolatfelvétel után. A második érték azt adja meg, hogy a rendszer mennyi ideig várakozik a vezérlő utolsó szekciójának befejezése után a vonal bontása előtt.

A rendszer csak akkor használja a szétkapcsolási időmérőt, ha a kapcsolt szétkapcsolás (SWTDSC) mező értéke *YES.

Az értékek nagyra állításakor a helyi rendszer érzékenyebb lesz az egymásra ületett szekciókra.

Vonalleírások paraméterei

Az 12. ábra: mutat be egy példát a vonalleírásokra vonatkozó Kommunikációs információs jelentésre. A jelentésben szereplő mezők leírása a jelentés után található.

```
                    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
```

12. ábra: APPC vonalleírások - Minta jelentés

Automatikus válasz mező

Az automatikus válasz (AUTOANS) mező határozza meg, hogy a kapcsolt vonal fogad-e hívásokat operátori beavatkozás nélkül.

*YES beállítása esetén a rendszer kevésbé biztonságos, mivel egyszerűbben elérhető. A biztonsági kockázat csökkentése érdekében *YES beállítás használata esetén a szükségtelen vonalat ki kell kapcsolni.

Automatikus hívás mező

Az automatikus hívás (AUTODIAL) mező adja meg, hogy a kapcsolt vonal kezdeményezhet-e kimenő hívásokat operátori beavatkozás nélkül. A *YES érték használata lehetővé teszi a kommunikációs vonalakhoz és modemekhez fizikai hozzáféréssel nem rendelkező helyi felhasználóknak más rendszerek elérését.

13. fejezet Biztonságos TCP/IP kommunikáció

A TCP/IP (Átvitelvezérlési protokoll/Internet protokoll) a különféle típusú számítógépek által az egymással való kommunikációhoz használt általános módszer. A TCP/IP alkalmazások közismertek és széles körben használják őket az “információs szupersztrádán”.

Ez a fejezet a következőkkel kapcsolatban ad tanácsokat:

- TCP/IP alkalmazások futásának megakadályozása a rendszeren.
- Rendszererőforrások védelme, ha a rendszeren futnak TCP/IP alkalmazások.

A TCP/IP alkalmazásokról az iSeries Információs központ Hálózatok → TCP/IP témaköre tartalmaz kimerítő információkat. Az iSeries szerver Internetre vagy intrenetekre csatlakoztatásával járó biztonsági szempontokat az iSeries Információs központ Biztonság → SecureWay → *SecureWay: iSeries és az Internet* témaköre taglalja. Az iSeries Információs központ elérésével kapcsolatban nézze meg az “Előfeltétel és kapcsolódó információk” oldalszám: xii szakaszt.

Ne feledje, hogy az iSeries szerverek sokféle lehetséges TCP/IP alkalmazást támogatnak. Ha úgy dönt, hogy engedélyez egy TCP/IP alkalmazást a rendszeren, akkor elképzelhető, hogy ezzel más TCP/IP alkalmazásokat is engedélyez. A biztonsági adminisztrátornak figyelemmel kell lennie a használt TCP/IP alkalmazásokra, és az ezekből adódó biztonsági következményekre.

TCP/IP feldolgozás megakadályozása

A TCP/IP szerverjobok a QSYSWRK alrendszerben futnak. A TCP/IP a TCP/IP indítása (STRTCP) paranccsal indítható el a rendszeren. Ha nem kíván futtatni semmilyen TCP/IP feldolgozást vagy alkalmazást, akkor ne adja ki az STRTCP parancsot. A rendszer alapértelmezett beállítása szerint az STRTCP parancs nyilvános jogosultsága *EXCLUDE.

Ha gyanítja, hogy a parancshoz hozzáférő valamelyik felhasználó elindítja a TCP/IP-t (munkaidőn kívül például), akkor állítsa be az STRTCP parancs objektum megfigyelését. A rendszer a parancs minden futtatása esetén létrehoz egy bejegyzést a megfigyelési naplóban.

TCP/IP biztonsági összetevők

A hálózat biztonságának és rugalmasságának növelése érdekében a rendszer több TCP/IP biztonsági összetevőt is tartalmaz. Bár a biztosított technológiák egy része tűzfal termékekben is megtalálható, az OS/400 TCP/IP biztonsági összetevők tűzfalként való felhasználása ellenjavallt. A szolgáltatások némelyike mindazonáltal bizonyos helyzetekben felhasználható a különálló tűzfal termék iránti igények kiküszöbölésére. Emellett az említett TCP/IP szolgáltatások tűzfal használata esetén felhasználhatók kiegészítő biztonsági intézkedések foganatosítására.

A TCP/IP biztonságának kibővítésére a következő összetevők állnak rendelkezésre:

- Csomagszabályok
- HTTP proxy szerver
- VPN (Virtuális magánhálózatok)
- SSL (Védett socket réteg)

TCP/IP forgalom biztonságossá tétele csomagszabályok felhasználásával

Az IP szűrést és hálózati cím fordítást (NAT) egyesítő csomagszabályok a tűzfalakhoz hasonlóan működnek a belső hálózat behatolókkal szembeni védelmének biztosításához. Az IP szűrés lehetővé teszi a hálózatba beengedett IP forgalom felügyeletét. A hálózat védelmét a csomagoknak a megadott szabályok szerinti szűrése biztosítja. A NAT lehetővé teszi a bejegyzetlen belső IP címek elrejtését bejegyzett IP címek mögött. Ez szintén védi a belső hálózatot a külső hálózatokkal szemben. A NAT emellett enyhít az IP címek fogyásával kapcsolatos problémán, mivel lehetővé teszi, hogy néhány bejegyzett cím nagy számú belső címet képviseljen. További részleteket az iSeries Információs központban talál.

HTTP proxy szerver

A HTTP proxy szerver az IBM HTTP Server for iSeries része. A HTTP szerver az OS/400 része. A proxy szerver fogadja web böngészők HTTP kéréseit, és továbbítja azokat a webszerverek felé. A kéréseket fogadó webszerverek csak a proxy szerver IP címét ismerik, és nem tudják meghatározni a kéréseket kezdeményező számítógépek neveit vagy címeit. A proxy szerver HTTP, FTP, Gopher és WAIS URL kéréseket kezel.

A proxy szerver a felhasználók által kért összes weblapot ideiglenes tárolóba helyezi. Amikor a felhasználók lekérnek egy lapot, a proxy szerver először ellenőrzi, hogy az megtalálható-e az ideiglenes tárolóban. Ha igen, akkor a proxy szerver a tárolt lapot adja vissza. A lapok tárolásával a proxy szerver gyorsabban tudja visszaadni a weblapokat, így kiküszöbölve a webszerver felé irányuló időigényes kérések szükségességét.

A proxy szerver emellett nyomkövetési céllal naplózza az összes URL kérést. A naplók áttekintésével képet kaphat a hálózati erőforrások használatáról és az ezzel kapcsolatos visszaélésekről.

Az IBM HTTP Server termékbe integrált proxy szervert használhatja a webes hozzáférés egyesítésére is. A PC kliensek címei rejtve maradnak a használt webszerverek előtt, ezek ugyanis csak a proxy szerver IP címét ismerik. A weblapok ideiglenes tárolása emellett csökkentheti a sávszélességre vonatkozó igényeket és a tűzfal terhelését. További információkat az IBM HTTP Server for iSeries honlapján talál: http://www-1.ibm.com/servers/eserver/iseries/software/http/index.html

Virtuális magánhálózatok (VPN)

A virtuális magánhálózatok (VPN) lehetővé teszik a vállalat számára a belső intranet kiterjesztését egy nyilvános hálózat, például az Internet meglévő keretrendszerének felhasználásával. A VPN segítségével a vállalat felügyelheti a hálózat forgalmát, emellett fontos biztonsági szolgáltatásokhoz is juthat, például hitelesítéshez és titoktartáshoz.

Az OS/400 VPN az iSeries navigátor, az OS/400 grafikus kezelőfelületének választhatóan telepíthető összetevője. Lehetővé teszi biztonságos útvonalak létrehozását hosztok és átjárók tetszőleges kombinációja között. Az OS/400 VPN a kapcsolat két végpontja között forgalmazott adatok biztonságának érdekében hitelesítési módszereket, titkosítási algoritmusokat és további funkciókat biztosít.

A VPN a TCP/IP rétegekre osztott kommunikációs verem modelljének hálózati rétegén fut. Pontosabban a VPN az IP biztonsági architektúra (IPSec) keretrendszerét használja. Az IPSec alapvető biztonsági funkciókat nyújt az Interneten, emellett rugalmas építőelemeket biztosít hatékony és biztonságos virtuális magánhálózatok létrehozásához.

A VPN funkció támogatja a 2. szintű alagútkezelési protokollt (L2TP) alkalmazó VPN megoldásokat is. A virtuális vonalaknak is nevezett L2TP kapcsolatok költséghatékony

hozzáférést biztosítanak a távoli felhasználók számára azáltal, hogy lehetővé teszik a vállalati hálózat szervereinek a távoli felhasználókhoz hozzárendelt IP címek kezelését. Ezen kívül az L2TP kapcsolatok IPSec védelem használata esetén biztonságos hozzáférést nyújtanak a rendszerhez vagy hálózathoz.

Fontos megérteni, hogy a VPN a teljes hálózatra hatással van. A gondos tervezés és megvalósítás a siker kulcsfontosságú része. A virtuális magánhálózatok működéséről és felhasználási lehetőségeiről az iSeries Információs központ VPN témakörében tájékozódhat. További információkat az iSeries Információs központ Biztonság→ Virtuális magánhálózatok című témakörében talál. Az iSeries Információs központ elérésével kapcsolatban nézze meg az “Előfeltétel és kapcsolódó információk” oldalszám: xii szakaszt.

Védett socket réteg (SSL)

A Védett socket réteg (SSL) a nem védett hálózatok, például az Internet feletti védett kommunikációt biztosító ipari szabvány biztonsági protokoll. Az SSL protokoll felhasználásával lehetővé válik a védett kapcsolatok kialakítása a kliensek és szerver alkalmazások között, továbbá lehetőség van a kapcsolati végpontok hitelesítésére is. Az SSL emellett biztosítja a kliens és a szerver alkalmazás közötti adatcsere bizalmasságát és integritását. További részleteket az iSeries Információs központ Biztonság → Védett socket réteg (SSL) című témakörében talál. Az iSeries Információs központ elérésével kapcsolatban nézze meg az “Előfeltétel és kapcsolódó információk” oldalszám: xii szakaszt.

A TCP/IP környezet biztonságosabbá tétele

Ez a témakör írja le a rendszer TCP/IP környezete miatt keletkezett biztonsági kockázatok csökkentése érdekében foganatosítható általános lépéseket. A megadott információk a teljes TCP/IP környezetre vonatkoznak; az egyes alkalmazásokra jellemző tudnivalókat a későbbiek során tárgyaljuk.

- TCP/IP portot használó alkalmazások írásakor győződjön meg róla, hogy az alkalmazás elég biztonságos. Mindig azt kell szem előtt tartani, hogy az alkalmazást megpróbálják felhasználni a rendszerbe való behatolásra. Egy hozzáértő külső felhasználó például Telnet segítségével becsatlakozhat az alkalmazáshoz.
- A rendszer TCP/IP portjain érdemes megfigyelést végezni. A TCP/IP porthoz társított felhasználói alkalmazások “hátsó ajtót” biztosíthatnak a rendszerre való bejutáshoz. Az elegendő jogosultsággal rendelkező felhasználók társíthatnak alkalmazást TCP vagy UDP porttal.
- Biztonsági adminisztrátorként tisztában kell lennie a betörők által alkalmazott *IP cím hamisítási* technikával. A TCP/IP hálózatok valamennyi rendszere rendelkezik egy IP címmel. Az IP cím hamisítást alkalmazó felhasználó úgy állít be egy rendszert (általában egy személyi számítógépet), hogy az egy meglévő IP címet vagy megbízható IP címet szimuláljon. Ezáltal az imposztor úgy alakíthat ki kapcsolatot a rendszerrel, hogy közben a rendszer azt hiszi, hogy egy elfogadott kapcsolatról van szó.

  Ha a rendszeren fut a TCP/IP, és a rendszer fizikailag nem védett hálózathoz csatlakozik (csak dedikált porthoz csatlakozó vonalakat és előre meghatározott összeköttetéseket tartalmazó hálózat), akkor a rendszert bármikor érheti IP cím hamisításos támadás. A rendszer védelme érdekében (a “hamisító” ellen) először alkalmazza ezen fejezetnek például a bejelentkezés védelmére és az objektumok biztonságára vonatkozó javaslatait. Ezeken kívül biztosítani kell, hogy a rendszeren ésszerű háttértár korlátok vannak beállítva. Ez megakadályozza az olyan jellegű támadásokat is, amikor a támadó elárasztja a rendszert levelekkel vagy spoolfájlokkal, amelynek eredményeként a rendszer végül működésképtelen állapotba kerül.

  Mindezek mellett a TCP/IP tevékenységet rendszeresen meg kell figyelni a rendszeren. IP cím hamisításra utaló jelek észlelésekor próbálja feltérképezni a TCP/IP konfiguráció gyenge pontjait, és végezze el a megfelelő módosításokat.

- Az intraneten (közvetlen külső kapcsolattal nem rendelkező rendszerek hálózata) használjon újrafelhasználható IP címeket. Az újrafelhasználható címek csak belső hálózatokon alkalmazhatók. Az internetes útválasztók nem továbbítják az újrafelhasználható IP címmel rendelkező csomagokat. Ennek következtében az újrafelhasználható címek alkalmazása újabb biztonsági réteget eredményez a tűzfalon belül.

  Az IP címek hozzárendeléséről, az IP címtartományokról és a TCP/IP biztonságról az iSeries Információs központ Hálózatok → TCP/IP témaköre nyújt kimerítő ismereteket.
- Ha a rendszer Internetre vagy intranetre csatlakoztatását tervezi, akkor nézze át az erre vonatkozó biztonsági szempontokat az iSeries Információs központ Biztonság → SecureWay → *SecureWay: iSeries és az Internet* című témakörében. Az iSeries Információs központ elérésével kapcsolatban nézze meg az “Előfeltétel és kapcsolódó információk” oldalszám: xii szakaszt.

Automatikusan induló TCP/IP szerverek meghatározása

Biztonsági adminisztrátorként meg kell határoznia, hogy mely TCP/IP alkalmazásoknak kell automatikusan elindulni a TCP/IP indításakor. A TCP/IP indítására két parancs használható. A rendszer mindkét parancsnál eltérő módszert használ az indítandó alkalmazások (szerverek) meghatározásához.

A két parancsot, és a rájuk vonatkozó biztonsági javaslatokat a 22. táblázat: mutatja be. A 23. táblázat: oldalszám: 123 a szerverek alapértelmezett automatikus indítási értékeit sorolja fel. A szerverek automatikus indítás értékének módosításához használja a CHGxxxA (xxx attribútumainak módosítása) parancsot a megfelelő szerveren. A Telnet szerver esetén például a parancs CHGTELNA.

22. táblázat: Indítandó szerverek meghatározása a TCP/IP parancsokban

Parancs	Induló szerverek	Biztonsági javaslatok
TCP/IP indítása (STRTCP)	A rendszer az összes AUTOSTART(*YES) szervert elindítja. Az egyes TCP/IP szerverek alapértelmezett értékeit a 23. táblázat: oldalszám: 123 tartalmazza.	• Az *IOSYSCFG speciális jogosultság adományozását kellő körültekintéssel végezze, mivel ezzel módosíthatók az automatikus indításra vonatkozó beállítások. • Az STRTCP parancsra vonatkozó jogosultságokra oda kell figyelni. A parancs alapértelmezett nyilvános jogosultságsága *EXCLUDE. • A *Szervernév* attribútumok módosítása (például CHGTELNA) parancsokra állítson meg objektum megfigyelést, és kövesse nyomon, hogy kik próbálkoznak egy szerver AUTOSTART értékének módosításával.
TCP/IP szerver indítása (STRTCPSVR)	Az indítandó szerver paraméterben adható meg. A parancs alapértelmezés szerint minden szervert elindít.	• A Parancs alapértelmezés módosítása (CHGCMDDFT) paranccsal állíthatja át az STRTCPSVR parancs alapértelmezését úgy, hogy csak egy adott szervert indítson el. Ez nem akadályozza meg a felhasználókat más szerverek elindításában. A parancs alapértelmezésének módosításával mindazonáltal elkerülhetők azok a helyzetek, amikor véletlenül elindítják az összes szervert. A következő paranccsal állíthatja be például, hogy a parancs alapértelmezésben csak a Telnet szervert indítsa el: CHGCMDDFT CMD(STRTCPSVR) NEWDFT('SERVER(*TELNET)') **Megjegyzés:** Az alapértelmezett érték módosításakor csak egyetlen szerver adható meg. Ehhez válasszon olyan szervert, amelyet rendszeresen használ, vagy amely a legkevésbé valószínű, hogy biztonsági problémát jelent (például TFTP). • Az STRTCPSVR parancsra vonatkozó jogosultságokra oda kell figyelni. A parancs alapértelmezett nyilvános jogosultságsága *EXCLUDE.

Az alábbi táblázat tartalmazza a TCP/IP szerverek automatikus indítás értékeit. Az egyes szerverekről további részleteket az iSeries Információs központ **Hálózatok → TCP/IP** témaköréből tudhat meg. Az iSeries Információs központ elérésével kapcsolatban nézze meg az “Előfeltétel és kapcsolódó információk” oldalszám: xii szakaszt.

23. táblázat: TCP/IP szerverek automatikus indítás értékei

Szerver	Alapértelmezett érték	Saját érték
TELNET	AUTOSTART(*YES)	
FTP (Fájlátviteli protokoll)	AUTOSTART(*YES)	
BOOTP (Rendszerbetöltési protokoll)	AUTOSTART(*NO)	
TFTP (egyszerű fájlátviteli protokoll)	AUTOSTART(*NO)	
REXEC (Távoli végrehajtási szerver)	AUTOSTART(*NO)	
RouteD (Útvonal démon)	AUTOSTART(*NO)	
SMTP (egyszerű levéltovábbítási protokoll)	AUTOSTART(*YES)	
POP (Postahivatal protokoll)	AUTOSTART(*NO)	
HTTP (Hiperszöveg átviteli protokoll) [1]	AUTOSTART(*NO)	
ICS (Internet Connection Server)[1]	AUTOSTART(*NO)	
LPD (sornyomtató démon)	AUTOSTART(*YES)	
SNMP (Simple Network Management Protocol (SNMP))	AUTOSTART(*YES)	
DNS (tartománynév rendszer)	AUTOSTART(*NO)	
DDM	AUTOSTART(*NO)	
DHCP (dinamikus hoszt konfigurációs protokoll)	AUTOSTART(*NO)	
NSMI	AUTOSTART(*NO)	
INETD	AUTOSTART(*NO)	

Megjegyzések:

1. Az IBM HTTP Server for iSeries szerver esetén az AUTOSTART érték beállítására a CHGHTTPA parancs használható.

SLIP biztonsági szempontok

Az iSeries szerver TCP/IP támogatása magában foglalja a Soros vonali Internet protokollt (SLIP). A SLIP alacsony költségigényű pont-pont kapcsolatot biztosít. A SLIP felhasználók úgy csatlakozhatnak egy helyi (LAN) vagy nagy távolságú (WAN) hálózathoz, hogy pont-pont kapcsolatot alakítanak ki egy olyan rendszerrel, amely tagja a hálózatnak.

A SLIP aszinkron kapcsolaton fut. A SLIP segítségével telefonos kapcsolatok alakíthatók ki az iSeries szervereken. A SLIP segítségével például egy számítógépről betárcsázhat az iSeries rendszerre. A kapcsolat kialakítása után a PC Telnet alkalmazásával csatlakozhat az iSeries Telnet szerveréhez. Vagy egy FTP alkalmazással fájlokat vihet át a két rendszer között.

Alapértelmezésben a rendszer nem tartalmaz SLIP konfigurációt. Ennek megfelelően ha nem kíván SLIP (és telefonos TCP/IP) protokollt használni a rendszeren, akkor egyszerűen ne állítson be SLIP konfigurációs profilokat. SLIP konfigurációkat egyébként a TCP/IP Pont-pont kezelése (WRKTCPPTP) paranccsal hozhat létre. A WRKTCPPTP parancs használatához *IOSYSCFG speciális jogosultság szükséges.

Ha a rendszeren tervezi a SLIP használatát, akkor ehhez SLIP (pont-pont) konfigurációs profilokat kell létrehoznia. A konfigurációs profilok kétféleképpen működhetnek:
- Hívásfogadás (*ANS)
- Hívás (*DIAL)

Az alábbi témakörök a SLIP kapcsolati profilok biztonságos beállítását írják le.

Megjegyzés: A **felhasználói profil** olyan iSeries szerver objektum, amely lehetővé teszi a bejelentkezést. Minden iSeries szerverjobnak rendelkeznie kell egy felhasználói profillal a futáshoz. A **konfigurációs profilok** tárolják az iSeries szerver SLIP kapcsolatának kialakításához szükséges információkat. SLIP kapcsolat létesítésekor egy összeköttetés jön létre az iSeries szerverrel. Bejelentkezésre és iSeries job indítására még nem került sor. Ennek megfelelően SLIP kapcsolat kialakításához nem feltétlenül kell felhasználói profillal rendelkeznie az iSeries szerveren. Az alábbiakból azonban ki fog derülni, hogy a SLIP konfigurációs profilnak is lehet szüksége felhasználói profilra, például a kapcsolat engedélyezésének megállapításához.

Behívó SLIP kapcsolatok felügyelete

Mielőtt valaki SLIP behívó kapcsolatot alakíthatna ki a rendszerrel, el kell indítani egy SLIP *ANS konfigurációs profilt. A SLIP konfigurációs profilok létrehozására és módosítására a TCP/IP Pont-pont kezelése (WRKTCPPTP) parancs használható. A konfigurációs profilok indítására a TCP/IP Pont-pont indítása (STRTCPPTP) parancs, vagy a WRKTCPPTP képernyő megfelelő menüpontja használható. A rendszer alapértelmezett beállításai szerint az STRTCPPTP és az ENDTCPPTP parancsok nyilvános jogosultsága *EXCLUDE. A SLIP konfigurációs profilok hozzáadásához, módosításához és törléséhez pedig *IOSYSCFG speciális jogosultság szükséges. A biztonsági adminisztrátornak a parancsra vonatkozó jogosultságok és a speciális jogosultságok segítségével pontosan meg kell határoznia, hogy ki engedélyezhet a rendszeren bejövő kapcsolatokat.

Behívó SLIP kapcsolatok biztonságosabbá tétele

Ha ellenőrizni kívánja a rendszert felhívó távoli rendszereket, akkor a kérést kiadó rendszernek felhasználói azonosítót és jelszót kell küldenie. A felhasználói azonosítót és a jelszót a helyi rendszer ellenőrzi. Ha a felhasználói azonosító vagy jelszó érvénytelen, akkor a rendszer visszautasíthatja a szekciókérést.

A behívás ellenőrzésének beállításához tegye a következőket:

__ Lépés 1. Hozzon létre egy felhasználói profilt, amelyet a távoli rendszer a kapcsolat létesítéséhez használhat. A rendszer által küldött felhasználói azonosítónak és jelszónak meg kell egyezni ezen profilnévvel és jelszóval.

Megjegyzés: Ahhoz, hogy a rendszer ellenőrizze a jelszavakat, a QSECURITY rendszerváltozót legalább 20-ra kell állítani.

A védelem kibővítéseként érdemes olyan felhasználói profilokat létrehozni, amelyeket csak SLIP kapcsolatok kialakításához használnak. A felhasználói profilok profilok a rendszeren csak korlátozott jogosultságokkal rendelkezzenek. Ha a profilokat kizárólag SLIP kapcsolatok kialakítására fogja használni, akkor a felhasználói profilokban érdemes beállítani a következő értékeket:
- Kezdeti menü (INLMNU): *SIGNOFF
- Kezdeti program (INLPGM): *NONE.
- Képességek korlátozása (LMTCPB): *YES

Ezek az értékek megakadályozzák a felhasználói profil interaktív bejelentkezését.

__ Lépés 2. Hozzon létre egy jogosultsági listát, amelyet a rendszer a SLIP kapcsolatok kialakításakor végzett ellenőrzéshez használ.

Megjegyzés: Ezt a jogosultsági listát a *Rendszer hozzáférési jogosultsági lista* mezőben kell megadni a SLIP profil létrehozásakor vagy módosításakor. (Lásd a lépés: 4 helyen leírtakat.)

__ Lépés 3. A Jogosultsági bejegyzés hozzáadása (ADDAUTLE) paranccsal adja hozzá a lépés: 1 helyen létrehozott felhasználói profilt a jogosultsági listához. Létrehozhat külön jogosultsági listát minden egyes pont-pont konfigurációs profilhoz, illetve a konfigurációs profilok meg is oszthatják a jogosultsági listákat.

__ Lépés 4. A WRKTCPPTP parancs segítségével állítson be egy TCP/IP pont-pont *ANS profilt a következőképpen:

- A konfigurációs profilnak felhasználó ellenőrzési funkciót tartalmazó kapcsolati párbeszéd parancsfájlt kell használnia. A felhasználó ellenőrzése a távoli fél által küldött felhasználói azonosító és jelszó átvételét és ellenőrzését jelenti. A rendszeren több minta párbeszéd parancsfájl is található, amely tartalmazza ezt a funkciót.
- A konfigurációs profilnak meg kell adnia a lépés: 2 helyen létrehozott jogosultsági lista nevét. A kapcsolati párbeszéd parancsfájl által fogadott felhasználói azonosítónak szerepelnie kell a jogosultsági listában.

Ne feledje, hogy a behívó kapcsolatok biztonságára hatással vannak a kapcsolatot kezdeményező távoli rendszerek biztonsági eljárásai és képességei is. Felhasználói azonosító és jelszó megkövetelésekor a kezdeményező rendszer kapcsolati párbeszéd parancsfájljának el kell küldenie a felhasználói azonosítót és jelszót. Bizonyos rendszerek, például az iSeries szerverek lehetővé teszik a felhasználói azonosítók és jelszavak biztonságos tárolását. (A módszert a “Kimenő szekciók biztonsága” oldalszám: 126 szakasz részletezi.) Más rendszerek a felhasználói azonosítót és jelszót a parancsfájlban tárolják, amely elképzelhető, hogy bárki számára hozzáférhető, csak a parancsfájl helyét kell ismernie.

A kommunikációs partnerek eltérő biztonsági gyakorlata és képességei miatt a különféle távoli környezetek számára érdemes eltérő konfigurációs profilokat létrehozni. Az STRTCPPTP paranccsal a rendszer beállítható oly módon, hogy egy szekciót csak egy adott konfigurációs profilnál fogadjon el. Megadható például, hogy bizonyos konfigurációs profilok csak a megadott időszakban indíthatnak szekciókat. A társított felhasználói profilok tevékenységének nyomon követéséhez érdemes beállítani a profilok biztonsági megfigyelését.

Behívó felhasználók megakadályozása más rendszerek elérésében

A rendszer és a hálózat konfigurációjától függően a SLIP kapcsolatot kialakító felhasználók képesek lehetnek arra, hogy a rendszerre való bejelentkezés nélkül csatlakozzanak a hálózat más rendszereihez. Vegyünk például egy felhasználót, aki SLIP kapcsolatot alakít ki a rendszerrel. Ezután FTP kapcsolatot építhet fel a hálózat egy másik rendszerével, amely nem teszi lehetővé a behívást.

A SLIP felhasználókat a hálózat más rendszereinek elérésében a konfigurációs profil *IP adatcsomag továbbítás engedélyezése* paraméterének Nem beállításával akadályozhatja meg. Ebben az esetben a felhasználó a rendszerre való bejelentkezés hiányában nem férhet hozzá a hálózathoz. Viszont miután a felhasználó sikeresen bejelentkezett a rendszerre, az adatcsomag továbbítás értékének nincs hatása. Nem korlátozza ugyanis a felhasználót abban, hogy az iSeries rendszeren található TCP/IP alkalmazások (például FTP vagy Telnet) segítségével kapcsolatba lépjen más rendszerekkel a hálózatban.

Kimenő szekciók felügyelete

Ahhoz, hogy a rendszeren kimenő SLIP kapcsolatot lehessen kialakítani, el kell indítani egy SLIP *DIAL konfigurációs profilt. A SLIP konfigurációs profilok létrehozására és módosítására a WRKTCPPTP parancs használható. A konfigurációs profilok indítására a TCP/IP Pont-pont indítása (STRTCPPTP) parancs, vagy a WRKTCPPTP képernyő megfelelő menüpontja használható. A rendszer alapértelmezett beállításai szerint az STRTCPPTP és az ENDTCPPTP parancsok nyilvános jogosultsága *EXCLUDE. A SLIP konfigurációs profilok hozzáadásához, módosításához és törléséhez pedig *IOSYSCFG speciális jogosultság szükséges. A biztonsági adminisztrátornak a parancsra vonatkozó jogosultságok és a speciális jogosultságok segítségével pontosan meg kell határoznia, hogy ki engedélyezhet a rendszeren kimenő kapcsolatokat.

Kimenő szekciók biztonsága

Az iSeries rendszer felhasználóinak elképzelhető, hogy szükségük van kimenő kapcsolatok kialakítására felhasználó hitelesítést igénylő rendszerekkel. Ebben az esetben az iSeries szerveren futó kapcsolati párbeszéd parancsfájlnak el kell küldenie egy felhasználói azonosítót és jelszót a távoli rendszerre. Az iSeries szerverek biztonságos módszert nyújtanak ezen jelszó tárolásához. A jelszót nem kell a kapcsolati párbeszéd parancsfájl részeként tárolni.

Megjegyzések:

1. Bár a kapcsolati jelszó tárolása titkosított formában történik, az elküldés előtt ezt vissza kell fejteni. A SLIP jelszavak, az FTP és Telnet jelszavakhoz hasonlóan titkosítás nélkül “sima szövegként” kerülnek elküldésre. Az FTP és Telnet jelszavaktól eltérően azonban a SLIP jelszavak még azelőtt kerülnek elküldésre, hogy a tényleges TCP/IP kapcsolat létrejönne a két rendszer között.

   Mivel a SLIP aszinkron módú pont-pont kapcsolatot használ, jelszó titkosítás nélküli formában küldése nem ugyanazt a biztonsági veszélyt hordozza magában, mint az FTP és Telnet jelszavak. A titkosítás nélküli FTP és Telnet jelszavak IP adatcsomagban haladnak a hálózaton, így ezeket le lehet hallgatni. A SLIP jelszó átvitele annyira biztonságos, mint a két rendszer közötti telefonos összeköttetés.
2. A SLIP kapcsolati párbeszéd parancsfájlok tárolása alapértelmezésben a QUSRSYS/QATOCPPSCR fájlban történik. A fájl nyilvános jogosultsága *USE, amely megakadályozza a nyilvános felhasználókat az alapértelmezett kapcsolati párbeszéd parancsfájlok módosításában.

Ellenőrzést igénylő távoli rendszerrel kialakított SLIP kapcsolat konfigurációs profiljának létrehozásához tegye a következőket:

__ Lépés 1. Győződjön meg róla, hogy a Szerver biztonsági adatok megtartása (QRETSVRSEC) rendszerváltozó értéke 1 (Igen). Ez a rendszerváltozó határozza meg, hogy engedélyezett-e a visszafejthető jelszavak tárolása a szerver egy védett területén.

__ Lépés 2. A WRKTCPPTP parancs segítségével állítson be egy konfigurációs profilt a következőképpen:

- A konfigurációs profil módjának adja meg a *DIAL értéket.
- A *Távoli szolgáltatás hozzáférési név* mezőbe írja be a távoli rendszer által várt felhasználói azonosítót. Ha például másik iSeries szerverhez csatlakozik, akkor adja meg a másik iSeries szerveren használt felhasználói profil nevét.
- A *Távoli szolgáltatás hozzáférési jelszó* mezőbe írja be a felhasználói azonosító jelszavát. A jelszó az iSeries szerver védett területén kerül tárolásra visszafejthető formában. A konfigurációs profilokhoz rendelt nevek és jelszavak a QTCP felhasználói profillal vannak társítva. A nevek

és jelszavak felhasználói parancsok és felületek számára nem hozzáférhetők. A jelszó információkat csak bejegyzett rendszerprogramok érhetik el.

Megjegyzés: Ne feledje, hogy a kapcsolati profilok jelszavai nem kerülnek mentésre a TCP/IP konfigurációs fájlok mentésekor. A SLIP jelszavak mentése érdekében a Biztonsági adatok mentése (SAVSECDTA) paranccsal mentse a QTCP felhasználói profilt.

- A kapcsolati párbeszéd parancsfájl paraméterben adjon meg egy olyan parancsfájlt, amely elküldi a felhasználói azonosítót és jelszót. A rendszeren több minta párbeszéd parancsfájl is található, amely tartalmazza ezt a funkciót. A rendszer a parancsfájl futtatásakor visszakeresi a jelszót, visszafejti, és elküldi a távoli rendszerre.

PPP biztonsági szempontok

A Pont-pont protokoll (PPP) a TCP/IP részeként áll rendelkezésre. A PPP a pont-pont összeköttetések ipari szabvány protokollja, amely a SLIP protokollhoz képest további többletfunkciókat biztosít.

A PPP segítségével az iSeries szerver nagy sebességű közvetlen kapcsolatokat alakíthat ki Internet szolgáltatókkal (ISP), illetve az intranet vagy extranet más rendszereivel. A távoli hálózatok valószerű behívó kapcsolatokat alakíthatnak ki a helyi iSeries szerverrel.

Ne feledje, hogy a PPP a SLIP protokollhoz hasonlóan hálózati kapcsolatot biztosít az iSeries szerver számára. A PPP kapcsolatok lényegében elvezetik a rendszer kapujához az ezt kérőket. A kérőnek ettől függetlenül még mindig meg kell adnia egy felhasználói azonosítót és jelszót a rendszerre való bejelentkezéshez, illetve a TCP/IP alkalmazások, például az FTP vagy Telnet használatához. Ne feledkezzen meg a PPP új kapcsolati lehetőségeivel kapcsolatos alábbi biztonsági szempontokról:

Megjegyzés: A PPP kapcsolatokat az IBM iSeries Access for Windows munkaállomásokon lehet beállítani az iSeries navigátor segítségével.

- A PPP lehetővé teszi dedikált kapcsolatok kialakítását, ahol ugyanaz a felhasználó mindig ugyanazzal az IP címmel rendelkezik. A dedikált címek elvileg könnyebbé teszik az IP cím hamisítás kihasználását. A PPP által biztosított kiterjesztett hitelesítési képességek azonban védelmet nyújtanak ez ellen.
- A PPP esetén a SLIP-hez hasonlóan szintén felhasználói névvel és társított jelszóval rendelkező kapcsolati profilokat kell létrehozni. A SLIP protokollal ellentétben azonban itt nincs szükség arra, hogy a felhasználónak érvényes felhasználói profilja és jelszava legyen. A felhasználónév és jelszó nem tartozik felhasználói profilhoz. A PPP hitelesítés ehelyett ellenőrzési listákat használ. A PPP emellett kapcsolati parancsfájlt sem igényel. A hitelesítés (vagyis a felhasználónév és jelszó feldolgozása) a PPP architektúra része, így alacsonyabb szinten történik a SLIP-nél.
- A PPP esetén lehetőség van CHAP használatára. A továbbiakban nem kell aggódnia a jelszavak lehallgatása miatt, mivel a CHAP titkosítja a felhasználóneveket és jelszavakat.

  A PPP kapcsolat csak akkor használ CHAP hitelesítést, ha azt mindkét fél támogatja. A rendszerek az egyeztetést a két modem közötti kommunikációt meghatározó jelcsere során végzik. Ha például a SYSTEMA támogatja a CHAP hitelesítést, a SYSTEMB viszont nem, akkor a SYSTEMA visszautasíthatja a kapcsolatot, vagy elfogadhatja titkosítás nélküli felhasználónév és jelszó használatát. A titkosítás nélküli felhasználónév és jelszó használatába való beleegyezést lefelé irányuló egyeztetésnek nevezzük. A lefelé irányuló egyeztetés beállítható lehetőség. A belső hálózaton például, ahol tudható, hogy az összes rendszer támogatja a CHAP használatát, a kapcsolati profilok beállíthatók oly módon, hogy

a lefelé irányuló egyeztetés ne legyen lehetséges. A kimenő hívást igénylő nyilvános kapcsolatok esetén elképzelhető, hogy szükség van lefelé irányuló egyeztetésre.

A PPP kapcsolati profilok lehetővé teszik érvényes IP címek meghatározását. Jelezheti például, hogy egy felhasználó számára egy adott címet vagy címtartományt vár. Ez a képesség a titkosított jelszavak használatának támogatásával hatékony védelmet nyújt az IP cím hamisítás ellen.

Az aktív szekciókkal szembeni hamisításos vagy ráültetéses támadások elleni védekezésként a PPP beállítható úgy, hogy megadott időközönként a hitelesítést ismételten végezze el. A PPP szekció során például az iSeries szerver megkérheti a távoli rendszert a felhasználónév és jelszó ismételt elküldésére. Ennek rendszeres időközönkénti végrehajtásával a rendszer meggyőződhet arról, hogy még mindig ugyanazzal a kapcsolati profillal kommunikál. (A végfelhasználónak az ismételt hitelesítéssel nem kell foglalkoznia. A felhasználónevek és jelszavak cseréje alacsonyabb szinten történik.)

A PPP segítségével megoldhatók az olyan konfigurációk, amikor távoli hálózatok az iSeries szerverre becsatlakozva kiterjesztett hálózatot alkotnak. Az ilyen környezetekben az IP továbbítás bekapcsolása valószínűleg követelmény. Az IP továbbítás elvileg lehetővé teszi a támadónak, hogy hálózatban mozogjon. A PPP erősebb védelme (például a jelszavak titkosítása és az IP címek ellenőrzése) ezt azonban megnehezíti. Kevésbé valószínű, hogy a behatoló egyáltalán képes hálózati kapcsolat kialakítására.

A PPP-ről további részleteket az iSeries Információs központból tudhat meg.

Rendszerbetöltési protokoll szerver biztonsági szempontok

A Rendszerbetöltési protokoll (BOOTP) dinamikus módszert biztosít a munkaállomások szerverekhez társítására, munkaállomás IP címek hozzárendelésére, illetve rendszerindító programbetöltés (IPL) források meghatározására.

A BOOTP olyan TCP/IP protokoll, amelynek segítségével az adathordozó nélküli munkaállomások lekérdhetik egy hálózati szerverről a rendszer indításához szükséges kódot. A BOOTP szerver a közismert 67-es porton figyel. A kliens kérésének fogadásakor a szerver kikeresi a kliens számára meghatározott IP címet, majd visszaadja a kliensnek az IP címet és a rendszerbetöltési fájl nevét. A kliens ezután TFTP kérést küld a szerverre a rendszerbetöltési fájl megszerzéséhez. A kliens hardvercíme és IP címe közötti leképezést a BOOTP tábla tartalmazza az iSeries szerveren.

BOOTP hozzáférés megakadályozása

Ha a hálózathoz nem csatlakoznak vékony kliensek, akkor a rendszeren nincs szükség BOOTP szerver futtatására. A protokoll használható ugyan más eszközökhöz is, ezeknél azonban az előnyben részesített megoldás a DHCP használata. A BOOTP szerver futásának megakadályozásához tegye a következőket:

__ Lépés 1. Ha meg kívánja akadályozni a BOOTP szerverjobok elindítását a TCP/IP indításakor, akkor írja be a következő parancsot:

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

Megjegyzések:

a. Az alapértelmezett érték az AUTOSTART(*NO).

b. Az automatikusan induló TCP/IP szerverek beállításával kapcsolatban további információkat az “Automatikusan induló TCP/IP szerverek meghatározása” oldalszám: 122 szakaszban talál.

__ Lépés 2. Ha meg kívánja akadályozni, hogy valaki felhasználói alkalmazást, például egy socket alkalmazást futtasson azon a porton, amelyet általában a BOOTP használ, akkor tegye a következőket:

Megjegyzés: Mivel a DHCP és a BOOTP azonos portszámot használ, ezzel a DHCP port használatát is megtiltja. Ne korlátozza a portot, ha DHCP használatát tervezi.

__ Lépés a. Írja be a GO CFGTCP parancsot a TCP/IP beállítása menü megjelenítéséhez.

__ Lépés b. Válassza a 4. menüpontot (TCP/IP port korlátozások kezelése).

__ Lépés c. A TCP/IP port korlátozások kezelése képernyőn válassza az 1. lehetőséget (Hozzáadás).

__ Lépés d. A porttartomány kezdetének adja meg a 67-es portot.

__ Lépés e. A porttartomány végének adja meg az *ONLY értéket.

Megjegyzések:

1) A port korlátozás a TCP/IP következő újraindításakor lép életbe. Ha a TCP/IP aktív a port korlátozások beállításakor, akkor be kell fejezni a TCP/IP-t, és újra kell indítani.
2) Az általános portszám hozzárendeléseket az RFC1700 írja le.

__ Lépés f. A protokollnak adja meg az *UDP értéket.

__ Lépés g. A felhasználói profil mezőben védett felhasználói profil nevet kell megadni. (A védett felhasználói profilok olyan profilok, amelyek nem birtokolnak jogosultságot átvevő programokat, és nem rendelkeznek más felhasználók számára ismert jelszavakkal.) A portnak egy adott felhasználóra korlátozásával automatikusan kizár minden más felhasználót.

BOOTP szerver biztonságosabbá tétele

A BOOTP szerver nem biztosít közvetlen hozzáférést az iSeries rendszerhez, ezért csak korlátozott biztonsági kockázatot képvisel. A biztonsági adminisztrátornak elsősorban a megfelelő információknak a megfelelő vékony klienshez rendelését kell biztosítania. Más szavakkal meg kell akadályozni, hogy egy bajkeverő a BOOTP tábla módosításával működésképtelenné tegye a vékony klienseket.

A BOOTP szerver és a BOOTP tábla kezeléséhez *IOSYSCFG speciális jogosultság szükséges. A rendszer *IOSYSCFG speciális jogosultsággal rendelkező felhasználói profiljait gondosan meg kell válogatni.

DHCP szerver biztonsági szempontok

A Dinamikus hoszt konfigurációs protokoll (DHCP) a TCP/IP hálózati hosztok konfigurációs információinak átadására biztosít egy keretrendszert. A kliens munkaállomások számára a DHCP az automatikus konfigurációhoz hasonló szolgáltatást nyújt. A kliens munkaállomás DHCP programja egy üzenet küldésével kéri a konfigurációs információkat. Az iSeries rendszeren futó DHCP szerver a kliens munkaállomás által a TCP/IP megfelelő beállításához igényelt információk elküldésével válaszol az kérésre.

A DHCP segítségével leegyszerűsíthető az iSeries szerverre való csatlakozás. Ez azért lehetséges, mert ilyenkor a felhasználóknak nem kell megadniuk a TCP/IP konfigurációs információkat. A DHCP emellett használható az alhálózatban szükséges belső TCP/IP címek számának csökkentésére. A DHCP szerver az IP címtárolóból ideiglenesen osztja ki az IP címeket az aktív felhasználóknak.

Vékony kliensekhez a BOOTP helyett DHCP is használható. A DHCP a BOOTP szerverhez képest több funkciót biztosít, mivel ez a vékony kliensek mellett személyi számítógépek dinamikus konfigurációját is támogatja.

DHCP hozzáférés megakadályozása

Ha *nem* kíván DHCP szervert használni a rendszeren, akkor tegye a következőket:

1. Ha meg kívánja akadályozni a DHCP szerverjobok elindítását a TCP/IP indításakor, akkor írja be a következő parancsot:

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

   Megjegyzések:

   a. Az alapértelmezett érték az AUTOSTART(*NO).

   b. Az automatikusan induló TCP/IP szerverek beállításával kapcsolatban további információkat az “Automatikusan induló TCP/IP szerverek meghatározása” oldalszám: 122 szakaszban talál.

2. Ha meg kívánja akadályozni, hogy valaki felhasználói alkalmazást, például egy socket alkalmazást futtasson azon a porton, amelyet általában a DHCP használ, akkor tegye a következőket:

   a. Írja be a GO CFGTCP parancsot a TCP/IP beállítása menü megjelenítéséhez.

   b. Válassza a 4. menüpontot (TCP/IP port korlátozások kezelése).

   c. A TCP/IP port korlátozások kezelése képernyőn válassza az 1. lehetőséget (Hozzáadás).

   d. A porttartomány kezdetének adja meg a 67-es portot.

   e. A porttartomány végének adja meg a 68-as portot.

      Megjegyzések:

      1) A port korlátozás a TCP/IP következő újraindításakor lép életbe. Ha a TCP/IP aktív a port korlátozások beállításakor, akkor be kell fejezni a TCP/IP-t, és újra kell indítani.

      2) Az általános portszám hozzárendeléseket az RFC1700 írja le.

   f. A protokollnak adja meg az *UDP értéket.

   g. A felhasználói profil mezőben védett felhasználói profil nevet kell megadni. (A védett felhasználói profilok olyan profilok, amelyek nem birtokolnak jogosultságot átvevő programokat, és nem rendelkeznek más felhasználók számára ismert jelszavakkal.) A portnak egy adott felhasználóra korlátozásával automatikusan kizár minden más felhasználót.

DHCP szerver biztonságosabbá tétele

Ha az iSeries rendszeren DHCP szervert kíván futtatni, akkor tartsa szem előtt az alábbi biztonsági szempontokat:

- Korlátozza a DHCP felügyeletére jogosult felhasználók számát. A DHCP felügyelete a következő jogosultságokat igényli:
  - *IOSYSCFG speciális jogosultság
  - *RW jogosultság a következő fájlokhoz:

    ```
    /QIBM/UserData/OS400/DHCP/dhcpsd.cfg
    /QIBM/UserData/OS400/DHCP/dhcprd.cfg
    ```

- Értékelje ki a LAN fizikai elérhetőségét. Mennyire egyszerűen oldható meg egy kívülálló számára, hogy besétáljon az épületbe, és csatlakoztassa a laptopját a hálózathoz? Az ehhez hasonló biztonsági kockázatok elkerülése érdekében a DHCP lehetővé teszi a támogatott kliensek (hardvercímek) listájának összeírását. A szolgáltatás használata esetén a DHCP szerver által a hálózati adminisztrátorok számára biztosított kényelmi funkciók egy része is megszűnik. Ily módon megakadályozható viszont az ismeretlen munkaállomások konfigurálása.

- Lehetőség szerint újrafelhasználható (Interneten nem továbbított) IP címkészletet használjon. Ez segít megakadályozni azt, hogy a hálózaton kívüli munkaállomások használható konfigurációs információkhoz jussanak a szervertől.
- További biztonsági igények esetén használja ki a DHCP kilépési pontokat. A kilépési pontok és ezek képességeinek leírását az alábbiakban találja. A kilépési pontok használatát az *iSeries System API Reference* című kiadvány tárgyalja.

  Port belépés
  A rendszer ezt a végprogramot hívja meg minden egyes alkalommal, amikor beolvas egy adatcsomagot a 67-es (DHCP) portról. A végprogram a teljes adatcsomagot megkapja. Eldöntheti, hogy a rendszernek fel kell dolgoznia vagy el kell dobnia a csomagot. A kilépési pont akkor használható, ha a meglévő DHCP szűrési szolgáltatások nem elegendők.

  Cím hozzárendelés
  A rendszer ezt a végprogramot hívja meg minden egyes alkalommal, amikor a DHCP hozzárendel egy címet egy klienshez.

  Cím felszabadítás
  A rendszer ezt a végprogramot hívja meg minden egyes alkalommal, amikor a DHCP felszabadítja egy kliens címét.

TFTP szerver biztonsági szempontok

Az Egyszerű fájlátviteli protokoll (TFTP) felhasználói hitelesítés nélküli, alapszintű fájlátviteli funkciókat biztosít. A TFTP általában a Rendszerbetöltési protokolllal (BOOTP) vagy a Dinamikus hoszt konfigurációs protokolllal (DHCP) karöltve nyújt támogatást.

A kliens először a BOOTP vagy DHCP szerverrel veszi fel a kapcsolatot. A BOOTP vagy DHCP szerver a kliens IP címével és a rendszerbetöltési fájl nevével válaszol. A kliens ezután TFTP kérést küld a szerverre a rendszerbetöltési fájl megszerzéséhez. A kliens a rendszerbetöltési fájl letöltése után befejezi a TFTP kapcsolatot.

TFTP hozzáférés megakadályozása

Ha a hálózathoz nem csatlakoznak vékony kliensek, akkor a rendszeren valószínűleg nincs szükség TFTP szerver futtatására. A TFTP szerver futásának megakadályozásához tegye a következőket:

__ Lépés 1. Ha meg kívánja akadályozni a TFTP szerverjobok elindítását a TCP/IP indításakor, akkor írja be a következő parancsot:

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

Megjegyzések:

a. Az alapértelmezett érték az AUTOSTART(*NO).

b. Az automatikusan induló TCP/IP szerverek beállításával kapcsolatban további információkat az “Automatikusan induló TCP/IP szerverek meghatározása” oldalszám: 122 szakaszban talál.

__ Lépés 2. Ha meg kívánja akadályozni, hogy valaki felhasználói alkalmazást, például egy socket alkalmazást futtasson azon a porton, amelyet általában a TFTP használ, akkor tegye a következőket:

__ Lépés a. Írja be a GO CFGTCP parancsot a TCP/IP beállítása menü megjelenítéséhez.

__ Lépés b. Válassza a 4. menüpontot (TCP/IP port korlátozások kezelése).

__ Lépés c. A TCP/IP port korlátozások kezelése képernyőn válassza az 1. lehetőséget (Hozzáadás).

__ Lépés d. A porttartomány kezdetének adja meg a 69-es portot.

__ Lépés e. A porttartomány végének adja meg az *ONLY értéket.

Megjegyzések:

1) A port korlátozás a TCP/IP következő újraindításakor lép életbe. Ha a TCP/IP aktív a port korlátozások beállításakor, akkor be kell fejezni a TCP/IP-t, és újra kell indítani.
2) Az általános portszám hozzárendeléseket az RFC1700 írja le.

__ Lépés f. A protokollnak adja meg az *UDP értéket.

__ Lépés g. A felhasználói profil mezőben védett felhasználói profil nevet kell megadni. (A védett felhasználói profilok olyan profilok, amelyek nem birtokolnak jogosultságot átvevő programokat, és nem rendelkeznek más felhasználók számára ismert jelszavakkal.) A portnak egy adott felhasználóra korlátozásával automatikusan kizár minden más felhasználót.

TFTP szerver biztonságosabbá tétele

A TFTP szerver alapértelmezésben rendkívül korlátozott hozzáférést biztosít az iSeries szerverhez. Kifejezetten úgy van beállítva, hogy csak a vékony kliensek rendszerbetöltési kódját biztosítsa. A biztonsági adminisztrátornak mindazonáltal tisztában kell lennie a TFTP szerver következő jellemzőivel:

- A TFTP szerver nem igényel hitelesítést, vagyis felhasználói azonosítót és jelszót. Minden TFTP job a QTFTP felhasználói profil alatt fut. A QTFTP felhasználói profil nem rendelkezik jelszóval. Ennek megfelelően nem használható interaktív bejelentkezéshez. A QTFTP felhasználói profil nem rendelkezik speciális jogosultságokkal, és rendszererőforrásokra vonatkozó kifejezett jogosultságokkal. A vékony kliensek számára kiszolgált erőforrások eléréséhez nyilvános jogosultságot használ.
- A TFTP szerver az alapértelmezett beállítások szerint a vékony kliensekre vonatkozó információkat tartalmazó katalógushoz fér hozzá. A katalógusnak *PUBLIC jogosultsággal kell rendelkeznie, vagy a QTFTP profilt fel kell jogosítani a katalógus olvasására és írására. A katalógus írásához a CHGTFTPA parancsban a Fájl írások engedélyezése paraméternek a *CREATE értéket kell megadni. Meglévő fájl írásához a Fájl írások engedélyezése paraméterben a *REPLACE értéket kell választani. A *CREATE lehetővé teszi a meglévő fájlok felülírását és új fájlok létrehozását. A *REPLACE csak meglévő fájlok felülírását engedélyezi.

  A TFTP kliensek nem férhetnek hozzá más katalógushoz, kivéve, ha ezt kifejezetten megadja a TFTP attribútumok módosítása (CHGTFTPA) paranccsal. Ennek megfelelően ha egy helyi vagy távoli felhasználó TFTP szekciót kezdeményez a rendszerrel, akkor a felhasználó csak korlátozott mértékben képes információk elérésére és károk okozására.
- Ha úgy dönt, hogy a TFTP szervert a vékony kliensek kezelésén kívül más szolgáltatások biztosítására is beállítja, akkor a TFTP kérések kiértékelésére és hitelesítésére megadhat egy végprogramot. A TFTP szerver az FTP szerveren biztosítotthoz hasonló kilépési pontot nyújt a kérések ellenőrzéséhez. További részleteket az iSeries Információs központ Hálózatok → TCP/IP → TFTP című témakörében talál. Az iSeries Információs központ elérésével kapcsolatban nézze meg az “Előfeltétel és kapcsolódó információk” oldalszám: xii szakaszt.

REXEC szerver biztonsági szempontok

A Távoli végrehajtási szerver (REXEC) REXEC kliensek parancsait fogadja és futtatja le. A REXEC kliensek általában olyan PC vagy UNIX alkalmazások, amelyek támogatják REXEC parancsok küldését. A szerver által nyújtott támogatás hasonló az FTP szervereken használható RCMD (Távoli parancs) részparancs képességeihez.

REXEC hozzáférés megakadályozása

Ha nem szeretné, hogy az iSeries szerver parancsokat fogadjon a REXEC kliensektől, akkor a következő intézkedésekkel akadályozza meg a REXEC szerver futását:

__ Lépés 1. Ha meg kívánja akadályozni a REXEC szerverjobok elindítását a TCP/IP indításakor, akkor írja be a következő parancsot:

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

Megjegyzések:

a. Az alapértelmezett érték az AUTOSTART(*NO).

b. Az automatikusan induló TCP/IP szerverek beállításával kapcsolatban további információkat az “Automatikusan induló TCP/IP szerverek meghatározása” oldalszám: 122 szakaszban talál.

__ Lépés 2. Ha meg kívánja akadályozni, hogy valaki felhasználói alkalmazást, például egy socket alkalmazást futtasson azon a porton, amelyet általában a REXEC használ, akkor tegye a következőket:

__ Lépés a. Írja be a GO CFGTCP parancsot a TCP/IP beállítása menü megjelenítéséhez.

__ Lépés b. Válassza a 4. menüpontot (TCP/IP port korlátozások kezelése).

__ Lépés c. A TCP/IP port korlátozások kezelése képernyőn válassza az 1. lehetőséget (Hozzáadás).

__ Lépés d. A porttartomány kezdetének adja meg az 512-es portot.

__ Lépés e. A porttartomány végének adja meg az *ONLY értéket.

__ Lépés f. A protokollnak adja meg a *TCP értéket.

__ Lépés g. A felhasználói profil mezőben védett felhasználói profil nevet kell megadni. (A védett felhasználói profilok olyan profilok, amelyek nem birtokolnak jogosultságot átvevő programokat, és nem rendelkeznek más felhasználók számára ismert jelszavakkal.) A portnak egy adott felhasználóra korlátozásával automatikusan kizár minden más felhasználót.

Megjegyzések:

a. A port korlátozás a TCP/IP következő újraindításakor lép életbe. Ha a TCP/IP aktív a port korlátozások beállításakor, akkor be kell fejezni a TCP/IP-t, és újra kell indítani.

b. Az általános portszám hozzárendeléseket az RFC1700 írja le.

REXEC szerver biztonságosabbá tétele

Ha a rendszeren Távoli végrehajtási szerver szervert kíván futtatni, akkor tartsa szem előtt az alábbi biztonsági szempontokat:

- A REXCD kérésekben egy felhasználói azonosító, egy jelszó és a futtatandó parancs található. A végrehajtásra az iSeries szerver szokásos hitelesítési eljárásai és jogosultságai vonatkoznak:
  - A felhasználói profil és jelszó kombinációjának érvényesnek kell lennie.
  - A rendszer foganatosítja a felhasználói profil *Képességek korlátozása* (LMTCPB) paraméterének értékét.
  - A felhasználónak megfelelő jogosultsággal kell rendelkeznie a parancshoz, illetve a parancs által használt valamennyi erőforráshoz.
- A REXEC szerver az FTP szerverhez hasonló kilépési pontokat biztosít. Az ellenőrzés kilépési ponttal a parancs kiértékelhető, és eldönthető, hogy futtatása engedélyezett legyen-e. További részleteket az iSeries Információs központ Hálózatok → TCP/IP →

REXEC című témakörében talál. Az iSeries Információs központ elérésével kapcsolatban nézze meg az “Előfeltétel és kapcsolódó információk” oldalszám: xii szakaszt.

- REXEC szerver futtatásakor tartsa szem előtt, hogy a parancsok futtatására a menü hozzáférés felügyelet nem vonatkozik. Ennek megfelelően biztosítani kell, hogy az objektum jogosultsági séma megfelelően védi az erőforrásokat.

RouteD biztonsági szempontok

Az Útvonal démon (RouteD) szerver Útválasztási információs protokoll (RIP) támogatást biztosít az iSeries szervereken. A RIP a legáltalánosabban használt útvonalkezelési protokoll. Ez egy olyan belső átjáró protokoll, amely a TCP/IP számára nyújt segítséget az IP csomagok továbbításához az autonóm rendszereken.

A RouteD a hálózati forgalom hatékonyabbá tételére szolgál azáltal, hogy lehetővé teszi a megbízható hálózatok rendszereinek egymás frissítését az aktuális útvonalkezelési információkkal. A RouteD futtatásakor a rendszert más részvevő rendszerek frissíthetik az átvitelek (csomagok) útválasztására vonatkozó információkkal. Ezáltal ha a RouteD szerver elérhető egy cracker számára, akkor a cracker felhasználhatja arra, hogy a csomagokat egy másik rendszerre irányítsa lehallgatás vagy módosítás céljából. Néhány javaslat a RouteD biztonságával kapcsolatban:

- Az iSeries szerverek a RIP 1. változatát használják, amely semmilyen módszert nem biztosít az útválasztók hitelesítésére. Ezt csak megbízható hálózatban szabad használni. Ha a rendszer ″nem megbízható″ rendszereket is tartalmazó hálózat része, akkor ne használja a RouteD szervert. A RouteD szerver automatikus indításának megakadályozásához írja be a következő parancsot:

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

  Megjegyzések:

  1. Az alapértelmezett érték az AUTOSTART(*NO).
  2. Az automatikusan induló TCP/IP szerverek beállításával kapcsolatban további információkat az “Automatikusan induló TCP/IP szerverek meghatározása” oldalszám: 122 szakaszban talál.
- A RouteD konfiguráció módosítására vonatkozó jogosultságot (*IOSYSCFG speciális jogosultság) érdemes szűk körben biztosítani.
- Ha a rendszer egynél több hálózatnak része (például egy intranet és az Internet), akkor a RouteD szerver beállítható úgy, hogy csak a biztonságos hálózatból fogadjon frissítéseket.

DNS szerver biztonsági szempontok

A Tartománynév rendszer (DNS) szerver fordítja le a hosztneveket IP címmé és vissza. Az iSeries rendszerek DNS szervere belső, biztonságos hálózatok (intranetek) cím fordítására készült.

DNS hozzáférés megakadályozása

Ha *nem* kíván DNS szervert használni a rendszeren, akkor tegye a következőket:

1. Ha meg kívánja akadályozni a DNS szerverjobok elindítását a TCP/IP indításakor, akkor írja be a következő parancsot:

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

   Megjegyzések:

   a. Az alapértelmezett érték az AUTOSTART(*NO).
   b. Az automatikusan induló TCP/IP szerverek beállításával kapcsolatban további információkat az “Automatikusan induló TCP/IP szerverek meghatározása” oldalszám: 122 szakaszban talál.

2. Ha meg kívánja akadályozni, hogy valaki felhasználói alkalmazást, például egy socket alkalmazást futtasson azon a porton, amelyet általában a DNS használ, akkor tegye a következőket:
   a. Írja be a GO CFGTCP parancsot a TCP/IP beállítása menü megjelenítéséhez.
   b. Válassza a 4. menüpontot (TCP/IP port korlátozások kezelése).
   c. A TCP/IP port korlátozások kezelése képernyőn válassza az 1. lehetőséget (Hozzáadás).
   d. A porttartomány kezdetének adja meg az 53-as portot.
   e. A porttartomány végének adja meg az *ONLY értéket.

      Megjegyzések:

      1) A port korlátozás a TCP/IP következő újraindításakor lép életbe. Ha a TCP/IP aktív a port korlátozások beállításakor, akkor be kell fejezni a TCP/IP-t, és újra kell indítani.
      2) Az általános portszám hozzárendeléseket az RFC1700 írja le.

   f. A protokollnak adja meg a *TCP értéket.
   g. A felhasználói profil mezőben védett felhasználói profil nevet kell megadni. (A védett felhasználói profilok olyan profilok, amelyek nem birtokolnak jogosultságot átvevő programokat, és nem rendelkeznek más felhasználók számára ismert jelszavakkal.) A portnak egy adott felhasználóra korlátozásával automatikusan kizár minden más felhasználót.
   h. Ismételje meg a fenti lépéseket (2c - 2g) még egyszer azzal a különbséggel, hogy *UDP protokollt határoz meg.

DNS szerver biztonságosabbá tétele

Ha az iSeries rendszeren DNS szervert kíván futtatni, akkor tartsa szem előtt az alábbi biztonsági szempontokat:

- A DNS szerver IP cím és név fordítási funkciókat biztosít. Az iSeries rendszer semmilyen objektumához nem biztosít hozzáférést. A DNS szerverhez hozzáférő külső felhasználó veszélye, hogy egyszerűen alkothat képet a belső hálózat felépítéséről. A DNS szerverrel a cracker időt takaríthat meg a lehetséges célpontok címeinek meghatározásakor. A DNS mindazonáltal semmiféle információt nem biztosít, amely bármilyen módon megkönnyítené ezen célrendszerek feltörését.
- Az iSeries DNS szerver általában intraneten kerül felhasználásra. Ennek megfelelően valószínűleg nincs szükség a DNS lekérdezés képességének korlátozására. Az intranet azonban tartalmazhat több alhálózatot is. Elképzelhető, hogy más alhálózatok felhasználóinak nem kívánja engedélyezni az iSeries rendszeren futó DNS szerver lekérdezését. A DNS egyik biztonsági lehetőségével a hozzáférés korlátozható egy elsődleges tartományra. A DNS szerver által kiszolgált IP címeket az iSeries navigátorban állíthatja be.

  Egy másik biztonsági beállítással meghatározhatja, hogy milyen másodlagos szerverek másolhatják le az elsődleges DNS szerver információit. A beállítás használata esetén a DNS szerver csak a kifejezetten felsorolt másodlagos szerverek által küldött zónaátviteli (információmásolási) kéréseket fogadja el.
- A DNS szerver konfigurációs fájljának módosítását gondosan le kell korlátozni. Ennek hiányában például egy rossz szándékú felhasználó ″megmérgezheti″ a DNS fájlt, hogy az egy másik, például hálózaton kívüli IP címre mutasson. Az adott hamis címen egy hálózaton belüli szerver szimulálásával pedig elképzelhető, hogy bizalmas információkhoz juthatnak a szerverről.

iSeries HTTP szerver biztonsági szempontok

A HTTP szerver lehetőséget ad a web böngésző klienseknek az iSeries szerveren tárolt multimédia objektumok, például HTML fájlok elérésére. Támogatja emellett a *Common Gateway Interface (CGI)* specifikációkat. Az alkalmazásprogramozók CGI programok írásával kibővíthetik a szerver funkcionalitását.

Az adminisztrátor az Internet Connection Server vagy az IBM HTTP Server for iSeries felhasználásával több szervert is futtathat egyszerre ugyanazon az iSeries rendszeren. Az ilyen szervereket **szerver példányoknak** nevezzük. Minden szerver példány egyedi névvel rendelkezik. Az elinduló példányokat, illetve az egyes példányok által végrehajtható tevékenységeket az adminisztrátor határozza meg.

Megjegyzés: A következők web böngészőből végzett beállításához vagy felügyeletéhez futnia kell a HTTP szerver *ADMIN példányának:

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

A felhasználók, vagyis a webhelyek látogatói sohasem találkoznak iSeries bejelentkezési képernyővel. Az iSeries szerver adminisztrátorának ettől függetlenül különféle HTTP direktívákkal kifejezetten meg kell adnia ezen felhasználók jogosultságait a HTML dokumentumok és CGI programok vonatkozásában. Emellett az adminisztrátor beállíthat erőforrás biztonságot és felhasználói hitelesítést (felhasználói azonosító és jelszó) a kérések egy részénél.

A támadások a webszerver szolgáltatásának megbénítását eredményezhetik. A szerver a szolgáltatás megbénítására irányuló támadásokat bizonyos kliens kérések időkorlátjának kimérésével ismeri fel. Ha a szerver nem kap kérést a klienstől, akkor a felismeri, hogy szolgáltatás megbénítási támadás van ellene folyamatban. Ez a szerver kezdeti kapcsolatának kialakítása után történik. A szerver alapértelmezésben felismeri a támadást, és reagál is rá.

HTTP hozzáférés megakadályozása

Ha *nem szeretné*, hogy programmal bárki is hozzáférjen a rendszerhez, akkor meg kell akadályozni a HTTP szerver elindítását. Tegye a következőket:

__ Lépés 1. Ha meg kívánja akadályozni a HTTP szerverjobok elindítását a TCP/IP indításakor, akkor írja be a következő parancsot:

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

Megjegyzések:

a. Az alapértelmezett érték az AUTOSTART(*NO).

b. Az automatikusan induló TCP/IP szerverek beállításával kapcsolatban további információkat az “Automatikusan induló TCP/IP szerverek meghatározása” oldalszám: 122 szakaszban talál.

__ Lépés 2. A HTTP szerver alapértelmezésben a QTMHHTTP felhasználói profilt használja. A HTTP szerver indításának megakadályozásához tiltsa le a QTMHHTTP felhasználói profilt.

HTTP szerver elérésének felügyelete

A HTTP szerver elsődleges célja az iSeries rendszeren lévő webhelyek kiszolgálása a látogatók számára. A webhelyekre ellátogató felhasználókat valahogy úgy lehet tekinteni, mint a szaklapok hirdetéseit böngésző személyeket. A látogató nem ismeri a webhelyet futtató

hardver és szoftvert, például a szerver típusát és annak tényleges fizikai helyét. A potenciális látogatók és a webhely közé általában nem szokás semmiféle korlátot (például bejelentkezési képernyőt) helyezni. Ettől függetlenül elképzelhető, hogy a webhely bizonyos dokumentumainak vagy CGI programjainak használatát korlátozni kell.

Az iSeries rendszerek általában több logikai webhelyet is kiszolgálnak. Elképzelhető például, hogy az iSeries rendszert a vállalat több üzletága is használja, amelyek más és más információkat biztosítanak az ügyfelek számára. A vállalat valamennyi üzletága rendelkezhet a látogató számára teljesen függetlennek tűnő egyedi webhellyel. Emellett elképzelhető, hogy bizalmas vállalati információkat tartalmazó belső (intranetes) webhelyeket is ki kíván szolgálni.

A biztonsági adminisztrátornak egyfelől meg kell védenie a webhely tartalmát, másfelől biztosítania kell, hogy a biztonsági módszerek nincsenek káros hatással a webhely értékére. Mindemellett biztosítania kell kell, hogy a HTTP tevékenység ne jelentsen fenyegetést a rendszer és a hálózat biztonságára vonatkozóan. A soron következő témakörök adnak biztonsági tanácsokat a program használatával kapcsolatban.

Adminisztrációs szempontok

Az Internet szerver adminisztrálásának van néhány biztonsági vonzata.

- A beállítási és konfigurációs funkciók végrehajtásához egy web böngésző és az *ADMIN példány szükséges. Bizonyos funkciókhoz, például további szerver példányok létrehozásához az *ADMIN szervert *kell* használni.
- Az adminisztrációs honlap (vagyis az *ADMIN szerver honlapjának) alapértelmezett URL címe a böngésző alapú adminisztrációs funkciókat biztosító termékek dokumentációjában nyilvánosan elérhető. Ennek megfelelően betörők valószínűleg ismerik az URL-t, ugyanúgy, ahogy az IBM által szállított felhasználói profilok alapértelmezett jelszava is közzé van téve különböző cracker fórumokon. Ezen kockázattal szemben a rendszert többféleképpen is megvédheti:
  - A HTTP szerver *ADMIN példányát csak akkor futtassa, amikor adminisztrációs funkciók végrehajtásához erre szükség van. Ne futtassa folyamatosan az *ADMIN példányt.
  - A Digitális igazolás kezelő segítségével aktiválja az *ADMIN példány SSL támogatását. Az *ADMIN példány HTTP védelmi direktívák felhasználásával felhasználói azonosító és jelszó megadását igényli. SSL használata esetén a felhasználói azonosító és jelszó (az adminisztrációs űrlapokon megadott konfigurációs információkkal egyetemben) titkosított formában kerül továbbításra.
  - Tűzfal használatával tiltsa le az *ADMIN szerver elérését az Internet felől, illetve rejtse el az eléréshez szükséges URL címben található rendszer- és tartományneveket.
- Adminisztrációs funkciók végrehajtásakor *IOSYSCFG speciális jogosultsággal rendelkező felhasználói profillal kell bejelentkezni. Emellett rendelkezni kell a megfelelő jogosultságokkal a rendszer különféle objektumaihoz, például a következőkhöz:
  - A HTML dokumentumokat és CGI programokat tároló könyvtárak és katalógusok.
  - A szerver direktíváiban felhasználni kívánt felhasználói profilok.
  - A direktívák által használt katalógusok hozzáférés felügyeleti listái.
  - Ellenőrzési lista a felhasználói azonosítók és jelszavak létrehozásához és karbantartásához.

  Az *ADMIN szerver és a Telnet is lehetővé teszi adminisztrációs funkciók távoli végrehajtását, akár egy internetes kapcsolaton keresztül is. Legyen figyelemmel arra, hogy a nyilvános összeköttetésen (például az Interneten) keresztül végzett adminisztráció során ″erős″ felhasználói azonosítók és jelszavak hallgathatók le. A lehallgató a felhasználói azonosítók és jelszavak használatával megkísérelheti a rendszerre való bejutást például Telnet vagy FTP segítségével.

Megjegyzések:

1. A Telnet esetén a bejelentkezési képernyő kezelése ugyanúgy történik, mint bármely más képernyőé. Bár a jelszó a beíráskor nem jelenik meg, a rendszer mindenfajta titkosítás és kódolás nélkül továbbítja azt.
2. Az *ADMIN szerver esetén a jelszó kódolt, de nem titkosított. A kódolási séma ipari szabvány, tehát a cracker közösségek is jól ismerik. Bár a kódolás védelmet nyújt a kezdő ″hallgatózók″ ellen, a tapasztaltabbak minden valószínűség szerint rendelkeznek a jelszó dekódolásához szükséges eszközökkel.

Biztonsági tipp

Ha Internet feletti távoli adminisztráció használatát tervezi, akkor az adatforgalom titkosítása érdekében az *ADMIN példányt SSL támogatással kell használni. Ne használjon nem biztonságos alkalmazásokat, például V4R4 előtti Telnetet. (A Telnet SSL támogatása a V4R4 kiadásban jelent meg.) Ha az *ADMIN szervert *megbízható* felhasználókból álló intraneten keresztül használja, akkor elképzelhető, hogy további intézkedésekre nincs szükség.

- A szerveren végbemenő tevékenységek alapját a HTTP direktívák biztosítják. A rendszer kezdeti alapértelmezései egy alapértelmezett üdvözlet oldal kiszolgálását jelentik. A kliensek az üdvözlet oldalon kívül semmilyen más dokumentumot nem tekinthetnek meg, amíg az adminisztrátor be nem állítja a szerver direktíváit. A direktívák meghatározásához használja az *ADMIN szervert egy böngészővel, vagy futtassa a HTTP konfiguráció kezelése (WRKHTTPCFG) parancsot. Mindkét módszer *IOSYSCFG speciális jogosultságot igényel. Az iSeries szerver Internetre csatlakoztatásakor különösen kritikus az *IOSYSCFG speciális jogosultsággal rendelkező felhasználók erre vonatkozó igényének kiértékelése, és a felhasználók nyomon követése.

Erőforrások védelme

Az IBM HTTP Server for iSeries HTTP direktíváival részletesen szabályozható a szerver információs tulajdonához való hozzáférés. A direktívák segítségével megadhatók a webszerver által a HTML fájlok és CGI programok kiszolgálásához használt katalógusok, beállítható, hogy a szerver más felhasználói profil alatt fusson, illetve hitelesítés követelhető meg bizonyos erőforrások esetén.

Megjegyzés: A rendelkezésre álló HTTP direktívákat, illetve ezek használatát az Információs központ Web kiszolgálás témaköre sorolja fel. Néhány javaslat és szempont a támogatás használatával kapcsolatban:

- A HTTP szerver ″kifejezett jogosultsági″ alapon működik. A szerver csak a direktívákban kifejezetten megadott kéréseket fogadja el. Másként fogalmazva a szerver azonnal visszautasít minden URL kérést, kivéve, ha az URL-t a direktívák (akár névvel, akár általánosan) meghatározzák.
- A biztonsági direktívák segítségével bizonyos erőforrásokra vonatkozó kérések kiszolgálása előtt felhasználói azonosító és jelszó megadását írhatja elő.
  - Amikor a felhasználó (kliens) egy védett erőforrást kér, akkor a szerver felhasználói azonosítót és jelszót kér a böngészőtől. A böngésző felszólítja a felhasználót egy azonosító és jelszó megadására, majd elküldi az információkat a szervernek. Bizonyos böngészők képesek a felhasználói azonosító és jelszó tárolására és automatikus elküldésére a későbbi alkalmak során. Ez megkönnyíti a felhasználó életét, mivel nem kell minden egyes alkalommal megadni a felhasználói azonosítót és jelszót.

    A felhasználói azonosítók és jelszavak tárolása miatt a felhasználókat ugyanúgy ki kell oktatni ennek biztonsági vonatkozásairól, mint a bejelentkezés képernyő segítségével megvalósított belépések kapcsán. A felügyelet nélküli hagyott böngészők lehetséges biztonsági kockázatot jelentenek.

– A felhasználói azonosító és jelszó a biztonsági direktívák beállításától függően háromféleképpen kezelhető:

1. Használhatja az iSeries szerver szokásos felhasználói profil és jelszó ellenőrzését. Ez az intranetes (védett hálózaton kiszolgált) erőforrások jellemző védelmi módszere.
2. Létrehozhatók ″Internet felhasználók″, amelyek ellenőrzése anélkül történik, hogy ehhez iSeries felhasználói profilra lenne szükségük. Az Internet felhasználók megvalósítása egy ellenőrzési listának nevezett iSeries objektum segítségével történik. Az ellenőrzési lista objektumok egy adott alkalmazáshoz tartozó felhasználók és jelszavak listáját tartalmazzák.

   Az Internet felhasználók azonosítóinak és jelszavainak megadása (például automatikusan egy alkalmazásban, vagy egy adminisztrátor által), illetve az Internet felhasználók kezelésének módja az adott igényektől függ. Ennek beállítására a HTTP szerver böngésző alapú felülete használható.

   Megbízhatatlan hálózatok (például az Internet) esetén az Internet felhasználók a hagyományos felhasználói profilok és jelszavak használatához képest magasabb szintű védelmet nyújtanak. A felhasználói azonosítók és jelszavak egyedi listája beépített korlátozást jelent az ilyen felhasználók által végrehajtható tevékenységekre nézve. Ezek a felhasználói azonosítók nem használhatók szokásos bejelentkezéshez (például FTP vagy Telnet céljára). Emellett a felhasználói azonosítókat és jelszavakat sem teszi ki a lehallgatás veszélyének.
3. Az Egyszerűsített címtárhozzáférési protokoll (LDAP) olyan címtár szolgáltatási protokoll, amely címtárak elérését biztosítja Átvitelvezérlési protokoll (TCP) kapcsolatokon keresztül. Lehetővé teszi, hogy információkat tároljon egy címtárban, és lekérdezze azokat. A jelenlegi kiadásban LDAP is használható felhasználói hitelesítési célokra.

   Megjegyzések:

   1. Amikor a böngésző elküldi egy felhasználói profil vagy Internet felhasználó azonosítóját és jelszavát, akkor ezek csak kódolva vannak, nem titkosítva. A kódolási séma ipari szabvány, tehát a cracker közösségek is jól ismerik. Bár a kódolás védelmet nyújt a kezdő ″hallgatózók″ ellen, a tapasztaltabbak minden valószínűség szerint rendelkeznek a dekódoláshoz szükséges eszközökkel.
   2. Az iSeries szerver az ellenőrzési objektumot egy védett rendszerterületen tárolja. Elérése csak meghatározott felületek (API-k) felhasználásával és a megfelelő jogosultságok birtokában lehetséges.

– A Digitális igazolás kezelő segítségével saját igazolási hatóságot hozhat létre és üzemeltethet. A digitális igazolások automatikusan társításra kerülnek a tulajdonos felhasználói profilhoz. Az igazolás ugyanazzal a jogosultságokkal és engedélyekkel fog rendelkezni, mint a hozzá tartozó profil.

- Amikor a szerver elfogad egy kérést, életbe lépnek az iSeries szerver szokásos erőforrás biztonságra vonatkozó funkciói. Az erőforrást kérő felhasználói profilnak rendelkeznie kell a megfelelő jogosultsággal az erőforráshoz (például a HTML dokumentumot tartalmazó mappához vagy forrás fizikai fájlhoz). A jobok alapértelmezésben a QTMHHTTP felhasználói profil alatt futnak. A megfelelő direktíva segítségével átválthat ettől eltérő felhasználói profilra is. A rendszer ezután a másik felhasználói profil jogosultságait használja az objektumok elérésének kiértékelésekor. A támogatásra további szempontok is vonatkoznak:

  – A felhasználói profilok váltása különösen hasznos abban az esetben, ha a rendszer egynél több logikai webhelyet szolgál ki. Ilyen esetekben a direktívák segítségével minden egyes webhelyhez külön felhasználói profilt rendelhet, ily módon az egyes webhelyekhez tartozó dokumentumok védelméről az iSeries szerver erőforrás biztonsági funkciói gondoskodnak.

- A felhasználói profil váltás képességét az ellenőrzési objektummal együtt is használhatja. A szerver (a szokásos felhasználói azonosítótól és jelszótól eltérő) egyedi felhasználói azonosítót és jelszót használ a kezdeti kérés kiértékeléséhez. A felhasználó hitelesítése után a szerver átvált egy másik felhasználói profilra, így kihasználva az arra vonatkozó erőforrás biztonsági funkciókat. A felhasználó ily módon nem bír tudomással a valódi felhasználói profil nevéről, ily módon meg sem tudja próbálni más módon (például FTP vagy Telnet alkalmazásban) felhasználni.

- Bizonyos HTTP kérések egy program futtatását igénylik a HTTP szerveren. Egy program például adatokat kérdezhet le a rendszeren. Mielőtt a programot futtatni lehetne, a szerver adminisztrátorának a kérést (URL) le kell képezni egy CGI szabványnak megfelelő felhasználói programra. A CGI programok használatának biztonsági vonzatai a következők:
  - A biztonsági direktívák a CGI programokon ugyanúgy használhatók, mint HTML dokumentumok esetében. Magyarán a program futtatása előtt kérhet felhasználói azonosítót és jelszót.
  - A CGI programok alapértelmezésben a QTMHHTP1 felhasználói profil alatt futnak. A program futtatása előtt át lehet váltani egy másik felhasználói profilra. Ennek megfelelően megoldható, hogy a CGI programra az iSeries szerver szokásos biztonsági funkciói vonatkozzanak.
  - A biztonsági adminisztrátornak érdemes biztonsági szempontból átnézni a CGI programokat, mielőtt engedélyezné ezek használatát. Ismernie kell a programok származási helyét, illetve az általuk végrehajtott funkciókat. Érdemes megvizsgálni ezen kívül a CGI programokat futtató felhasználói profilok képességeit is. Emellett a CGI programokat érdemes megvizsgálni abból a szempontból is, hogy lehetőséget nyújtanak-e valamilyen módon parancssor szerzésére. A CGI programokat az átvett jogosultságot alkalmazó programokkal egyező óvatossággal kell kezelni.
  - Vizsgálja meg, hogy mely érzékeny objektumok rendelkezhetnek nem megfelelő nyilvános jogosultsággal. A rosszul tervezett CGI programok bizonyos esetekben lehetőséget biztosítanak a hozzáértő rosszindulatú felhasználóknak a rendszer bejárására.
  - A CGI programokat egy jól meghatározott könyvtárban tárolja (például CGILIB). az objektum jogosultságok segítségével gondosan határozza meg, hogy ki helyezhet el programokat a könyvtárban, és ki futtathatja ezeket. A HTTP szerver direktíváinak felhasználásával állítsa be, hogy a szerver csak ezen könyvtár programjait futtassa.

    Megjegyzés: Ha a szerveren több logikai webhely kiszolgálása történik, akkor érdemes ezek mindegyikének különálló CGI könyvtárat kijelölni.

További biztonsági szempontok

Érdemes megfontolni az alábbi biztonsági szempontokat is:

- A HTTP szerver csak olvasható hozzáférést biztosít az iSeries rendszerhez. A HTTP szerver kérések közvetlenül nem képesek a rendszer adatainak módosítására vagy törlésére. Ennek ellenére lehetnek olyan CGI programok, amelyek frissítenek különféle adatokat. Emellett elképzelhető, hogy engedélyezni kell Net.Data CGI programot az iSeries szerver adatbázisainak lekérdezéséhez. A rendszer egy végprogramhoz hasonló parancsfájlt használ a Net.Data programra vonatkozó kérések kiértékelésére. Ennek megfelelően a rendszeradminisztrátor felügyelheti a Net.Data program által végrehajtott tevékenységeket.
- A HTTP szerver hozzáférési naplót készít, amelyet felhasználhat a szerver hozzáférések és a hozzáférési kísérletek figyelésére.

IBM iSeries HTTP szerver SSL támogatására vonatkozó biztonsági szempontok

Az IBM HTTP Server for iSeries támogatja a biztonságos webes kapcsolatok kialakítását az iSeries szerverrel. A **biztonságos webhely** azt jelenti, hogy a kliens és a szerver közötti kommunikáció (mindkét irányban) titkosítva van. A titkosított adatátvitel a lehallgatókkal szemben, illetve az adatforgalmazás elfogására vagy módosítására törekvőkkel szemben is védett.

Megjegyzés: Tartsa szem előtt, hogy a biztonságos webhely kifejezés csak a kliens és szerver között folyó adatátvitel biztonságára utal. Ennek célja nem az, hogy csökkentse a szerver veszélyeztetettségét a betörőkkel szemben. Ettől függetlenül határozottan korlátozza a lehallgatással megszerezhető információk mennyiségét.

A titkosítási folyamat telepítésével, beállításával és kezelésével kapcsolatos részleteket az Információs központ SSL és Web kiszolgálás című témakörei tartalmazzák. A témakörök bemutatják a szerver ilyen irányú szolgáltatásait, és leírják a használatukra vonatkozó szempontokat is.

Az Internet Connection Server a következő licencprogramok valamelyikének telepítése esetén biztosít HTTP és HTTPS támogatást:

- 5722–NC1
- 5722–NCE

Az említett opciók telepítése esetén a termék neve Védett Internet kapcsolati szerver.

Az IBM HTTP Server for iSeries (5722–DG1) HTTP és HTTPS támogatást is biztosít. Az SSL engedélyezéséhez telepíteni kell a következő kriptográfiai termékek valamelyikét:

- 5722–AC2
- 5722–AC3

A titkosításon alapuló biztonságnak számos előfeltétele van:

- A szervernek és a kliensnek is ″értenie″ kell a titkosítási mechanizmust, és képesnek kell lennie a titkosítás és visszafejtés végrehajtására. A HTTP szerver SSL támogatással rendelkező klienst igényel. (A legtöbb népszerű web böngészőre ez teljesül.) Az iSeries titkosítási licencprogramok számos ipari szabvány titkosítási módszert támogatnak. Amikor a kliens biztonságos szekciót próbál kialakítani a szerverrel, akkor egyeztetik azt a legbiztonságosabb titkosítási módszert, amelyet mindkettejük támogat.
- A lehallgatók nem lehetnek képesek az átvitel visszafejtésére. Ennek megfelelően a titkosítási módszerek mindkét fél részéről megkövetelik egy olyan **magánkulcs** meglétét, amelyet csak ők ismernek. Ha biztonságos *külső* webhelyet kíván kialakítani, akkor a felhasználóknak és szervereknek egy független igazolási hatóság digitális igazolásait kell használniuk. Az igazolási hatóságot megbízható félnek is nevezik.

A titkosítás a továbbított információk bizalmasságát védi. Érzékeny információk, például pénzügyi tranzakciók esetén azonban a bizalmasságon felül az információk integritását és hitelességét is biztosítani kell. Más szavakkal a kliensnek (és bizonyos esetekben a szervernek is) meg kell tudniuk bízni a másik félben (általában egy független referencia alapján), és biztosaknak kell lenniük abban, hogy az átvitt információkat nem módosították az átvitel során. Az igazolási hatóságok által biztosított digitális aláírások megadják ezen hitelesítési és integritási funkciókat. Az SSL protokoll a hitelességet a szerver (és választhatóan a kliens) igazolásához tartozó digitális aláírás ellenőrzésével biztosítja.

A titkosítás és visszafejtés feldolgozási időt igényel, és hatással van az átvitel teljesítményére. Ennek megfelelően az iSeries szerverek támogatják védett és nem védett programok futtatását is. A nem védett HTTP szerver biztonságot nem igénylő dokumentumok, például termékkatalógusok kiszolgálására használható. Ezek a dokumentumok http:// kezdetű URL címmel érhetők el. Ezzel egyidőben az érzékeny információk kiszolgálását végezheti egy védett HTTP szerver. A program http:// és https:// kezdetű URL címmel elérhető dokumentumokat is kiszolgálhat.

Emlékeztető

Az Internet etikettje szerint a klienseket illik tájékoztatni arról, hogy az adatátvitel mikor védett és mikor nem védett, különösen akkor, ha a webhely csak bizonyos dokumentumokat szolgál ki a védett szerveren keresztül.

Ne feledje, hogy a titkosítás működéséhez a kliensnek és szervernek is támogatnia kell azt. A védett böngészők (HTTP kliensek) mostanára elég általánossá váltak.

LDAP biztonsági szempontok

Az Egyszerűsített címtárhozzáférési protokoll (LDAP) biztonsági funkciói közé tartozik a Védett socket réteg (SSL) támogatás, a hozzáférés felügyeleti listák alkalmazása és a CRAM-MD5 jelszó titkosítás. A V5R1 kiadásban az LDAP biztonságának kiterjesztése érdekében az LDAP szerver kibővült a Kerberos kapcsolatok és a biztonsági megfigyelés támogatásával.

Az említett témákról további ismereteket az iSeries Információs központ Hálózatok → TCP/IP → Címtár szolgáltatások (LDAP) témaköréből szerezhet. Az iSeries Információs központ elérésével kapcsolatban nézze meg az “Előfeltétel és kapcsolódó információk” oldalszám: xii szakaszt.

LPD biztonsági szempontok

A Sornyomtató démon (LPD) lehetővé teszi a rendszer számára nyomtatókimenetek fogadását. A rendszer az LPD kapcsolatoknál semmilyen bejelentkezési feldolgozást nem hajt végre.

LPD hozzáférés megakadályozása

Ha *nem szeretné*, hogy az LPD funkciókkal bárki is hozzáférjen a rendszerhez, akkor meg kell akadályozni az LPD szerver elindítását. Tegye a következőket:

__ Lépés 1. Ha meg kívánja akadályozni az LPD szerverjobok elindítását a TCP/IP indításakor, akkor írja be a következő parancsot:

```
CHGLPDA AUTOSTART(*NO)
```

Megjegyzések:

a. Az alapértelmezett érték az AUTOSTART(*YES).

b. Az automatikusan induló TCP/IP szerverek beállításával kapcsolatban további információkat az “Automatikusan induló TCP/IP szerverek meghatározása” oldalszám: 122 szakaszban talál.

__ Lépés 2. Ha meg kívánja akadályozni, hogy valaki felhasználói alkalmazást, például egy socket alkalmazást futtasson azon a porton, amelyet általában az LPD használ, akkor tegye a következőket:

__ Lépés a. Írja be a GO CFGTCP parancsot a TCP/IP beállítása menü megjelenítéséhez.

__ Lépés b. Válassza a 4. menüpontot (TCP/IP port korlátozások kezelése).

__ Lépés c. A TCP/IP port korlátozások kezelése képernyőn válassza az 1. lehetőséget (Hozzáadás).

__ Lépés d. A porttartomány kezdetének adja meg az 515-ös portot.

__ Lépés e. A porttartomány végének adja meg az *ONLY értéket.

Megjegyzések:

1) A port korlátozás a TCP/IP következő újraindításakor lép életbe. Ha a TCP/IP aktív a port korlátozások beállításakor, akkor be kell fejezni a TCP/IP-t, és újra kell indítani.
2) Az általános portszám hozzárendeléseket az RFC1700 írja le.

__ Lépés f. A protokollnak adja meg a *TCP értéket.

__ Lépés g. A felhasználói profil mezőben védett felhasználói profil nevet kell megadni. (A védett felhasználói profilok olyan profilok, amelyek nem birtokolnak jogosultságot átvevő programokat, és nem rendelkeznek más felhasználók számára ismert jelszavakkal.) A portnak egy adott felhasználóra korlátozásával automatikusan kizár minden más felhasználót.

__ Lépés h. Ismételje meg a fenti lépéseket (2c - 2g) az *UDP protokoll megadásával.

LPD hozzáférés felügyelete

Ha engedélyezni kívánja az LPD klienseknek a rendszer elérését, akkor legyen figyelemmel a következő biztonsági szempontokra:

- Ésszerű háttértár küszöbértékek beállításával meg kell akadályozni, hogy a rendszert elárasszák kéretlen objektumokkal. A háttértár küszöbértékek megjelenítése és beállítása a Rendszer szervizeszközökben (SST) és a Kijelölt szervizeszközökben (DST) lehetséges. Az ASP küszöbértékekről további részleteket a *Rendszermentés és visszaállítás* című kiadvány tartalmaz.
- A rendszerre spoolfájlokat küldő felhasználók korlátozása a kimeneti sorokra vonatkozó jogosultságok megfelelő beállításával lehetőséges. A felhasználói azonosítóval nem rendelkező LPD felhasználók a QTMPLPD felhasználói profilt használják. Adja meg, hogy ez a felhasználói profil csak néhány kimeneti sorhoz férjen hozzá.

SNMP biztonsági szempontok

Az iSeries szerver képes Egyszerű hálózatkezelési protokoll (SNMP) ügynökként működni a hálózaton. Az SNMP a hálózati környezetek átjáróinak, útválasztóinak és hosztjainak kezelésére ad lehetőséget. A rendszerről az SNMP ügynök gyűjti össze az információkat, és ez hajtja végre a távoli SNMP hálózatkezelők kéréseit is.

SNMP hozzáférés megakadályozása

Ha *nem szeretné*, hogy az SNMP funkciókkal bárki is hozzáférjen a rendszerhez, akkor meg kell akadályozni az SNMP szerver elindítását. Tegye a következőket:

__ Lépés 1. Ha meg kívánja akadályozni az SNMP szerverjobok elindítását a TCP/IP indításakor, akkor írja be a következő parancsot:

```
CHGSNMPA AUTOSTART(*NO)
```

Megjegyzések:

a. Az alapértelmezett érték az AUTOSTART(*YES).

b. Az automatikusan induló TCP/IP szerverek beállításával kapcsolatban további információkat az “Automatikusan induló TCP/IP szerverek meghatározása” oldalszám: 122 szakaszban talál.

__ Lépés 2. Ha meg kívánja akadályozni, hogy valaki felhasználói alkalmazást, például egy socket alkalmazást futtasson azon a porton, amelyet általában az SNMP használ, akkor tegye a következőket:

__ Lépés a. Írja be a GO CFGTCP parancsot a TCP/IP beállítása menü megjelenítéséhez.

__ Lépés b. Válassza a 4. menüpontot (TCP/IP port korlátozások kezelése).

__ Lépés c. A TCP/IP port korlátozások kezelése képernyőn válassza az 1. lehetőséget (Hozzáadás).

__ Lépés d. A porttartomány kezdetének adja meg a 161-es portot.

__ Lépés e. A porttartomány végének adja meg az *ONLY értéket.

Megjegyzések:

1) A port korlátozás a TCP/IP következő újraindításakor lép életbe. Ha a TCP/IP aktív a port korlátozások beállításakor, akkor be kell fejezni a TCP/IP-t, és újra kell indítani.
2) Az általános portszám hozzárendeléseket az RFC1700 írja le.

__ Lépés f. A protokollnak adja meg a *TCP értéket.

__ Lépés g. A felhasználói profil mezőben védett felhasználói profil nevet kell megadni. (A védett felhasználói profilok olyan profilok, amelyek nem birtokolnak jogosultságot átvevő programokat, és nem rendelkeznek más felhasználók számára ismert jelszavakkal.) A portnak egy adott felhasználóra korlátozásával automatikusan kizár minden más felhasználót.

__ Lépés h. Ismételje meg a fenti lépéseket (2c - 2g) az *UDP protokoll megadásával.

SNMP hozzáférés felügyelete

Ha engedélyezni kívánja az SNMP kezelőknek a rendszer elérését, akkor legyen figyelemmel a következő biztonsági szempontokra:

- Aki hozzá tud férni a hálózathoz SNMP segítségével, az információkhoz juthat a hálózatról. Az álnevek és tartománynév-szerverek segítségével elrejteni próbált információk SNMP segítségével elérhetővé válnak a betörni szándékozók részére. Emellett a betörő az SNMP segítségével módosíthatja a hálózati konfigurációt is, és megbéníthatja a kommunikációt.
- Az SNMP hozzáférés egy közösségnév alapján történik. Koncepcionálisan a közösségnév hasonló a jelszavakhoz. A közösség neve nincs titkosítva. Ennek megfelelően lehallgatható a hálózaton. Az SNMP közösség hozzáadása (ADDCOMSNMP) paranccsal állíthatja be a kezelő Internet címe (INTNETADR) paramétert adott IP címekre az *ANY érték helyett. Emellett az ADDCOMSNMP és CHGCOMSNMP parancsok OBJACC paraméterének *NONE beállításával megakadályozhatja, hogy a közösség kezelői hozzáférjenek a MIB objektumokhoz. Ez ideiglenes megoldásnak tekinthető a kezelők hozzáférésének megszüntetésére a közösség eltávolítása nélkül.

INETD biztonsági szempontok

A legtöbb TCP/IP szervertől eltérően az INETD szerver nem egyetlen szolgáltatást biztosít a kliensek számára. Ehelyett több különféle szolgáltatást is nyújt, amelyeket az adminisztrátor testre szabhat. Ezen okból az INETD szervert néha felső szintű szervernek is nevezik. Az INETD szerver a következő beépített szolgáltatásokat biztosítja:

- time
- daytime
- echo
- discard
- chargen

A szolgáltatások UDP és TCP kapcsolaton is támogatottak. UDP esetén az echo, time, daytime és chargen szolgáltatások fogadják az UDP csomagokat, majd visszaküldik azokat a kezdeményezőnek. Az echo szerver visszaküldi a kapott csomagokat, a time és daytime szerver a pontos időt küldi vissza egy speciális formátumban, a chargen szerver pedig nyomtatható ASCII karakterekből álló csomagot állít össze és küld vissza.

Az említett UDP szolgáltatások természetükből fakadóan felhasználhatók szolgáltatás megbénítási (DoS) támadásra. Tegyük fel például, hogy rendelkezik két iSeries szerverrel, amelyek neve rendre SYSTEMA és SYSTEMB. Egy rosszindulatú programozó meghamisíthat egy csomagot oly módon, hogy az IP és UDP fejlécben a SYSTEMA címét adja meg forráscímként, és a time szerver UDP portszámát portként. A csomagot elküldi a SYSTEMB time szerverének. Az válaszol a SYSTEMA rendszernek, amely szintén válaszol a SYSTEMB rendszernek, így végső soron végtelen ciklus jön létre, amely mindkét rendszeren CPU erőforrásokat igényel, emellett a hálózat sávszélességét is fogyasztja.

Ennek megfelelően az ilyen támadások kockázatának megfontolása után érdemes úgy dönteni, hogy ezeket a szolgáltatásokat csak biztonságos hálózatban futtatja. Az INETD szerver alapértelmezésben nem indul el a TCP/IP indításakor. Beállítható, hogy a szolgáltatások elinduljanak-e az INETD indításakor. Alapértelmezésben a TCP és UDP time és daytime szerver is elindul az INETD szerver elindításakor.

Az INETD szerver két konfigurációs fájlt használ:

```
/QIBM/UserData/OS400/inetd/inetd.conf
/QIBM/ProdData/OS400/inetd/inetd.conf
```

Ezek a fájlok határozzák meg az INETD szerver indulásakor elindítandó programokat. Emellett megadják azt is, hogy az INETD milyen felhasználói profil alatt indítsa ezeket.

Megjegyzés: A ProdData katalógusban található konfigurációs fájlt sohase módosítsa. A fájl a rendszer minden újratöltésével felülíródik. Az egyéni konfigurációs módosításokat az UserData katalógusban található fájlba kell bevezetni, mivel ez a fájl **nem** kerül felülírásra a kiadások frissítése során.

Ha egy rosszindulatú programozó hozzáfér ezen fájlokhoz, akkor bármilyen programot elindíttathat az INETD indulásakor. Ennek megfelelően fontos a fájlok védelme. Alapértelmezésben QSECOFR jogosultságot igényelnek a módosításhoz. Az elérésükhöz szükséges jogosultságot ne állítsa kisebbre.

Megjegyzés: A ProdData katalógusban található konfigurációs fájlt ne módosítsa. Ez a fájl a rendszer minden újratöltésével felülíródik. Az egyéni konfigurációs módosításokat az UserData katalógusban található fájlban kell elvégezni, mivel ez a fájl nem kerül felülírásra a kiadások frissítése során.

TCP/IP barangolás korlátozására vonatkozó biztonsági szempontok

Ha a rendszer hálózathoz csatlakozik, akkor elképzelhető, hogy érdemes korlátozni a felhasználók azon képességeit, hogy a TCP/IP alkalmazásokkal a hálózatban barangoljanak. Ennek egyik módja, hogy letiltja a következő kliens TCP/IP parancsok elérését:

Megjegyzés: A parancsok elképzelhető, hogy a rendszer több könyvtárában is megtalálhatók. Legalább a QSYS és QTCP könyvtár biztos, hogy tartalmazza ezeket. Győződjön meg róla, hogy valamennyi előfordulásukat megtalálta és bebiztosította.

- STRTCPFTP
- FTP
- STRTCPTELN
- TELNET
- LPR
- SNDTCPSPLF
- RUNRMTCMD (REXEC kliens)

A felhasználók lehetséges céljait következők határozzák meg:

- A TCP/IP hoszttábla bejegyzései.
- A TCP/IP útválasztási tábla *DFTROUTE bejegyzése. Ez lehetővé teszi a felhasználóknak a következő állomás címének megadását, ha a céljuk ismeretlen hálózaton található. A felhasználók az alapértelmezett útvonal segítségével léphetnek kapcsolatba távoli hálózatokkal.
- Távoli névszerver konfiguráció. Ez lehetővé teszi, hogy a hálózat egy másik szervere hosztneveket keressen a felhasználók számára.
- Távoli rendszer tábla.

Érdemes felügyelni, kik adhatnak hozzá bejegyzéseket ezen táblákhoz, és kik módosíthatják a konfigurációt. Emellett ajánlott megérteni a táblák bejegyzéseinek a konfigurációra gyakorolt hatásait.

Vigyázzon arra, nehogy az ILE C fordítót elérő hozzáértő felhasználók létrehozzanak egy TCP vagy UDP porthoz csatlakozó socket programot. Ez a QSYSINC könyvtár alábbi socket API fájlok hozzáférésének korlátozásával teheti nehezebbé:

- SYS
- NETINET
- H
- ARPA
- socketek és SSL

A szervizprogramoknál a következő szervizprogramok használatának megtiltásával korlátozhatja a már lefordított socket és SSL alkalmazásokat:

- QSOSRV1
- QSOSRV2
- QSOSKIT(SSL)
- QSOSSLSR(SSL)

A szervizprogramok alapértelmezett nyilvános jogosultsága *USE, de ez módosítható az *EXCLUDE (vagy bármilyen más szükséges) értékre.

14. fejezet Munkaállomások biztonságosabbá tétele

A rendszer felhasználóinak nagy része valószínűleg az asztalán található személyi számítógépet használja munkaállomásként. PC-n futó eszközöket használ, és a PC segítségével csatlakozik az iSeries szerverre is.

A személyi számítógépeket iSeries szerverre csatlakoztató módszerek legtöbbje több funkciót biztosít a munkaállomás emulációnál. A PC az iSeries szemszögéből terminálként működhet, amely interaktív bejelentkezési lehetőséget biztosít a felhasználóknak. Másrészt a PC az iSeries szerver felé egy másik számítógépként is megjelenhet, amely fájlátviteli, távoli eljáráshívási és hasonló funkciókat biztosít.

Az iSeries szerver biztonsági adminisztrátoraként oda kell figyelnie a következőkre:

- A rendszerhez csatlakozó PC felhasználók számára rendelkezésre álló funkciók.
- A PC felhasználók által elérhető iSeries rendszererőforrások.

A fejlett PC funkciókat (például a fájlátvitelt és távoli eljáráshívást) érdemes letiltani, ha az iSeries szerver biztonsági sémája nincs felkészítve ezekre. A hosszú távú cél valószínűleg az ilyen fejlett PC funkciók engedélyezése, csak a rendszeren tárolt információk védelmének fenntartásával. Az alábbi témakörök a PC hozzáféréssel kapcsolatos biztonsági kérdéseket feszegetik.

Munkaállomás vírusok megelőzése

Ez a szakasz tesz néhány javaslatot a PC vírusok elleni védelemre.

Munkaállomás adathozzáférés biztonságosabbá tétele

Bizonyos PC kliens szoftverek osztott mappákat használnak az információk tárolására a szerveren. Az iSeries adatbázisfájljainak használatához a PC felhasználók korlátozott és jól meghatározott felületekkel rendelkeznek. A legtöbb kliens/szerver szoftverben megtalálható fájlátvitel funkcióval a PC felhasználók fájlokat másolhatnak a szerver és a PC kliens között. Az adatbázis hozzáférési szolgáltatásokkal, például egy DDM fájllal, távoli SQL funkcióval vagy egy ODBC illesztőprogrammal a PC felhasználó elérheti a szerver adatait.

Ilyen környezetekben a PC felhasználók által a szerver erőforrásainak használatára vonatkozóan kiadott kéréseket egy erre a célra írt programmal érdemes elfogni és kiértékelni. DDM fájlok használatakor az osztott adatkezelési hozzáférés (DDMACC) hálózati attribútumban megadható egy végprogram. Bizonyos PC fájlátviteli funkcióknál a végprogramot a kliens hozzáférés kérés (PCSACC) hálózati attribútumban kell megadni. Ennek alternatívájaként megadhatja a PCSACC (*REGFAC) értéket is a bejegyzési funkció használatához. Ha a kérések más szerver funkciókkal férnek hozzá az adatokhoz, akkor a WRKREGINF paranccsal jegyezhet be végprogramokat ezen szerver funkciókhoz.

A végprogramok tervezése viszont nehéz lehet, és a megvalósításuk csak igen ritkán sikerül bolondbiztosra. A végprogramok nem helyettesíthetik az objektum biztonságot, hiszen ez biztosítja az objektumok védelmét bármilyen jogosulatlan hozzáféréssel szemben.

Bizonyos kliens szoftverek, például az IBM iSeries Access for Windows az integrált fájlrendszert használják az iSeries szerverek adatainak tárolására és elérésére. Az integrált fájlrendszer használatával a teljes szerver könnyebben elérhető a PC felhasználók számára. Ilyenkor az objektum jogosultságok még nagyobb jelentőséghez jutnak. Az integrált

fájlrendszeren keresztül az elegendő jogosultsággal rendelkező felhasználók a szerver könyvtárait PC mappaként láthatják. Az egyszerű másolási és áthelyezési parancsok azonnal áthelyezhetik az iSeries szerver könyvtáraiban tárolt adatokat egy PC mappába és viszont. A rendszer automatikusan elvégzi a megfelelő módosításokat az adatok formátumán.

Megjegyzések:

1. A QSYS.LIB fájlrendszer objektumainak használatát jogosultsági listával felügyelheti. További információk: “QSYS.LIB fájlrendszerre vonatkozó hozzáférés korlátozása” oldalszám: 101.
2. Az integrált fájlrendszerrel kapcsolatos biztonsági kérdéseket a 11. fejezet, “Integrált fájlrendszer használata a fájlok védelmére”, oldalszám: 95 szakasz tárgyalja.

Az integrált fájlrendszer ereje a felhasználók és fejlesztők felé mutatott egyszerűségében rejlik. A felhasználó egyetlen felületen keresztül kezelheti több környezet objektumait. Az objektumok eléréséhez a PC felhasználónak nincs szüksége speciális szoftverekre vagy alkalmazásprogram illesztőkre (API). Ehelyett a PC parancsok használatát ismerő felhasználók PC-s parancsokkal vagy az egérrel (“rámutatás és kattintás”) közvetlenül kezelhetik az objektumokat.

A PC csatlakozással rendelkező rendszereken, különösen az integrált fájlrendszert használó kliens szoftverrel rendelkező rendszereken, nagyon fontos egy jó objektum jogosultsági séma kialakítása. Mivel a biztonság az OS/400 integrált része, valamennyi adathozzáférési kérésnek át kell mennie a jogosultság ellenőrzési eljáráson. A jogosultságok ellenőrzése bármilyen forrásból származó, bármilyen adatok elérését célzó, bármilyen módszert használó kérésnél bekövetkezik.

Objektum jogosultság és munkaállomás hozzáférés

Az objektumok jogosultságának beállításakor ki kell értékelni a PC felhasználók számára biztosított jogosultságokat. Ha például egy felhasználó *USE jogosultsággal rendelkezik egy fájlhoz, akkor képes a fájl adatainak megjelenítésére és nyomtatására. A fájl információinak módosítására illetve a fájl törlésére nem. A PC felhasználók számára a megjelenítés egyenértékű az “olvasással”, amely elegendő a felhasználónak ahhoz, hogy a fájlról másolatot készítsen a PC-n. Vannak esetek, amikor ez nem helyénvaló.

Bizonyos kritikus fájlok esetén a letöltés megakadályozásának céljából a nyilvános jogosultságot *EXCLUDE-ra kell állítani. Ezután biztosíthat egy másik módszert a fájl “megtekintésére” a szerveren, például egy menü és egy átvett jogosultságot alkalmazó program segítségével.

A letöltés megakadályozására egy másik módszer egy olyan végprogram használata, amely (az interaktív bejelentkezés kivételével) a PC felhasználók által kezdeményezett valamennyi szerver funkció előtt lefut. A PCSACC hálózati attribútumban a Hálózati attribútum módosítása (CHGNETA) paranccsal adhat meg egy végprogramot. További végprogramokat a Bejegyzési információk kezelése (WRKREGINF) paranccsal jegyezhet be. Az alkalmazott módszer attól függ, hogy a számítógépek hogyan férnek hozzá a rendszer adataihoz, és hogy a számítógépeken milyen kliens programok futnak. A (QIBM_QPWFS_FILE_SERV) végprogram az IFS iSeries Access és hálózati szerver elérésére vonatkozik. Nem korlátozza viszont más mechanizmusok, például az FTP vagy az ODBC használatát.

A PC szoftverek általában biztosítanak feltöltési lehetőséget is, amelyekkel a felhasználók a számítógépről adatokat másolhatnak át a szerver adatbázisfájljaiba. Nem megfelelő jogosultsági séma alkalmazásakor elképzelhető, hogy egy PC felhasználó egy fájl összes adatát felülírja a saját adataival. A *CHANGE jogosultságot kellő körültekintéssel osztogassa. A különféle fájlműveletekhez szükséges jogosultságokat az *iSeries biztonsági összefoglaló* D függeléke tartalmazza.

A PC funkciók jogosultságairól és a végprogramok használatáról az iSeries Információs központ tartalmaz további részleteket. A részleteket az “Előfeltétel és kapcsolódó információk” oldalszám: xii szakaszban találja.

Alkalmazás adminisztráció

Az Alkalmazás adminisztráció az iSeries navigátor, az iSeries szerver grafikus kezelőfelületének választhatóan telepíthető összetevője. Az Alkalmazás adminisztráció lehetővé teszi a rendszeradminisztrátoroknak az egyes szervereken a felhasználók és csoportok számára rendelkezésre álló funkciók vagy alkalmazások felügyeletét. Ebbe az olyan funkciók is beletartoznak, amelyek klienseken keresztül biztosítják a felhasználók hozzáférését a szerverhez. Ezen a ponton fontos megjegyezni, hogy amikor a szervert Windows kliensről éri el, akkor az adminisztrálható funkciókat nem a Windows, hanem az iSeries szerver felhasználó határozza meg.

Az iSeries navigátor alkalmazás adminisztrációjáról további részleteket az iSeries Információs központ –> Csatlakozás az iSeries szerverhez —> Csatlakozási módszer —> iSeries navigátor című témaköréből (../html/as400/v5r2/ic2924/info/rzaj3/rzaj3overview.htm) tudhat meg.

Házirend adminisztráció

A házirendek az adminisztrátor eszközei a kliens számítógépek szoftvereinek beállításához. A házirendek a felhasználó által a számítógépen használható funkciókat és alkalmazásokat korlátozhatják. A házirendek emellett javasolhatnak vagy kötelezővé tehetnek bizonyos beállításokat a megadott felhasználók vagy számítógépek számára.

Megjegyzés: A házirendek nem biztosítják a szerver erőforrások felügyeletét. Ennek megfelelően a házirendek nem helyettesítik a szerver biztonságát. A házirendekkel az határozható meg például, hogyan férhet hozzá a szerverhez az iSeries Access program egy adott számítógépről egy adott felhasználó bejelentkezése esetén. Nincsenek viszont hatással a szerver erőforrásainak más módon végzett elérésére.

A házirendeket egy fájlszerver tárolja. Minden alkalommal, amikor egy felhasználó bejelentkezik a Windows munkaállomására, a fájlszerverről letöltődnek az adott Windows munkaállomásra vonatkozó házirendek. Mielőtt a felhasználó bármilyen tevékenységet tudna végezni a munkaállomáson, a házirendek bekerülnek a rendszerleíró adatbázisba.

Microsoft házirendek és az alkalmazás adminisztráció összehasonlítása

Az iSeries Access kétféle megközelítést biztosít a hálózat adminisztratív felügyeletének megvalósítására, a Microsoft rendszerházirendeket és az iSeries navigátor alkalmazás adminisztrációját. Az igényeknek leginkább megfelelő stratégia kiválasztásakor fontolja meg a következőket.

Microsoft rendszerházirendek

A házirendek a PC-re vonatkoznak, nem függnek bizonyos OS/400 kiadásoktól. A házirendek számítógépekre és Windows felhasználókra is vonatkozhatnak. Ezt azt jelenti, hogy ebben a megközelítésben a felhasználó kifejezés Windows felhasználónévre, nem szerver felhasználói profilra utal. A házirendek korlátozáson kívül konfigurálásra is használhatók. A házirendek általában részletesebben szabályozhatók az alkalmazás adminisztrációnál, és szélesebb körű funkciókat is biztosítanak annál. Ez azért van így, mert a szerver kapcsolatára nincs szükség annak megállapítására, hogy a felhasználó jogosult-e a funkció használatára vagy sem. A házirendek megvalósítása komplikáltabb az alkalmazás adminisztráció beállításánál, mivel ehhez szükség van a Microsoft rendszerházirend-szerkesztőre, és a számítógépeket is egyenként kell beállítani a házirendek letöltésére.

iSeries navigátor alkalmazás adminisztráció

Az alkalmazás adminisztráció a beállítási adatokat a felhasználói profillal társítja, nem a Windows felhasználónévvel, amely a Microsoft rendszerházirendhez társul. Bár az alkalmazás adminisztráció használatához az OS/400 V4R3 vagy újabb kiadását futtató iSeries szerverek szükségesek, bizonyos funkciók csak a V4R4 és újabb kiadásokban érhetők el. Az alkalmazás adminisztráció beállítása a rendszerházirend-szerkesztőnél lényegesen egyszerűbben kezelhető iSeries navigátorban történik. Az alkalmazás adminisztráció a bejelentkezéshez használt számítógéptől függetlenül vonatkozik a felhasználóra. Segítségével lehetőség van az iSeries navigátor egyes funkcióinak korlátozására is. Az alkalmazás adminisztráció akkor előnyösebb, ha a használt OS/400 kiadás és a korlátozni kívánt összes funkció támogatja az alkalmazás adminisztráció használatát.

SSL használata az iSeries Access for Windows termékkel

Az iSeries Access Express SSL támogatásának használatáról olvassa el az iSeries Információs központ következő témaköreit: *Védett socket réteg adminisztráció, iSeries Access Express és iSeries navigátor biztonságosabbá tétele, iSeries Developer Kit for Java és iSeries Java Toolbox* témakörök a Java főrész alatt. Az információkat a rendszerrel együtt szállított CD-n is megtalálja.

iSeries navigátor biztonság

Az iSeries navigátor az iSeries Access felhasználók számára egyszerűen használható felületet biztosít a szerver használatához. Az iSeries navigátor az OS/400 minden egyes kiadásával megannyi új funkcióval bővül. Az egyszerűen használható felületek számos előnnyel bírnak, beleértve a technikai támogatással kapcsolatos költségek csökkenését, és a rendszerről kialakított kép javulását is. Emellett persze biztonsági kihívásokat is jelent.

A biztonsági adminisztrátor a továbbiakban nem hagyatkozhat a felhasználók tudatlanságára. Az iSeries navigátor ugyanis igen sok funkciót tesz láthatóvá a felhasználók számára. A biztonsággal szemben támasztott igények kielégítéséhez át kell gondolni és meg kell valósítani a felhasználói profilokra és az objektum biztonságra vonatkozó biztonsági stratégiákat.

Az IBM e(logo)server iSeries Access for Windows V4R4 és újabb változatai a következő módszereket biztosítják a felhasználók által az iSeries navigátorban végrehajtható funkciók felügyeletére:

- Szelektív telepítés
- Alkalmazás adminisztráció
- Windows NT rendszerházirend támogatás

Az iSeries navigátor több, egymástól függetlenül telepíthető összetevőre van bontva. Ez lehetővé teszi, hogy csak a szükséges funkciókat telepítse. Az alkalmazás adminisztráció lehetővé teszi az adminisztrátornak a felhasználók vagy csoportok számára rendelkezésre álló funkciók felügyeletét az iSeries navigátorban. Az alkalmazás adminisztráció a következő kategóriákba szervezi az alkalmazásokat:

iSeries navigátor
Ide tartozik az iSeries navigátor és ennek bedolgozói.

Kliens alkalmazások
Ide tartozik minden más kliens alkalmazás, amely az alkalmazás adminisztrációval felügyelhető kliens funkciókat biztosít; ilyen például az iSeries Access.

Hoszt alkalmazások
Ide tartozik minden olyan alkalmazás, amely teljes egészében a szerveren található, és az alkalmazás adminisztrációval felügyelhető funkciókat biztosít.

A felhasználók által elérhető iSeries navigátor funkciók korlátozására a szelektív telepítőt, az alkalmazás adminisztrációt és a házirendeket használhatja. Ezek egyike sem biztosít azonban erőforrás biztonságot.

A V4R4 változattal kezdődően az IBM e(logo)server iSeries Access for Windows támogatja a Windows NT rendszerházirend-szerkesztőjét is, amelyben beállítható, hogy a bejelentkezett felhasználótól függően az adott PC kliensről milyen funkciók használhatók.

A szelektív telepítésről, az alkalmazás adminisztrációról és a házirend adminisztrációról további információkat az iSeries Információs központban talál. Az alkalmazás adminisztrációról néhány szóban a “Program funkciók elérésének korlátozása” oldalszám: 5 szakasz is beszámol.

ODBC hozzáférés megakadályozása

A Nyílt adatbázis csatlakozás (ODBC) a PC alkalmazások eszköze az iSeries adatok elérésére oly módon, mintha azok PC adatok lennének. Az ODBC programozó az adatok tényleges fizikai helyét transzparenssé teheti a PC alkalmazás felhasználója szemszögéből. Az ODBC biztonsági szempontjairól további információkat az iSeries Access for Windows adminisztráció című kiadvány ODBC biztonság szakaszában (/rzaii/rzaiiodbc09.HTM) találhat az iSeries Információs központban.

Munkaállomás szekció jelszavakkal kapcsolatos biztonsági szempontok

Amikor egy PC felhasználó elindítja a kapcsolati szoftvert, például az iSeries Access programot, akkor általában csak egyszer adja meg a felhasználói azonosítót és jelszót. A jelszó titkosított formában a PC memóriájában ideiglenesen tárolásra kerül. Azonos szerverrel kialakított további szekciók esetén a PC automatikusan elküldi a felhasználói azonosítót és jelszót.

Bizonyos kliens/szerver szoftverek lehetővé teszik az interaktív szekciók bejelentkezési képernyőjének kihagyását is. A szoftver az interaktív (5250 emulációs) szekció elindításakor elküldi a felhasználói azonosítót és jelszót. A támogatás működéséhez a szerver QRMTSIGN rendszerváltozóját a *VERIFY értékre kell állítani.

A bejelentkezési képernyő kihagyásának engedélyezésekor alaposan meg kell fontolni a biztonsági kompromisszumokat.

Biztonsági kockázat: Az 5250 emulációnál, illetve bármilyen interaktív szekciónál a bejelentkezési képernyő semmiben sem különbözik a többi képernyőtől. Bár a beíráskor a jelszó nem jelenik meg a képernyőn, elküldésére a többi adatmezőhöz hasonlóan titkosítás nélkül kerül sor. Bizonyos összeköttetések esetén ez lehetőséget nyújt a betörni szándékozók számára a felhasználói azonosítók és jelszavak lehallgatására. Az összeköttetés elektronikus berendezéssel végzett megfigyelését gyakran hívják **lehallgatásnak** (sniffelésnek). A V4R4 kiadással kezdődően az iSeries Access és az iSeries szerver közötti kommunikáció titkosítható a Védett socket réteg (SSL) felhasználásával. Ez megvédi az adatokat, köztük a jelszavakat a lehallgatástól.

Ha a bejelentkezési képernyő kihagyását választja, akkor a PC titkosítja a jelszót az elküldés előtt. A titkosítás segítségével elkerülhető a jelszavak lehallgatással való megszerzése. Meg kell viszont győződni arról, hogy a felhasználók biztonságtudatosan járnak el tevékenységük során. Ha valaki felügyelet nélkül hagyja a számítógépét, amelyen egy iSeries szekció fut éppen, akkor ez lehetőséget nyújt arra, hogy valaki a felhasználói azonosító és jelszó ismerete nélkül új szekciót kezdeményezzen a rendszerrel. A számítógépeket úgy kell beállítani, hogy huzamosabb tétlenség esetén zárják le magukat, és csak jelszó megadása után legyenek használhatók ismét.

Az aktív szekcióval rendelkező felügyelet nélkül hagyott számítógépek a bejelentkezés kihagyásának engedélyezése nélkül is elegendő biztonsági kockázatot képviselnek. A PC szoftvereinek segítségével bárki indíthat egy szerver szekciót, amelyben adatokhoz férhet hozzá, és mindezt ismét a felhasználói azonosító és jelszó ismerete nélkül. 5250 emuláció esetén a kockázat valamivel nagyobb, mivel a szekció elindítása és az adatok elérése kevesebb ismeretet igényel.

A felhasználókat fel kell világosítani az iSeries Access szekciók szétkapcsolásának következményeiről. A legtöbb felhasználó logikusan, ám helytelenül feltételezi, hogy a szétkapcsolás teljesen leállítja a szerverrel felépített kapcsolatot. Valójában a szétkapcsolás kiválasztásakor a szerver annyit tesz, hogy elérhetővé teszi a felhasználó szekcióját (licencét) más felhasználók számára. A kliens kapcsolata a szerverrel mindezektől függetlenül még meg van nyitva. Ha valaki ilyenkor odasétál a magára hagyott számítógéphez, akkor felhasználói azonosító és jelszó megadása nélkül férhet hozzá a szerver erőforrásaihoz.

Két lehetőséget ajánlhat azoknak a felhasználóknak, akiknek szét kell kapcsolniuk a szekciókat:

- A számítógépen be kell állítani egy jelszót kérő zárolási funkciót. Ez megakadályozza a felügyelet nélküli számítógép használatát.
- A szekciók teljes szétkapcsolásához jelentkezzen ki a Windowsból, vagy indítsa újra a számítógépet. Ez befejezi az iSeries szerver szekcióját.

Emellett el kell magyarázni a felhasználóknak, hogy milyen potenciális biztonsági kockázatokat eredményez az iSeries Access for Windows használata. Amikor egy felhasználó UNC elérési úttal ad meg egy iSeries erőforrást, akkor a Windows operációs rendszer hálózati kapcsolatot épít fel a szerverrel. UNC megadásakor a felhasználó ezt az erőforrást nem leképezett hálózati meghajtóként látja. A felhasználó gyakran nincs is tudatában a hálózati kapcsolatnak. A hálózati kapcsolat viszont biztonsági kockázatot jelent, mivel egy felügyelet nélkül hagyott számítógépen a szerver a PC könyvtárfájában jelenik meg. Ha a felhasználói szekció ″erős″ felhasználói profillal került kialakításra, akkor a szerver erőforrásai könnyedén hozzáférhetők a felügyelet nélküli számítógépen. A korábbi példához hasonlóan a megoldást itt is azt jelenti, hogy a felhasználók legyenek tisztában a biztonsági kockázatokkal, és használják a számítógépük zárolási funkcióját.

Szerver védelme a távoli parancsokkal és eljárásokkal szemben

A hozzáértő felhasználók az iSeries Access vagy egy hasonló szoftver felhasználásával a bejelentkezési képernyő kihagyásával futtathatnak parancsokat a szerveren. A PC felhasználóknak számos lehetőségük van szerver parancsok futtatására. A felhasználók által használható módszereket a kliens/szerver szoftver határozza meg.

- A felhasználó megnyithat egy DDM fájlt, és a távoli parancs funkcióval futtathat parancsokat.
- Egyes szoftverek, egyebek között az iSeries Access optimalizált kliensek is, a távoli parancs funkciókat a DDM használata nélkül, az Osztott programhívás (DPC) API-k használatával biztosítják.
- Más szoftverek, például a távoli SQL és az ODBC úgy biztosítanak távoli parancs funkciókat, hogy ehhez sem a DDM-et, sem a DPC-t nem használják.

A DDM távoli parancs támogatással rendelkező szoftverek esetén a távoli parancsok a DDMACC hálózati attribútum használatával akadályozhatók meg teljes mértékben. Más szerver támogatást használó kliens/szerver szoftverek esetében végprogramokat jegyezhet be a szerveren. Ha engedélyezni kívánja a távoli parancsok futtatását, akkor győződjön meg róla, hogy az objektum jogosultsági séma megfelelő védelmet nyújt az adatok számára. A távoli parancs támogatás ugyanaz, mintha a felhasználók parancssorral rendelkeznének. Emellett

amikor az iSeries egy DDM távoli parancsot kap, akkor a felhasználói profil Képességek korlátozása (LMTCPB) paraméterének beállítását sem foganatosítja.

Munkaállomások védelem a távoli parancsokkal és eljárásokkal szemben

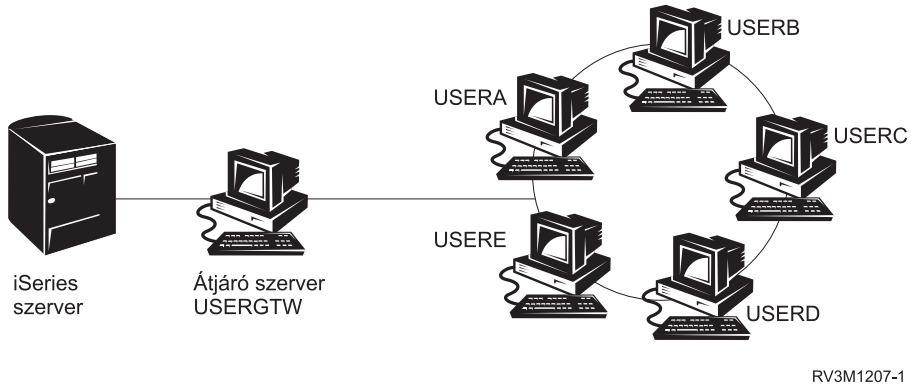
Az IBM iSeries Access for Windows lehetővé teszi távoli parancsok fogadását a számítógépen. A csatlakozó számítógépeken a szerver Távoli parancs futtatása (RUNRMTCMD) parancsával lehet parancsokat futtatni. A RUNRMTCMD funkció hasznos eszköz lehet a rendszeradminisztrátorok és a technikai támogatás számára. Emellett azonban lehetőséget nyújt a PC adatainak véletlen vagy akár szándékos megrongálására is.

A személyi számítógépek nem rendelkeznek az iSeries szerverekkel összehasonlítható szintű objektum jogosultsági funkciókkal. A RUNRMTCMD parancs használata során felmerülő lehetséges problémák kivédésére a legjobb módszer, ha gondosan megválogatja, hogy a rendszer milyen felhasználói legyenek jogosultak a parancs használatára. Az IBM iSeries Access for Windows lehetővé teszi az adott személyi számítógépen távoli parancsok futtatására jogosult felhasználók bejegyzését. TCP/IP feletti kapcsolatok esetén a távoli parancs hozzáférés az iSeries Access tulajdonságai alkalmazásban határozható meg a kliensen. A felhasználók felhatalmazása történhet felhasználói azonosító és távoli rendszernév alapján is. SNA kapcsolatok esetén bizonyos kliens szoftverek lehetővé teszik párbeszéd biztonság beállítását. Más kliensekben egyszerűen az állítható be, hogy engedélyezi-e a bejövő távoli parancs szolgáltatást.

Az adott környezetben használt kliens szoftverek és kapcsolattípusok (TCP/IP vagy SNA) összes kombinációjában meg kell vizsgálni a bejövő távoli parancsok lehetséges hatásait a hálózathoz csatlakozó személyi számítógépeken. Ehhez nézze meg a kliens dokumentációt, és keressen benne “bejövő parancsra” vagy a “RUNRMTCMD” parancsra vonatkozó információkat. Legyen felkészülve arra, hogy ellássa a PC felhasználókat és a hálózati adminisztrátorokat a kliensek helyes (biztonságos) beállítására vonatkozó útmutatásokkal.

Átjáró szerverek

Elképzelhető, hogy a rendszer olyan hálózat tagja, amelyben az iSeries rendszer és a számítógépek között köztes elem vagy átjáró található. Ilyen összeállítás például, amikor az iSeries rendszer egy PC szerveren keresztül csatlakozik a kliensek hálózatához. A helyzetből adódó biztonsági problémák jellege az átjáró szerveren futó szoftver képességeitől függ. Az 13. ábra: egy átjáró szervert alkalmazó konfigurációra mutat be egy példát.



13. ábra: iSeries rendszer átjáró szerverrel

Bizonyos szoftverek esetén az iSeries rendszer nem is tud az átjáró szerver másik végének felhasználóiról (a példában legyenek mondjuk USERA és USERC). A szerver a rendszerre való bejelentkezéshez egyetlen felhasználói azonosítót használ (USERGTW). A USERGTW felhasználói azonosító alatt történik az összes kliens kérés kezelése. A USERA felhasználótól származó kérések a rendszerre úgy jutnak el, mint a USERGTW kérései.

Ebben az esetben a biztonság foganatosítását az átjáró szervernek kell biztosítania. Ehhez meg kell ismernie az átjáró szerver biztonsági lehetőségeit és ezek kezelését. Az iSeries rendszer szemszögéből minden felhasználó azokkal a jogosultságokkal rendelkezik, amelyekkel az átjáró szerver által a szekció indításához használt felhasználói azonosító. Ez megfelel annak a helyzetnek, amikor egy átvett jogosultságot használó program parancssort biztosít a felhasználónak.

Más szoftverek esetén az átjáró szerver továbbadja az egyéni felhasználók kéréseit az iSeries rendszernek. Ilyenkor az iSeries rendszer tudja, hogy egy adott objektumhoz például a USERA felhasználó szeretne hozzáférni. Az átjáró ebben az esetben transzparens a rendszer számára.

Átjáró szervereket tartalmazó hálózatokban gondosan ki kell értékelni az átjáró szerverek által használt felhasználói azonosítóknak biztosítandó jogosultságok körét. Emellett meg kell ismernie a következőket is:
- Az átjáró szerveren foganatosított biztonsági mechanizmusok.
- Az átjáró mögötti felhasználók megjelenése az iSeries rendszer szemszögéből.

Vezetéknélküli LAN kommunikáció

Bizonyos környezetek szükségessé tehetik, hogy a kliensek egy része vezetéknélküli hálózaton kommunikáljon az iSeries szerverrel. Az iSeries vezetéknélküli LAN rádiófrekvenciás kommunikációs technológiát alkalmaz. Biztonsági adminisztrátorként tisztában kell lennie az iSeries vezetéknélküli LAN termékek alábbi biztonsági jellemzőivel:

- A vezetéknélküli LAN termékek szórt spektrumú technológiát alkalmaznak. Korábban ezt a technológiát a kormányzati szervek használták a rádiós kommunikáció védelmére. Az elektronikus eszközökkel megfigyelést végzők számára a forgalmazás tényleges kommunikáció helyett inkább zajnak tűnik.
- A vezetéknélküli kapcsolatok három biztonsággal kapcsolatos konfigurációs paraméterrel rendelkeznek:
  - Adatsebesség (két lehetséges adatsebesség)
  - Frekvencia (öt lehetséges frekvencia)
  - Rendszer azonosítója (8 millió lehetséges azonosító)

  Az elemek kombinációjával 80 millió lehetséges konfiguráció alakítható ki, amely jelentős mértékben csökkenti annak esélyét, hogy a betörők kitalálják a helyes konfigurációt.
- A többi kommunikációs módszerhez hasonlóan a vezetéknélküli kommunikáció biztonságát is jelentős mértékben befolyásolja a kliens eszköz biztonsága. A rendszer azonosítója és a többi konfigurációs paraméter egy fájlban található a kliens eszközön, amelyet ily módon védeni kell.
- A vezetéknélküli eszközök elvesztésekor vagy eltulajdonításakor a szerver szokásos biztonsági intézkedései, például a bejelentkezési jelszavak és az objektum jogosultságok védelmet nyújtanak az eltulajdonított eszköz felhasználásával végzett jogosulatlan hozzáférési kísérletek ellen.
- Egy vezetéknélküli kliens egység elvesztése vagy eltulajdonítása esetén fontolja meg a rendszer azonosító cseréjét minden felhasználónál, hozzáférési ponton és rendszeren. Ezt úgy kell tekinteni, mint a zárak szükségszerű lecserélését egy kulcskészlet eltulajdonításakor.

- Bizonyos helyetekben hasznos lehet a szerver klienscsoportokra particionálása, amelyek így egyedi rendszer azonosítókkal rendelkezhetnek. Ez korlátozza az egységek eltulajdonításából adódó lehetséges károkat. A módszer csak akkor működik, ha a felhasználók egy csoportja a környezet egy jól meghatározott területére lokalizálható.
- A vezetékes hálózatokban alkalmazott nyílt technológiákkal szemben a vezetéknélküli hálózatok egyéni technológiákra épülnek. Ennek megfelelően az efféle vezetéknélküli LAN termékekhez nincsenek nyilvánosan rendelkezésre álló elektronikus lehallgatókészülékek. (A lehallgatókészülék olyan elektronikus eszköz, amely lehetőséget ad a forgalmazás jogosulatlan megfigyelésére.)

15. fejezet Biztonsággal kapcsolatos végprogramok

Az iSeries szerver egyes funkciói kiegészítő ellenőrzési funkciókat megvalósító egyéni programok futtatására használható kilépési pontokat biztosítanak. Beállítható például úgy a rendszer, hogy minden alkalommal lefuttasson egy végprogramot, amikor egy felhasználó megpróbál megnyitni egy DDM (osztott adatkezelési) fájlt a rendszeren. A különféle helyzetekben futtatandó végprogramok meghatározására a bejegyzési funkció használható.

Biztonsági funkciókat végző végprogramokra vonatkozóan számos iSeries kiadvány tartalmaz példákat. Ezen végprogramokat, illetve példaprogramok forráskódját sorolja fel a 24. táblázat:.

24. táblázat: Példa végprogramok forrásai

Végprogram típusa	Felhasználás	Példák helye
Jelszó ellenőrzés	A QPWDVLDPGM rendszerváltozó megadhatja egy program nevét, vagy előírhatja a QIBM_QSY_VLD_PASSWRD kilépési ponton bejegyzett ellenőrzési programok használatát az új jelszavakra a QPWDxxx rendszerváltozókon túlmutatóan meghatározott speciális ellenőrzések végrehajtásához. A program használatát rendkívül gondosan meg kell figyelni, mivel titkosítatlan jelszavakat vesz át. A program **nem** tárolhatja fájlban vagy adhatja át más programnak a jelszavakat.	• *An Implementation Guide for iSeries Security and Auditing, GG24–4200* • *iSeries biztonsági összefoglaló*, SC22-0282-07
PC Support/400 vagy Client Access hozzáférés[1]	Ezt a programot a hálózati attribútumok kliens hozzáférési kérés (PCSACC) paraméterében állíthatja be a következő funkciók felügyeletének céljából: • Virtuális nyomtató funkciók • Fájlátviteli funkciók • 2. típusú osztott mappákkal kapcsolatos funkciók • Client Access üzenet funkciók • Adatsorok • Távoli SQL funkciók	*An Implementation Guide for iSeries Security and Auditing, GG24–4200*
Osztott adatkezelés (DDM) hozzáférés	Ezt a programot a hálózati attribútumok DDM hozzáférési kérés (DDMACC) paraméterében állíthatja be a következő funkciók felügyeletének céljából: • 0. és 1. típusú osztott mappákkal kapcsolatos funkciók • Távoli parancs küldési funkciók	*An Implementation Guide for iSeries Security and Auditing, GG24–4200*
Távoli bejelentkezés	A QRMTSIGN rendszerváltozóban megadhat egy programot, amely azt felügyeli, hogy milyen felhasználók jelentkezhetnek be automatikusan milyen helyekről (átjelentkezés).	*An Implementation Guide for iSeries Security and Auditing, GG24–4200*

24. táblázat: Példa végprogramok forrásai (Folytatás)

Végprogram típusa	Felhasználás	Példák helye
Nyílt adatbázis kapcsolat (ODBC) az iSeries Access termékkel[1]	A következő ODBC funkciók felügyeletére van lehetőség: • ODBC engedélyezése úgy általában. • iSeries adatbázisfájlokon engedélyezett függvények. • Engedélyezett SQL utasítások. • A szerver adatbázis objektumairól lekérdezhető információk. • Engedélyezett SQL katalógus funkciók.	Nincs.
QSYSMSG megszakítás kezelési program	Írható olyan program, amely figyeli a QSYSMSG üzenetsort, és az érkező üzenetek típusának megfelelően különféle tevékenységeket végezhet (például értesítheti a biztonsági adminisztrátort).	*An Implementation Guide for iSeries Security and Auditing, GG24–4200*
TCP/IP	Számos TCP/IP szerver biztosít kilépési pontokat (egyebek között a TFTP, a Telnet és a REXEC). A végprogramok segítségével kezelhetők a bejelentkezések, illetve ellenőrizhetők a kliensek például egy fájl letöltésére vagy feltöltésére vonatkozó kérései. Ezekkel a végprogramokkal biztosíthat anonim FTP funkciót is a rendszeren.	"*iSeries System API Reference* című kiadvány TCP/IP User Exits szakasza"
Felhasználói profilok változásai	Az alábbi felhasználói profillal kapcsolatos parancsokhoz hozhat létre végprogramokat: CHGUSRPRF CRTUSRPRF DLTUSRPRF RSTUSRPRF	• *iSeries biztonsági összefoglaló*, SC22-0282-07 • "*iSeries System API Reference* című kiadvány TCP/IP User Exits szakasza"

Megjegyzések:

1. A témát részletesebben az iSeries Információs központ tárgyalja. További részletek: "Előfeltétel és kapcsolódó információk" oldalszám: xii.

16. fejezet Internet böngészők biztonsági vonatkozásai

A vállalat legtöbb PC felhasználója valószínűleg használ web böngészőt a munkaállomásán. Elképzelhető, hogy az Internethez is csatlakoznak. Emellett csatlakozhatnak a helyi szerverhez is. Az alábbi biztonsági szempontok a személyi számítógépekre és a szerverre is vonatkoznak.

Kockázat: Munkaállomás károsodása

A felhasználók által meglátogatott weboldalakhoz tartozhat társított aktív tartalom, például Java kisalkalmazások, ActiveX vezérlőelemek vagy más bedolgozók. Bár ritka, az ilyen ″aktív tartalom″ a személyi számítógépen futva magában hordozza a lehetőséget PC információinak megrongálására. Biztonsági adminisztrátorként a vállalati számítógépek védelme érdekében érdemes megfontolni a következőket:

- Ismerje meg a felhasználók által használt különféle böngészők biztonsági lehetőségeit. Bizonyos böngészőknél például beállítható, hogy a Java kisalkalmazások milyen jogosultságokkal rendelkezzenek a böngészőn kívül. (A Java korlátozott működési környezetét *homokozónak* nevezik.) Ezzel megakadályozható, hogy a kisalkalmazások hozzáférjenek a PC adatokhoz.

  Megjegyzés: A homokozó koncepciója és az ebből adódó biztonsági korlátozások nem léteznek az ActiveX és egyéb bedolgozók esetén.
- Adjon tanácsokat a felhasználóknak a böngésző beállításaival kapcsolatban. Valószínűleg se ideje, se erőforrásai nincsenek arra, hogy ellenőrizze az ajánlások betartását. Ennek megfelelően fel kell világosítani őket a helytelen beállításokból adódó lehetséges kockázatokról.
- Fontolja meg a web böngészők szabványosítását a szükséges biztonsági beállítások központi meghatározásával.
- Utasítsa a felhasználókat, hogy értesítsék az adott webhelyekhez köthető valamennyi gyanús viselkedésről vagy tünetről.

Kockázat: iSeries katalógusok elérése leképezett meghajtókon keresztül

Tegyük fel, hogy egy PC IBM iSeries Access for Windows szekcióval csatlakozik a rendszerre. A szekció beállít néhány hálózati meghajtót az iSeries integrált fájlrendszerére. Például a PC **G** meghajtója a hálózat SYSTEM1 rendszerének integrált fájlrendszerére van leképezve.

Most tegyük fel, hogy ugyanennek a számítógépnek a felhasználója egy böngésző segítségével hozzáfér az Internethez. A felhasználó letölt egy rosszindulatú programot, például Java kisalkalmazást vagy ActiveX vezérlőelemet tartalmazó weboldalt. Elképzelhető, hogy a program funkciója a PC teljes G: meghajtójának törlése.

A leképezett meghajtókat érő rongálások elkerülésére számos módszer alkalmazható:

- A legfontosabb védelem itt is a szerver erőforrás biztonsága. A kártékony Java kisalkalmazás vagy ActiveX vezérlőelem a szerver szemszögéből ugyanaz, mint aki a PC szekciót kialakította. Ennek megfelelően pontosan meg kell határozni, hogy melyik felhasználó mit tehet meg a szerveren.

- Javasolja a PC felhasználóknak a böngészőjük beállítását a hálózati meghajtók használatának letiltására. Ez csak Java kisalkalmazások esetén működik, mivel az ActiveX vezérlőelemek nem ismerik a homokozó koncepcióját.
- Ismertesse a felhasználókkal, hogy milyen veszélyeket rejt magában, amikor egyidejűleg csatlakoznak az Internetre és a szerverre. Emellett értesse meg velük azt is (a Windows 95 kliensekkel például), hogy a hálózati meghajtók továbbra is megmaradnak, még akkor is, ha az iSeries szekció már úgy tűnik, hogy befejeződött.

Kockázat: Megbízható aláírt kisalkalmazások

A felhasználók lehet, hogy megfogadták a tanácsait, és beállították a böngészőjükben, hogy a kisalkalmazások ne tudjanak írni a PC meghajtóira. Ettől függetlenül a PC felhasználóknak figyelemmel kell lenniük arra, hogy az *aláírt kisalkalmazások* felülbírálhatják a böngésző ezen beállítását.

Az aláírt kisalkalmazások digitális aláírással rendelkeznek a hitelesítésük bizonyításához. Amikor a felhasználó aláírt kisalkalmazást tartalmazó weboldalra érkezik, akkor a böngésző üzenetet jelenít meg. Az üzenet megjeleníti a kisalkalmazás aláírását (aláíró és az aláírás időpontja). A felhasználó a kisalkalmazás elfogadásával engedélyezi a kisalkalmazásnak a böngésző biztonsági beállításainak felülbírálását. Az aláírt kisalkalmazások akkor is írhatnak a PC helyi meghajtóira, ha a böngésző alapértelmezett beállításai ezt megakadályozzák. Az aláírt kisalkalmazások emellett a rendszerre leképezett hálózati meghajtókra is tudnak írni, mivel szemszögükből ezek helyi meghajtóként jelentkeznek.

A helyi rendszerről kiszolgált saját Java kisalkalmazások esetén elképzelhető, hogy érdemes aláírt kisalkalmazásokat használnia. Mindazonáltal, utasítani kell a felhasználókat, hogy lehetőleg ne fogadjanak el ismeretlen forrásból származó aláírt kisalkalmazásokat.

17. fejezet Kapcsolódó információk

Kézikönyvek

- *APPC Programming*, SC41-5443-00 írja le az iSeries rendszer által biztosított APPC támogatást. A könyv segítséget nyújt APPC funkciókat használó alkalmazásprogramok fejlesztéséhez, illetve az APPC kommunikációs környezet beállításához. Részletekbe menően tárgyalja az APPC alkalmazásprogramokra vonatkozó szempontokat, a konfigurációs követelményeket és parancsokat, a problémakezelést illetve az általános hálózati megfontolásokat. A kiadvány az iSeries Információs központ CD-n található.
- *AS/400 Internet Security: Protecting Your AS/400 from HARM in the Internet* Redbook (SG24-4929) tárgyalja az iSeries Internetre csatlakoztatásával járó biztonsági kérdéseket és kockázatokat. Különféle példákat, javaslatokat, tippeket és technikákat sorol fel a TCP/IP alkalmazásokkal kapcsolatban.
- *Rendszermentés és visszaállítás*, SA12-7171-07 írja le a rendszermentési és helyreállítási stratégiák kialakítását, a rendszer információinak mentését, és a rendszer helyreállítását. A kiadvány az iSeries Információs központban található. A megadott témákat az iSeries Információs központ különféle témakörei is tárgyalják. További részletek: “Előfeltétel és kapcsolódó információk” oldalszám: xii.
- *CL Programming*, SC41-5721-06 részletes leírást biztosít a külsőleg leírható fájlok DDS meghatározásainak kódolásához. A fájlok fizikai, logikai, képernyő, nyomtató és rendszerközti kommunikációs funkcióval kapcsolatos (ICF) fájlok lehetnek. A kiadvány az iSeries Információs központban található.
- Az Információs központ CL parancsok témaköre (az elérésével kapcsolatos részleteket az “Előfeltétel és kapcsolódó információk” oldalszám: xii szakaszban találja) írja le az iSeries vezérlőnyelvét (CL) és az OS/400 parancsokat. Az OS/400 parancsok használhatók az Operating System/400 (5722-SS1) licencprogram funkcióinak kérésére. A más licencprogramokhoz, nyelvekhez és segédprogramokhoz kapcsolódó, vagyis nem OS/400 CL parancsokat a megfelelő licencprogramok dokumentációja tárgyalja.
- Wayne Madden, Carol Woodbury: *Implementing iSeries Security, 3rd Edition* Loveland, Colorado: 29th Street Press, a division of Duke Communications International, 1998. Ez a kiadvány iránymutatásokat és gyakorlati javaslatokat tartalmaz az iSeries biztonság megtervezéséhez, beállításához és kezeléséhez.

  ISBN rendelési szám:

  1-882419-78-2
- A HTTP szerverrel kapcsolatban további információkat a következő webhelyen talál:

  `http://www.ibm.com/eserver/iseries/software/http/docs/doc.htm`
- *iSeries biztonsági összefoglaló*, SC22-0282-07 – Ez a kiadvány nyújt összefoglaló információkat a biztonsággal kapcsolatos rendszerváltozóról, a felhasználói profilokról, az erőforrás biztonságról és a biztonsági megfigyelésről. A könyv nem tárgyalja a különféle licencprogramokkal, nyelvekkel és segédprogramokkal kapcsolatos biztonsági szempontokat. A kiadvány az iSeries Információs központban található.
- Az iSeries szerveren végrehajtandó alapfeladatokkal kapcsolatos koncepciókat az Információs központ Alapvető rendszerműveletek című témaköre írja le. További részletek: “Előfeltétel és kapcsolódó információk” oldalszám: xii.
- Az Információs központ tárgyalja a TCP/IP, illetve a különféle TCP/IP alkalmazások, például FTP, SMTP és Telnet beállítását és használatát. További részletek: “Előfeltétel és kapcsolódó információk” oldalszám: xii.

- *OS/400 TCP/IP fájlszerver támogatás Installation and User's Guide*, SC41-0125 – Ez a kiadvány mutatja be a Fájlszerver támogatás licencprogramot és írja le a rá vonatkozó beállítási eljárásokat. A könyv részletesen tárgyalja a termék funkcióit, emellett példákat mutat be a használatával kapcsolatban.
- *Trusted Computer Systems Evaluation Criteria* DoD 5200.28.STD – Ez a kiadvány írja le a különböző megbízhatósági szintet biztosító számítógéprendszerek kiértékelési feltételeit. A TCSEC az Egyesült Államok kormányának kiadványa. Megrendelhető a következő címen:

  Office of Standards and Products
  National Computer Security Center
  Fort Meade, Maryland 20755-6000 USA
  Attention: Chief, Computer Security Standards
- Az Információs központ számos témakört tartalmaz az iSeries rendszerfelügyelettel és jobkezeléssel kapcsolatban. Ilyen témakör például a Teljesítményadatok gyűjtése, a Rendszerváltozók kezelése és a Tárolókezelés. Az Információs központ elérésére vonatkozó részleteket az "Előfeltétel és kapcsolódó információk" oldalszám: xii szakaszban találja. A Jobkezelés (SC41-5306-03) című kiadvány tárgyalja a jobkezelési környezetek létrehozásával és beállításával kapcsolatos részleteket. A kiadvány az iSeries Információs központban található.

A felsorolt Információs központ témakörök és Kiegészítő kézikönyvek mellett a következő információforrásokból meríthet:

- **IBM SecureWay**
  Az IBM SecureWay az IBM biztonsági ajánlatait tartalmazó termékportfólió márkaneve, amelyben hardveres, szoftveres, konzultációs és támogatási szolgáltatások találhatók az IT erőforrások biztonságosabbá tételéhez. Legyen szó akár egyéni igények kielégítéséről, akár átfogó vállalati megoldások létrehozásáról, az IBM SecureWay ajánlatok magukban foglalják a biztonság tervezéséhez, kialakításához és fenntartásához szükséges szakértelmet. Az IBM SecureWay ajánlatokról további információkért látogasson el az IBM SecureWay honlapjára:

  `http://www.ibm.com/secureway`
- **Szerviz ajánlatok**
  Új hardverek vagy szoftverek telepítése nagy mértékben növelheti az üzletmenet hatékonyságát. Felveti viszont az üzleti műveletek megszakadásával és az állásidővel járó veszélyeket, amelyek értékes belső erőforrásokat vonhatnak el. Az IBM Global Services iSeries biztonsággal kapcsolatos szolgáltatásokat is nyújt. Az iSeries szerverekre vonatkozó szolgáltatások teljes listáját a következő címen találja:

  `http://www.as.ibm.com/asus`

Megjegyzések

Ez a tájékoztatás az Egyesült Államokban kínált termékekhez vagy szolgáltatásokhoz készült.

Az IBM lehet, hogy nem ajánlja az ebben a dokumentációban tárgyalt termékeket, szolgáltatásokat vagy kiegészítőket más országokban. Az adott országokban rendelkezésre álló termékekről és szolgáltatásokról a helyi IBM képviseletek szolgálnak felvilágosítással. Az IBM termékekre, programokra vagy szolgáltatásokra vonatkozó hivatkozások sem állítani, sem sugallni nem kívánják, hogy az adott helyzetben csak az IBM termékeit, programjait vagy szolgáltatásait lehet alkalmazni. Minden olyan működésében azonos termék, program vagy szolgáltatás alkalmazható, amely nem sérti az IBM szellemi tulajdonjogát. A nem IBM termékek, programok és szolgáltatások működésének megítélése és ellenőrzése természetesen a felhasználó felelőssége.

A dokumentum tartalmával kapcsolatban az IBM-nek bejegyzett, vagy bejegyzés alatt álló szabadalmai lehetnek. Jelen dokumentum nem ad semmiféle jogos licencet ezen szabadalmakhoz. Az írásos licenckérelmeket az alábbi címre küldheti:

IBM Director of Licensing
IBM Corporation
500 Columbus Avenue
Thornwood, NY 10594-1785
U.S.A.

Ha duplabyte-os (DBCS) információkkal kapcsolatban van szüksége licencre, akkor lépjen kapcsolatba az országában az IBM szellemi tulajdon osztályával, vagy írjon a következő címre:

IBM World Trade Asia Corporation
Licensing
2-31 Roppongi 3-chome, Minato-ku
Tokyo 106, Japan

A következő bekezdés nem vonatkozik az Egyesült Királyságra, valamint azokra az országokra, amelyeknek jogi szabályozása ellentétes a bekezdés tartalmával: AZ INTERNATIONAL BUSINESS MACHINES CORPORATION JELEN KIADVÁNYT "ÖNMAGÁBAN", BÁRMIFÉLE KIFEJEZETT VAGY VÉLELMEZETT GARANCIA NÉLKÜL ADJA KÖZRE, IDEÉRTVE, DE NEM KIZÁRÓLAG A JOGSÉRTÉS KIZÁRÁSÁRA, A KERESKEDELMI ÉRTÉKESÍTHETŐSÉGRE ÉS BIZONYOS CÉLRA VALÓ ALKALMASSÁGRA VONATKOZÓ VÉLELMEZETT GARANCIÁT. Bizonyos államok nem engedélyezik egyes tranzakciók kifejezett vagy vélelmezett garanciáinak kizárását, így elképzelhető, hogy az előző bekezdés Önre nem vonatkozik.

Jelen dokumentum tartalmazhat technikai, illetve szerkesztési hibákat. Az itt található információk bizonyos időnként módosításra kerülnek; a módosításokat a kiadvány új kiadásai tartalmazzák. Az IBM mindennemű értesítés nélkül fejlesztheti és/vagy módosíthatja a kiadványban tárgyalt termékeket és/vagy programokat.

A kiadványban a nem IBM webhelyek megjelenése csak kényelmi célokat szolgál, és semmilyen módon nem jelenti ezen webhelyek előnyben részesítését másokhoz képest. Az ilyen webhelyeken található anyagok nem képezik az adott IBM termék dokumentációjának részét, így ezek használata csak saját felelősségre történhet.

Az IBM legjobb belátása szerint bármilyen formában felhasználhatja és továbbadhatja a felhasználóktól származó információkat anélkül, hogy a felhasználó felé ebből bármilyen kötelezettsége származna.

Az ezen program licencével rendelkezők vegyék fel a kapcsolatot az alábbi címmel, ha információra van szükségük a következő célú engedélyezésekről: (i) információcsere függetlenül alkotott programok és más programok (ideértve ezt a programot is) között, és (ii) a kicserélt információ kölcsönös használata.

IBM Corporation
Software Interoperability Coordinator, Department 49XA
3605 Highway 52 N
Rochester, MN 55901
U.S.A.

Az ilyen információk bizonyos feltételek és kikötések mellett állnak rendelkezésre, ideértve azokat az eseteket is, amikor ez díjfizetéssel jár.

Az IBM a könyvben tárgyalt licencprogramokat és a hozzájuk tartozó licenc anyagokat IBM Vásárlói megállapodás, IBM nemzetközi programlicenc szerződés, vagy a felek azonos tartalmú megállapodása alapján biztosítja.

A könyvben található teljesítményadatok ellenőrzött környezetben kerültek meghatározásra. Ennek következtében a más működési körülmények között kapott adatok jelentősen különbözhetnek a dokumentumban megadottaktól. Egyes mérések fejlesztői szintű rendszereken kerültek végrehajtásra, így nincs garancia arra, hogy ezek a mérések azonosak az általánosan hozzáférhető rendszerek esetében is. Bizonyos mérések eredményei becslés és következtetés útján jöttek létre. A tényleges értékek eltérhetnek. A dokumentum felhasználóinak ellenőrizni kell az adatok alkalmazhatóságát az adott környezetben.

A nem IBM termékekre vonatkozó információk a termékek szállítóitól, illetve azok publikált dokumentációiból, valamint egyéb nyilvánosan hozzáférhető forrásokból származnak. Az IBM nem tesztelte ezeket a termékeket, így a nem IBM termékek esetében nem tudja megerősíteni a teljesítményre és kompatibilitásra vonatkozó, valamint egyéb állítások pontosságát. A nem IBM termékekkel kapcsolatos kérdéseivel forduljon az adott termék szállítóihoz.

Az IBM jövőbeli tevékenységére vagy szándékaira vonatkozó állításokat az IBM mindennemű értesítés nélkül módosíthatja, azok csak célokat jelentenek.

Jelen kiadvány csak tervezési célokat szolgál. A megadott információk megváltozhatnak a tárgyalt termékek elérhetővé válásáig.

Az információk között példaként napi üzleti tevékenységekhez kapcsolódó jelentések és adatok lehetnek. A valóságot a lehető legjobban megközelítő illusztrálás érdekében a példákban egyének, vállalatok, márkák és termékek nevei szerepelnek. Minden ilyen név a képzelet szüleménye, és valódi üzleti vállalkozások neveivel és címeivel való bármilyen hasonlóságuk teljes egészében a véletlen műve.

SZERZŐI JOGI LICENC:

A könyv forrásnyelvi példa alkalmazásokat tartalmaz, amelyek a programozási technikák bemutatására szolgálnak a különböző működési környezetekben. A példaprogramokat tetszőleges formában, az IBM-nek való díjfizetés nélkül másolhatja, módosíthatja és terjesztheti fejlesztési, használati, eladási vagy a példaprogram operációs rendszer alkalmazásprogram illesztőjének megfelelő alkalmazásprogram terjesztési céllal. Ezek a példák nem kerültek minden állapotban tesztelésre. Az IBM így nem tudja garantálni a

megbízhatóságukat, javíthatóságukat vagy a program funkcióit. A példaprogramokat tetszőleges formában, az IBM-nek való díjfizetés nélkül másolhatja, módosíthatja és terjesztheti fejlesztési, használati, eladási vagy az IBM alkalmazásprogram illesztőjének megfelelő alkalmazásprogram terjesztési céllal.

Ha a fenti szöveget elektronikus formában olvassa, akkor elképzelhető, hogy nem jelennek meg a fotók és színes ábrák.

Védjegyek

Az alábbi kifejezések az IBM Corporation védjegyei az Egyesült Államokban és/vagy más országokban:

Advanced Peer-to-Peer Networking
APPN
AS/400
DB2
DRDA
e (embléma)
IBM
iSeries
Net.Data
Operating System/400
OS/400
PowerPC
SecureWay
System/36
System/38
400

Az ActionMedia, a LANDesk, az MMX, a Pentium és a ProShare az Intel Corporation védjegye vagy bejegyzett védjegye az Egyesült Államokban és/vagy más országokban.

A Microsoft, Windows, Windows NT és Windows embléma a Microsoft Corporation védjegye az Egyesült Államokban és/vagy más országokban.

A Java és az összes Java alapú védjegy a Sun Microsystems, Inc. védjegye az Egyesült Államokban és/vagy más országokban.

A UNIX az Open Group bejegyzett védjegye az Egyesült Államokban és más országokban.

Más cégek, termékek vagy szolgáltatások nevei mások védjegyei, szolgáltatás jegyei vagy egyéb tulajdonai lehetnek.

Tárgymutató

Különleges jelek

számok

A, Á

B

C

CS

D

E, É

F

G

GY

H

I, Í

J

K

L

M

N

NY

O, Ó

P

Q

R

S

SZ

T

U, Ú

Ü, Ű

V

W

Olvasóink írják

iSeries
iSeries biztonsági tanácsok és technikák
5. verzió

Kiadványszám SC22-5311-07

Szeretnénk megismerni a jelen kiadványról alkotott véleményét. Kérjük, nyíltan írja meg a jelen könyv egyes hibáit, pontatlanságait, szerkezeti vagy témakörbeli hiányosságait. Kérjük, hogy megjegyzéseit korlátozza a jelen könyvben foglalt tájékoztatásra és e tájékoztatás megjelenítési módjára.

Ha műszaki kérdései vannak, vagy termékekről és árakról szeretne tájékozódni, keresse föl a helyi IBM kirendeltséget, IBM üzlettársat vagy meghatalmazott viszonteladót.

Megjegyzései elküldésével (nem kizárólagos) jogot ad az IBM-nek arra, hogy belátása szerint használja vagy terjessze az Ön megjegyzéseit, anélkül, hogy ezzel bármilyen kötelezettséget róna Önre.

Megjegyzések:

Köszönjük támogatását.

Véleményét sokféleképpen eljuttathatja hozzánk:
- Megjegyzéseit küldje el a jelen űrlap túloldalán látható címre.
- Küldjön távmásolatot a következő számra: Egyesült Államok és Kanada: 1-800-937-3430
- Megjegyzéseit küldje el elektronikus levélben erre a címre: RCHCLERK@us.ibm.com

Ha szeretne választ kapni az IBM-től, kérjük, adja meg a következő adatokat:

Név	Cím
Vállalat	
Telefonszám	Elektronikus levelezési cím

Olvasóink írják
SC22-5311-07

IBM

IBM CORPORATION
ATTN DEPT 542 IDCLERK
3605 Highway 52 N
ROCHESTER MN

Nyomtatva Dániában

SC22-5311-07