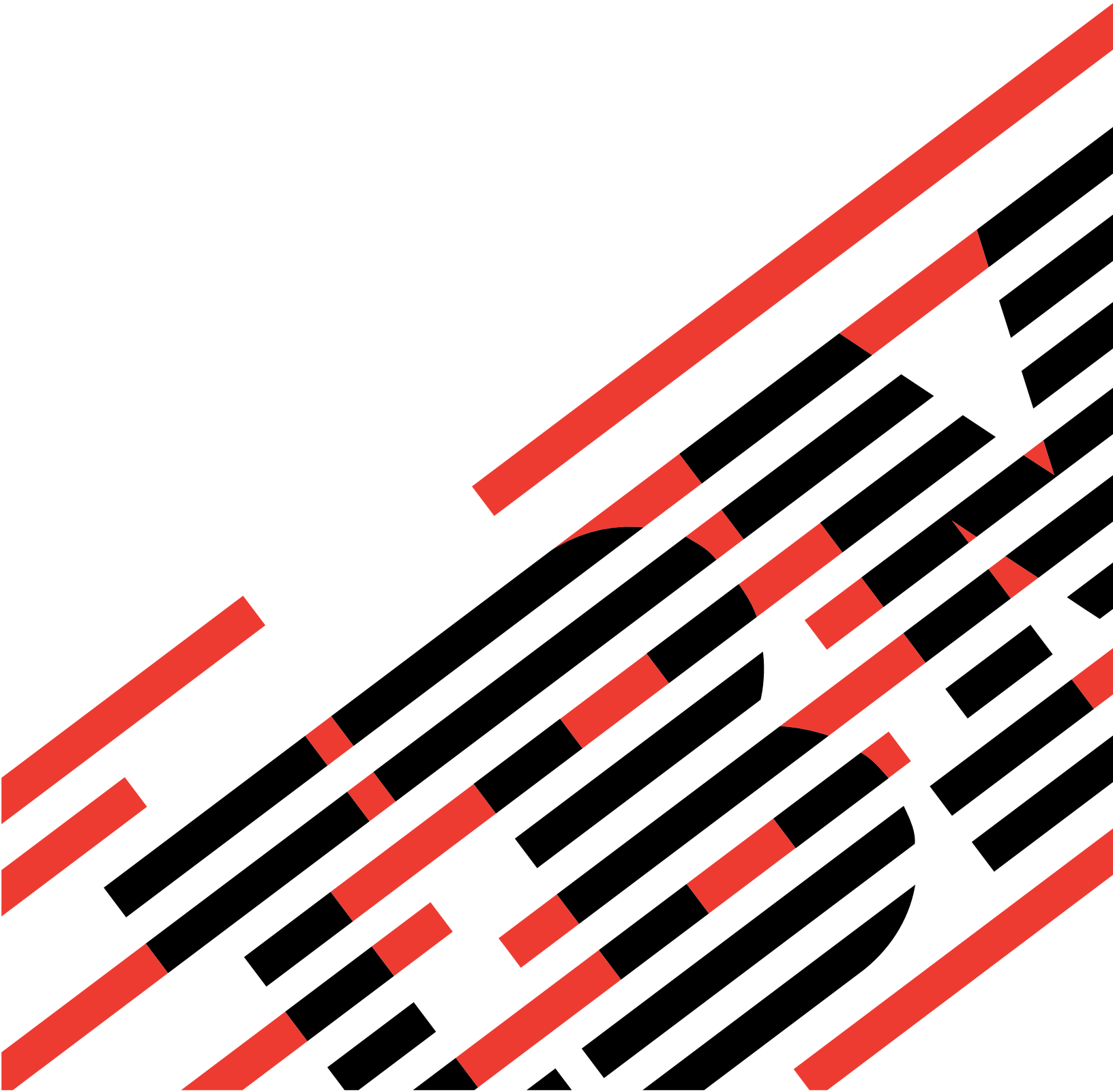
IBM

eserver

iSeries

Základné zabezpečenie systému a plánovanie

Verzia 5 vydanie 3



IBM

@server

iSeries

Základné zabezpečenie systému a plánovanie

Verzia 5 vydanie 3

Poznámka

Skôr, ako použijete tieto informácie a produkt, ktorý podporujú, určite si prečítajte informácie v časti “Oznamy”, na strane 129.

Piate vydanie (August 2005)

Toto vydanie sa týka verzie 5, vydania 3, modifikácie 0 operačného systému IBM Operating System/400 (číslo produktu 5722-SS1) a všetkých nasledujúcich vydaní a modifikácií, pokiaľ nebude v nových vydaniach uvedené inak. Táto verzia nebeží na všetkých modeloch RISC (reduced instruction set computer) a nebeží ani na modeloch CICS.

Obsah

Základné zabezpečenie systému a plánovanie

Základná bezpečnosť systému a plánovanie poskytuje detailné informácie o plánovaní a nastavovaní bezpečnosti iSeries. Táto téma zdôrazňuje plánovanie a poskytuje formuláre, ktoré môžete použiť pri plánovaní a zaznamenávaní vašich rozhodnutí týkajúcich sa bezpečnosti. Poskytuje aj podrobné inštrukcie na nastavenie základného zabezpečenia systému. Vzhľadom na to, že táto téma je charakteru pracovnej knižky, možno si ju budete chcieť vytlačiť, aby ste si mohli tento materiál pozrieť dôkladnejšie.

Nastavenie najlepšej bezpečnosti vášho systému iSeries pozostáva z dvoch hlavných skupín aktivít: plánovacích úloh a konfiguračných úloh. Pri nastavovaní bezpečnosti tak, aby to zodpovedalo potrebám vášho podniku, by ste si mali pozrieť tieto témy plánovania:

- Téma Začíname so základným zabezpečením systému poskytuje prehľad všeobecných základných bezpečnostných pojmov a odpovedá na otázky o základnom zabezpečení systému.
- Téma Plánovanie užívateľského zabezpečenia poskytuje informácie o tom, ako sa má plánovať zabezpečenie, ktoré ovplyvňuje užívateľov vo vašom systéme. Zahŕňa to fyzické zabezpečenie, aplikačné zabezpečenie, celkovú stratégiu zabezpečenia a užívateľské profily vo vašom systéme.
- Téma Plánovanie zabezpečenia prostriedkov poskytuje informácie o tom, ako sa má plánovať zabezpečenie objektov vo vašom systéme, vrátane knižníc a objektov v nich, tlačiarní, tlačového výstupu a pracovných staníc.

Po dokončení plánovacích činností si môžete pozrieť tieto témy, aby vám pomohli nastaviť zabezpečenie vášho systému:

- Téma Nastavenie užívateľského zabezpečenia poskytuje podrobnosti o nastavovaní užívateľského a skupinového zabezpečenia.
- Téma Nastavenie zabezpečenia prostriedkov poskytuje informácie o tom, ako sa má nastaviť vlastníctvo objektov, verejné a špecifické oprávnenia pre objekty a zabezpečenie pre tlačiarne a pracovné stanice.
- Téma Testovanie zabezpečenia poskytuje informácie o testovaní zabezpečenia.
- Téma Zmena bezpečnostných informácií poskytuje informácie o aktualizovaní a modifikovaní užívateľských a skupinových profilov a zabezpečenia prostriedkov.
- Téma Uloženie bezpečnostných informácií poskytuje informácie o zálohovaní bezpečnostných informácií.
- Téma Monitorovanie zabezpečenia poskytuje kontrolné zoznamy pre sledovanie zabezpečenia a informácie o auditovaní zabezpečenia.

Okrem týchto tém použite plánovacie formuláre na zdokumentovanie vašich plánovacích stratégií a bezpečnostných rozhodnutí.

Tlač tejto témy

Môžete si zobraziť alebo stiahnuť PDF verziu tohto dokumentu na prezeranie alebo tlač. Aby ste si mohli prezerať PDF súbory, musíte mať nainštalovaný prezerač Adobe® Acrobat® Reader. Kópiu prezerača si môžete stiahnuť z domovskej stránky Adobe 

Keď chcete zobraziť alebo stiahnuť PDF verziu, vyberte Základné zabezpečenie systému a plánovanie (950 KB alebo 164 strán).

Keď chcete uložiť PDF na pracovnej stanici pre prezeranie alebo tlač:

1. Otvorte PDF v prehliadači (kliknite na vyššie uvedený odkaz).
2. V ponuke prehliadača kliknite na **File**.
3. Kliknite na **Save As...**
4. Prejdite do adresára, kam chcete uložiť PDF.

5. Kliknite na **Save**.

Začínate so základným zabezpečením systému

Všetci od systémového administrátora až po užívateľov by sa mali starať o bezpečnosť. Systémová bezpečnosť chráni iSeries a vaše citlivé podnikové informácie pred úmyselnými aj neúmyselnými bezpečnostnými narušeniami.

Na základe vášho bezpečnostného prostredia a požiadaviek si bezpečnosť vášho systému môžete prispôsobiť.

Zabezpečenie berte ako vstup do vášho systému. Bezpečnostné funkcie používajte na **uzamknutie** alebo ochranu vašich informácií pred neoprávneným použitím.

Bezpečnostné funkcie môžete použiť aj na **odomknutie** prispôsobivosti systému a prispôsobiť ju pre každého užívateľa.

Kvalitný bezpečnostný plán môže chrániť váš systém, no nemôže zaručiť bezpečnosť vášho zariadenia alebo vašich informácií. Systémové zodpovednosti by ste mali rozdeliť medzi viacerých zamestnancov, aby ste zabezpečili, že váš systém nebude riadiť výlučne jedna osoba.

Základné zabezpečenie systému a plánovanie vám poskytuje postupný prístup k plánovaniu a nastaveniu základného zabezpečenia systému. Táto téma kladie dôraz na dôležitosť plánovania bezpečnosti systému a poskytuje plánovacie formuláre, ktoré použijete na zaznamenávanie vašich rozhodnutí o bezpečnosti. V celej tejto téme nájdete príklad firmy, ktorá plánuje bezpečnosť, čo vám môže pomôcť pri vašom rozhodovaní o bezpečnosti.

Ak chcete, aby zabezpečenie systému prebehlo naozaj úspešne, základom je jeho kvalitné a dôkladné naplánovanie. V týchto témach sa dozviete o požiadavkách na základné zabezpečenie a o dôležitosti plánovania bezpečnosti:

- Často kladené otázky o základnom zabezpečení systému
- Prehľad základného zabezpečenia systému
- Metóda plánovania základného zabezpečenia systému

Kvalitný plán by ste mali mať aj pre zálohovanie a obnovu všetkých informácií vo vašom systéme. Okrem toho by ste mali naplánovať aj výmenu vášho zariadenia v prípade katastrofy. Bližšie informácie o koncepcii kvalitného plánu zálohovania nájdete v téme Zálohovanie a obnova v Informačnom centre.

Podrobné informácie o plánovaní bezpečnosti užívateľov

Techniky plánovania bezpečnosti užívateľov nájdete v nasledujúcich témach:

- Plánovanie bezpečnosti pre vaše aplikácie
- Plánovanie vašej bezpečnostnej stratégie
- Plánovanie skupín užívateľov
- Plánovanie individuálnych užívateľských profilov

Podrobné informácie o plánovaní zabezpečenia prostriedkov

Nasledujúce témy poskytujú systematický prístup k plánovaniu zabezpečenia prostriedkov pre vašich užívateľov.

- Pochopenie typov oprávnení
- Plánovanie bezpečnosti pre knižnice aplikácií
- Určenie vlastníctva knižníc a objektov
- Zoskupovanie objektov
- Ochrana tlačového výstupu
- Ochrana pracovných staníc
- Plánovanie inštalácie vašich aplikácií

Vytlačiteľné plánovacie formuláre

Základné zabezpečenie systému a plánovanie poskytuje vytlačiteľné plánovacie formuláre, ktoré vám umožňujú zaznamenávať všetky vaše rozhodnutia o bezpečnosti. Celú túto tému môžete vytlačiť ako PDF alebo ako jednotlivé plánovacie formuláre pomocou tlačidla pre tlač vo vašom prehliadači.

Pokyny k jednotlivým krokom nastavenia vášho základného zabezpečenia systému

Po naplánovaní bezpečnosti vám táto téma poskytne kroky k zrealizovaniu tohto vášho plánu. Nasledujúce témy vám pomôžu nastaviť bezpečnosť vášho systému.
- Nastavenie bezpečnosti užívateľov
- Nastavenie zabezpečenia prostriedkov

Často kladené otázky o základnom zabezpečení systému

Keď si pozriete odpoveď na tieto často kladené otázky o bezpečnosti, lepšie pochopíte význam bezpečnosti vášho systému.

Prečo je bezpečnosť dôležitá ?

Informácie, uložené vo vašom systéme, sú jednou z najdôležitejších súčastí majetku vašej firmy. Keď rozmýšľate, ako chrániť informácie, ktoré sú súčasťou majetku vašej firmy, majte na pamäti tri dôležité ciele:
- **Dôvernosť:** Kvalitné bezpečnostné opatrenia môžu zabrániť ľudom v prezeraní a odhaľovaní dôverných informácií.
- **Integrita:** Dobre navrhnutý bezpečnostný systém môže do určitej miery zabezpečiť presnosť informácií na vašom počítači. Správnym zabezpečením môžete zabrániť neautorizovaným zmenám alebo vymazávaniu údajov.
- **Dostupnosť:** Ak niekto náhodne alebo úmyselne poškodí údaje vo vašom systéme, k týmto prostriedkom nemáte prístup, kým ich neobnovíte. Kvalitný bezpečnostný systém môže zabrániť tomuto druhu poškodenia.

Keď užívatelia rozmýšľajú o bezpečnosti systému, zvyčajne rozmýšľajú o ochrane svojho systému pred osobami zvonka, akými môžu byť obchodní konkurenti. Skutočne, ochrana pred zvedavosťou alebo nehodami systému, spôsobenými vlastnými užívateľmi, je často najväčšou výhodou dobre navrhnutého bezpečnostného systému. V systéme bez kvalitných bezpečnostných funkcií môže užívateľ neúmyselne vymazať dôležitý súbor. Dobre navrhnutý bezpečnostný systém pomáha predchádzať tomuto typu nehody.

Keď sa rozhodujete, nakoľko potrebujete mať svoj systém zabezpečený, položte si nasledujúce otázky:
- Akú dôležitosť má váš počítač (a údaje, ktoré do neho ukladáte) pre vašu firmu?
- Máte firemnú politiku, ktorú vyžadujú určité úrovne bezpečnosti ?
- Vyžadujú vaši audítori úroveň bezpečnosti informácií, uložených na vašom počítači ?
- Budete v blízkej budúcnosti potrebovať istý stupeň bezpečnosti ?

Prečo treba prispôsobiť váš systém ?

Systém iSeries pokrýva široký rozsah užívateľov. Na malom systéme môžu byť traja až piati užívatelia, ktorí používajú niekoľko aplikácií. Na veľkom systéme môžu byť tisíce užívateľov vo veľkej komunikačnej sieti, ktorí používajú mnoho aplikácií.

Dizajn systému iSeries poskytuje veľkú flexibilitu na prispôsobenie širokému rozsahu užívateľov a situácií. Máte možnosť veľa zmeniť v tom, ako tento systém vyzerá z pohľadu vašich užívateľov a ako funguje.

Keď dostanete nový systém, pravdepodobne ho nebudete musieť alebo chcieť veľmi prispôsobovať. IBM dodáva systém s úvodnými nastaveniami, nazývanými **štandardné nastavenia**, pre mnoho volieb. Týmito štandardnými nastaveniami sú voľby, ktoré zvyčajne najlepšie fungujú v prípade nových inštalácií.

Poznámka: Všetky nové systémy sa dodávajú so štandardnou úrovňou bezpečnosti, ktorá je **40**. Táto úroveň bezpečnosti zabezpečuje, že tento systém môžu používať len užívatelia, ktorých zadefinujete. Zabraňuje tiež možnej integrite bezpečnostných rizík z programov, ktoré vedia bezpečnosť obchádzať.

Ak však systém trocha prispôsobíte, môžete ho urobiť jednoduchším a účinnejším nástrojom pre vašich užívateľov. Môžete napríklad zabezpečiť, aby užívateľ pri prihlásení dostal správnu ponuku. Môžete zabezpečiť, aby každá správa od užívateľa odišla na správnu tlačiareň. Vaši užívatelia budú tomuto systému viac dôverovať, ak ho na začiatku trocha prispôsobíte tak, aby mali pocit, že je to ich vlastný systém.

Kto má byť zodpovedný ?

Rôzne spoločnosti pristupujú k bezpečnosti rôzne. Zodpovednosť za všetky aspekty bezpečnosti majú niekedy programátori. V iných prípadoch nesie zodpovednosť za bezpečnosť aj osoba, ktorá manažuje systém. Ak nemáte istotu, ako prideliť zodpovednosť vo vašej spoločnosti, navrhujeme tento spôsob:

- Vaša metóda plánovania zabezpečenia prostriedkov závisí od toho, či vaša spoločnosť kupuje alebo vyvíja aplikácie. Ak vyvíjate vlastné aplikácie, odovzdajte vaše požiadavky na zabezpečenie prostriedkov počas procesu ich vyvíjania. Ak aplikácie kupujete, dohovorte sa a spolupracujte s návrhárom týchto aplikácií. V oboch prípadoch by projektanti, ktorí aplikácie navrhujú, mali bezpečnosť považovať za súčasť návrhu.
- Za nastavenie bezpečnosti by mal zodpovedať správca bezpečnosti. Správca bezpečnosti definuje užívateľov systému a ich prístup do systému. Správca bezpečnosti často zodpovedá za ďalšie záležitosti vo vašom systéme, napríklad za zálohovanie a obnovu informácií.
- Správca bezpečnosti by mal váš systém aj prispôsobovať, pretože mnoho prvkov bezpečnosti hrá v prispôsobovaní systému dôležitú úlohu.

Bez ohľadu na metódu, ktorú použijete na pridelenie zodpovednosti za bezpečnosť, **deklarujte bezpečnostnú politiku**. Riadiaci pracovník vo vašej spoločnosti musí všetkým oznámiť, najlepšie písomne, že informácie vo vašom počítači sú dôležitou súčasťou majetku spoločnosti. Tieto informácie musíte chrániť rovnako, ako by ste chránili súčasť majetku inej spoločnosti. Príklad bezpečnostnej politiky nájdete v časti ″Príklad: Bezpečnostná politika spoločnosti JKL Toy Company″.

Teraz, keď chápete potrebu bezpečnosti vášho systému, pravdepodobne si budete chcieť pozrieť prehľad úvah o bezpečnosti systému.

Prehľad základného zabezpečenia systému

Ak chcete plánovať efektívne, musíte pochopiť, ako sa vaše stanovisko k tomu, čo chcete uskutočniť, týka nástrojov, poskytovaných systémom. Na dosiahnutie vašich cieľov musíte vedieť, ako užívateľ a systémové funkcie spolupracujú.

Nasledujúce témy predstavujú dôležité časti bezpečnosti a prispôsobenia a ukážu vám, v akom sú súlade. Tieto témy vám majú poskytnúť prehľad predtým, než začnete plánovať. Všetky pojmy, ktoré sú tu uvedené, sú vysvetlené podrobnejšie, pretože sú potrebné v procese plánovania.

- Zabudovaná bezpečnosť systému
- Základná terminológia
- Názor užívateľa na bezpečnosť
- Systémové nástroje pre bezpečnosť a prispôsobenie

Zabudovaná bezpečnosť systému

Všetky časti systémovej stránky bezpečnosti sú zabudované do systému. Nie sú osobitným produktom, ktorý sa dá kúpiť. Tento integrovaný prístup má niekoľko výhod:

- Bezpečnosť je v súlade so zvyškom operačného systému. Používa rovnaké obrazovky, príkazy a terminológiu.
- Užívatelia sa bezpečnosti nemôžu vyhnúť, pretože to nie je osobitná časť softvéru.
- Správne navrhnutá bezpečnosť má minimálny vplyv na výkon.
- Bezpečnosť vždy drží krok s novými vývojmi softvéru. Keď sa nové funkcie stanú dostupnými, stane sa dostupnou aj bezpečnosť týchto funkcií.

Server iSeries sa dodáva s úrovňou bezpečnosti 40, ktorá chráni neautorizovaných užívateľov pred prihlásením na tento systém. Zabraňuje tiež možnej integrite bezpečnostných rizík z programov, ktoré vedia bezpečnosť obchádzať. Určité nastavenia bezpečnosti však môžete prispôsobiť alebo môžete zmeniť úrovne bezpečnosti. Úrovne bezpečnosti sú opísané v téme ″Výber vašej úrovne bezpečnosti.″

Teraz, keď lepšie rozumiete ako funguje zabudovaná bezpečnosť, môžete sa zoznámiť s bežnou terminológiou iSeries .

Základná terminológia

Táto časť všeobecnej terminológie je veľmi dôležitá pre pochopenie a porozumenie bezpečnosti iSeries:

Objekt Objekt je pomenovaný priestor v systéme, s ktorým sa dá narábať. Najbežnejšími príkladmi objektov sú súbory a programy. Medzi ďalšie typy objektov patria príkazy, fronty, knižnice a zložky. Objekty sa v systéme identifikujú podľa názvu objektu, typu objektu a knižnice, v ktorej je objekt umiestnený. Každý objekt v systéme je možné zabezpečiť.

Knižnica
Knižnica je zvláštnym typom objektu, ktorý sa používa na zoskupovanie ďalších objektov. Mnohé objekty v systéme sú umiestnené v knižnici.

Adresár
Adresár je ďalším spôsobom zoskupovania objektov v systéme. Objekty môžu byť umiestnené v adresári. Adresár môže byť umiestnený v ďalšom adresári, tvoriac hierarchickú štruktúru.

Teraz, keď lepšie rozumiete všeobecnej bezpečnostnej terminológii iSeries, môžete si pozrieť ako užívateľ vidí bezpečnosť.

Názor užívateľa na bezpečnosť

Bezpečnosť má z pohľadu užívateľov vplyv na to, ako používajú a vykonávajú úlohy v systéme. Zahrňuje aj spôsob ich interakcie so systémom, aby mohli tieto úlohy vykonávať. Je dôležité uvedomiť si, ako bude užívateľ bezpečnosť posudzovať. Napríklad nastavenie hesiel tak, aby stratili platnosť každých päť dní, by užívateľa znechutilo a prekážalo by mu vo vykonávaní jeho úloh. Na druhej strane, príliš uvoľnená politika hesiel by mohla spôsobiť bezpečnostné problémy.

Aby ste mohli pre váš systém poskytnúť správnu bezpečnosť, musíte ju rozdeliť na konkrétne časti, ktoré môžete plánovať, manažovať a monitorovať. Z pohľadu užívateľa môžete bezpečnosť vášho systému rozdeliť na niekoľko častí:

Fyzický prístup k systému

Fyzické zabezpečenie chráni systémovú jednotku, všetky systémové zariadenia a zálohovacie úložné médiá, napríklad diskety, pásky alebo CD pred náhodnou alebo úmyselnou stratou alebo poškodením.

Väčšina opatrení, ktoré prijmete na fyzické zabezpečenie vášho systému, sú vzhľadom na systém externými opatreniami. Systém sa však dodáva s uzamykateľným vypínačom alebo elektronickým kľúčom, ktorý zabraňuje neoprávnenému používaniu funkcií systémovej jednotky.

Téma ″Plánovanie fyzického zabezpečenia″ poskytuje podrobné informácie, ktoré vám pomôžu naplánovať fyzické zabezpečenie vášho systému.

Ako sa užívatelia prihlasujú

Bezpečnosť prihlasovania zabraňuje prihlásiť sa osobe, ktorá nie je v systéme identifikovaná. Aby sa jednotlivec mohol prihlásiť, musí zadať platnú kombináciu užívateľského ID a hesla.

Ak chcete zabezpečiť, aby vaša bezpečnosť prihlasovania nebola narušená, môžete použiť systémové hodnoty aj individuálne užívateľské profily. Môžete napríklad vyžadovať, aby sa heslá pravidelne menili. Rovnako môžete zabrániť používaniu hesiel, ktoré je ľahké uhádnuť.

Čo smú užívatelia robiť

Dôležitým poslaním bezpečnosti a prispôsobenia systému je zadefinovanie, čo smú užívatelia robiť. Z hľadiska bezpečnosti je to často **obmedzujúca** funkcia, ktorá napríklad bráni užívateľom vidieť určité informácie. Z hľadiska prispôsobenia systému je to **oprávňujúca** funkcia. Správne prispôsobený systém umožňuje užívateľom dobre vykonávať ich úlohy tým, že odstráni nepotrebné úlohy a informácie.

Niektoré metódy na zadefinovanie, čo smú užívatelia robiť, sú vhodné pre správcu bezpečnosti, kým ďalšie sú v zodpovednosti programátorov. Tieto informácie sa zameriavajú v prvom rade na to, čo zvyčajne robí správca bezpečnosti. Opisy pre všetky systémové hodnoty nájdete v kapitole 3 ″Security System Values″, v publikácii

Security-Reference (SC41-5302).

V individuálnych užívateľských profiloch, opisoch úloh a triedach sú k dispozícii parametre na určenie, čo smie užívateľ v systéme robiť. Nižšie uvedený zoznam stručne opisuje dostupné techniky:

Obmedzenie užívateľov na používanie niekoľkých funkcií
Užívateľov môžete na základe ich užívateľského profilu obmedziť na používanie konkrétneho programu, ponuky alebo skupiny ponúk a niekoľkých systémových príkazov. Užívateľské profily zvyčajne vytvára a riadi správca bezpečnosti.

Obmedzenie systémových funkcií
Systémové funkcie vám umožňujú ukladať a obnovovať informácie, manažovať tlačový výstup a nastavovať nových užívateľov systému. Každý užívateľský profil špecifikuje, ktorú z najbežnejších systémových funkcií môže užívateľ vykonávať.

Na serveri iSeries vykonávate systémové funkcie pomocou príkazu riadiaceho jazyka (CL) a aplikačných programovacích rozhraní (API). Pretože každý príkaz a API je objektom, na určenie, kto ich môže používať a vykonávať systémové funkcie, môžete použiť oprávnenia na objekt.

Určenie, kto môže používať súbory a programy
Zabezpečenie prostriedkov poskytuje schopnosť riadiť používanie každého objektu v systéme. V prípade každého objektu môžete určiť, kto a ako ho môže používať. Môžete napríklad určiť, že jeden užívateľ môže len prezerať informácie v súbore; ďalší užívateľ môže v tomto súbore meniť údaje; tretí užívateľ môže tento súbor meniť alebo ho celý vymazať.

Zabránenie zneužitiu systémových prostriedkov
Schopnosť spracovávania vo vašom systéme sa môže stať rovnako dôležitou pre váš podnik ako údaje, ktoré v ňom ukladáte. Správca bezpečnosti pomáha zabezpečiť, aby užívatelia nezneužívali systémové prostriedky na spúšťanie svojich úloh s vysokou prioritou, netlačili ako prvé svoje správy alebo nepoužívali príliš veľa diskového priestoru.

Ako komunikuje váš systém s inými počítačmi

Ak váš systém komunikuje s inými počítačmi alebo s programovateľnými pracovnými stanicami, pravdepodobne bude potrebné prijať ďalšie bezpečnostné opatrenia. Ak nemáte správne ovládacie prvky bezpečnosti, niekto na inom počítači vo vašej sieti môže spustiť úlohu alebo sa môže dostať k informáciám vo vašom počítači bez toho, aby prešiel procesom prihlásenia.

Na určenie, či povolíte vzdialené úlohy, vzdialený prístup k údajom alebo prístup do vášho systému zo vzdialeného PC, môžete použiť systémové hodnoty aj sieťové atribúty. Ak povolíte vzdialený prístup, môžete špecifikovať, ktorú bezpečnosť treba uplatniť. Opisy pre všetky systémové hodnoty nájdete v kapitole 3 ″Security System Values″, v

publikácii *Security-Reference* (SC41-5302).

Ako ukladať vaše bezpečnostné informácie

Informácie vo vašom systéme musíte pravidelne zálohovať. Okrem ukladania údajov do vášho systému musíte ukladať aj bezpečnostné informácie. V prípade katastrofy musíte byť schopný obnoviť informácie o užívateľoch systému, informácie o oprávneniach a informácie samy o sebe.

Téma ″Ukladanie bezpečnostných informácií″ vysvetľuje, ako sa ukladajú bezpečnostné informácie. Téma Zálohovanie a obnova v Informačnom centre poskytuje podrobnejšie informácie o zálohovaní a obnove bezpečnostných údajov.

Ako monitorovať váš plán bezpečnosti

Systém poskytuje niekoľko nástrojov na monitorovanie efektívnosti bezpečnosti:

- V prípade určitého narušenia bezpečnosti sa systémovému operátorovi posielajú správy.
- Rôzne transakcie, súvisiace s bezpečnosťou, možno zaznamenať do zvláštneho auditovacieho žurnálu.

Téma ″Monitorovanie bezpečnosti″ hovorí o používaní týchto nástrojov všeobecne. Podrobnejšie informácie o auditovaní bezpečnosti nájdete v kapitole 9 ″Auditing Security on the System″ v publikácii *Security-Reference* (SC41-5302).

Ak chcete lepšie pochopiť, ako máte prispôsobiť váš systém, mali by ste prispôsobenie pochopiť z pohľadu užívateľa.

Názor užívateľa na prispôsobenie systému: Váš systém môžete prispôsobiť, aby ste vašim užívateľom pomohli vykonávať ich každodennú prácu. Ak chcete váš systém pre vašich užívateľov prispôsobiť čo najlepšie, porozmýšľajte, čo potrebujú k úspešnému vykonávaniu svojej práce. Systém môžete prispôsobiť tak, aby ukazoval ponuky a aplikácie niekoľkými spôsobmi:

Ukázať užívateľom to, čo chcú vidieť

Väčšina z nás si upravuje svoje stoly a kancelárie tak, aby sme ľahko dočiahli na veci, ktoré potrebujeme najviac. O prístupe užívateľa k systému rozmýšľajte tým istým spôsobom. Po prihlásení do systému by mal užívateľ najprv vidieť ponuku alebo obrazovku, ktorú používa najčastejšie. Užívateľské profily môžete ľahko navrhnúť tak, aby k tomu dochádzalo.

Odstránenie nepotrebného

Vo väčšine systémov je veľa rôznych aplikácií. Väčšina užívateľov chce vidieť len veci, ktoré potrebujú k vykonávaniu svojich úloh. Ich obmedzenie na niekoľko funkcií v systéme im tieto úlohy uľahčuje. Pomocou užívateľských profilov, opisov úloh a príslušných ponúk môžete každému užívateľovi poskytnúť konkrétny pohľad na systém.

Odosielanie niečoho na správne miesto

Užívatelia by sa nemali starať o to, ako sa ich správy dostanú na správnu tlačiareň alebo ako majú bežať ich dávkové úlohy. Toto majú na starosti systémové hodnoty, užívateľské profily a opisy úloh.

Poskytovanie pomoci

Bez ohľadu na to, ako dobre sa vám podarí systém prispôsobiť, užívatelia môžu byť ešte stále zvedaví ″Kde je moja správa?″ alebo ″Bola už moja úloha spustená?″ Obrazovky **Operačného asistenta** poskytujú jednoduché rozhranie pre systémové funkcie, ktoré pomáhajú užívateľom odpovedať na tieto otázky. Rozličné verzie systémových obrazoviek, nazývané **úrovne pomoci**, poskytujú pomoc užívateľom s rozličnými úrovňami technických skúseností. Váš systém sa dodáva s obrazovkami Operačného asistenta, ktoré sú automaticky k dispozícii všetkým užívateľom. Návrh vašich aplikácií však môže vyžadovať, aby ste zmenili spôsob, akým sa užívatelia dostanú do ponuky Operačného asistenta.

Sever iSeries poskytuje systémové nástroje, ktoré vám umožňujú prispôsobiť systémovú bezpečnosť na ochranu vašich prostriedkov, a zároveň umožnia užívateľom prístup k týmto prostriedkom.

Systémové nástroje pre bezpečnosť a prispôsobenie

Ak chcete plánovať efektívne, musíte pochopiť, ako sa vaše stanovisko k cieľom vašej bezpečnosti týka nástrojov, poskytovaných systémom. Tieto systémové nástroje môžete použiť na prispôsobenie bezpečnosti vo vašom systéme.

Úroveň bezpečnosti

IBM dodáva všetky nové servery iSeries s úrovňou bezpečnosti 40. Úroveň bezpečnosti 40 poskytuje bezpečnosť hesiel a prostriedkov a integritu systému. Ak chcete zmeniť aktívnu úroveň bezpečnosti vo vašom systéme, môžete zmeniť systémovú hodnotu QSECURITY. Avšak IBM dôrazne odporúča, aby ste ponechali úroveň bezpečnosti nastavenú na 40. Na zmenu úrovne bezpečnosti potrebuje užívateľ triedu užívateľa *SECOFR alebo zvláštne oprávnenia *ALLOBJ a *SECADM.

Systém ponúka štyri úrovne bezpečnosti a znázorňuje to nasledujúca tabuľka:

Tabuľka 1. Úrovne bezpečnosti, dostupné v systéme

Úroveň bezpečnosti	**Opis**
Úroveň bezpečnosti 20	Poskytuje len bezpečnosť hesiel.
Úroveň bezpečnosti 30	Poskytuje bezpečnosť hesiel a prostriedkov.
Úroveň bezpečnosti 40	Poskytuje bezpečnosť hesiel a prostriedkov a bezpečnosť integrity.
Úroveň bezpečnosti 50	Poskytuje bezpečnosť hesiel a prostriedkov a vylepšenú ochranu integrity.

Téma ″Výber vašej úrovne bezpečnosti″ obsahuje podrobné informácie o tom, ako určíte, ktorá úroveň bezpečnosti by najlepšie vyhovovala vaším požiadavkám.

Systémové hodnoty

Tieto systémové hodnoty môžete nastaviť, aby určovali ako budú fungovať niektoré funkcie operačného systému na vašom iSeries. Na systémové hodnoty sa pozerajte ako na firemnú politiku. Systémové hodnoty platia pre každého, kto používa systém, pokiaľ niečo konkrétnejšie, napríklad užívateľský profil, nedostane pred systémovou hodnotou prednosť.

Systémové hodnoty určujú také záležitosti, ako je hlavná tlačiareň, ako systém zobrazuje dátum a ako často musíte zmeniť vaše heslo.

Sieťové atribúty

Sieťové atribúty definujú niektoré charakteristiky spôsobu, akým váš systém komunikuje s inými počítačmi vrátane osobných počítačov. Sieťové atribúty platia pre celý váš systém.

Skupinové profily

Skupinový profil definuje skupinu užívateľov. Na skupinové profily sa pozerajte ako na politiku oddelenia. Skupinové profily môžete používať ako vzor pre vytváranie individuálnych užívateľských profilov. Pomocou skupinových profilov môžete tiež zadefinovať, ako majú členovia skupiny povolené pristupovať k objektom v systéme. Viac informácií o skupinových profiloch nájdete v téme ″Plánovanie skupín užívateľov.″

Užívateľské profily

Užívateľský profil je jedným z najvýznamnejších a najuniverzálnejších objektov v systéme. Obsahuje napríklad heslo užívateľa a ponuku, ktorú užívateľ vidí po prihlásení. Užívateľský profil definuje, čo môže a čo nemôže užívateľ robiť v systéme. Určuje jedinečný pohľad užívateľa na systém. Téma ″Plánovanie bezpečnosti užívateľa″ uvádza tipy na plánovanie užívateľských profilov.

Opisy úloh

Opis úlohy pracuje so systémovými hodnotami a užívateľskými profilmi, aby určil spôsob, akým systém spracováva úlohy užívateľa. Opis úlohy nastavuje úvodný zoznam knižníc užívateľa, určujúci knižnice, ku ktorým užívateľ po prihlásení automaticky dostane prístup.

Zabezpečenie prostriedkov

Správca bezpečnosti chráni prostriedky (objekty) v systéme tým, že určuje, kto má oprávnenie na ich používanie a ako môže užívateľ k týmto prostriedkom pristúpiť. Správca bezpečnosti môže nastaviť oprávnenia na objekt pre jednotlivé objekty alebo skupiny objektov (autorizačné zoznamy). Súbory, programy a knižnice sú najbežnejšími objektmi, ktoré vyžadujú ochranu, ale bezpečnosť systému vám umožňuje nastaviť oprávnenia na objekt pre všetky objekty v systéme.

Zabezpečenie prostriedkov môžete manažovať jednoducho a efektívne, ak vopred naplánujete všeobecný a priamy prístup. Schéma zabezpečenia prostriedkov, vytvorená bez predchádzajúceho plánovania, sa môže stať komplikovanou a neefektívnou. Téma ″Plánovanie zabezpečenia prostriedkov″ opisuje spôsoby plánovania zabezpečenia vašich prostriedkov.

Systém poskytuje niekoľko nástrojov, ktoré vám majú pomôcť pri navrhovaní priamej schémy zabezpečenia prostriedkov:

- **Skupinové profily:** Podobných užívateľov môžete zoskupiť pod jeden užívateľský profil. Potom môže celá skupina užívateľov zdieľať rovnaké oprávnenie na objekty.
- **Autorizačné zoznamy:** Objekty s podobnými požiadavkami na bezpečnosť môžete zoskupiť do jedného zoznamu. Potom môžete udeliť oprávnenie na tento zoznam namiesto oprávnenia na jednotlivé objekty.
- **Vlastníctvo objektu:** Každý objekt v systéme má vlastníka. Skupinové profily alebo jednotliví užívatelia môžu vlastniť objekty. Správne priradenie vlastníctva objektu vám pomôže (1) manažovať aplikácie a (2) preniesť zodpovednosť za bezpečnosť vašich informácií.
- **Primárna skupina:** Môžete špecifikovať oprávnenie primárnej skupiny na objekt. Systém ukladá oprávnenie primárnej skupiny spolu s objektom. Používanie oprávnenia primárnej skupiny môže zjednodušiť manažovanie vášho oprávnenia a zlepšiť výkon kontroly oprávnení.
- **Oprávnenie na knižnicu:** Súbory a programy, ktoré vyžadujú ochranu, môžete umiestniť do knižnice a prístup k tejto knižnici môžete obmedziť. Je to často jednoduchšie ako obmedzenie prístupu ku každému jednotlivému objektu. Na ochranu významných objektov budete pravdepodobne chcieť zabezpečiť objekt aj knižnicu.
- **Oprávnenie na objekt:** V prípadoch, keď prístup ku knižnici nie je obmedzený a dostatočne konkrétny, môžete obmedziť oprávnenie na jednotlivé objekty, napríklad na súbory.
- **Verejné oprávnenie:** V prípade každého objektu môžete zadefinovať, ktorý typ prístupu je k dispozícii každému užívateľovi systému, ktorý nemá žiadne iné oprávnenie na tento objekt. Verejné oprávnenie je efektívnym prostriedkom zabezpečenia objektov, ktoré nie sú dôverné a umožňuje kvalitný výkon systému.
- **Oprávnenie na adresár:** Oprávnenie na adresár môžete používať rovnakým spôsobom ako používate oprávnenie na knižnicu. Objekty môžete zoskupovať do adresára a tento adresár zabezpečiť namiesto zabezpečenia jednotlivých objektov.
- **Držiteľ oprávnenia:** Pri vymazávaní objektu vymazávate aj informácie o oprávnení na tento objekt. Držitelia oprávnení udržujú informácie o oprávnení na programom zadefinované súbory, ktoré vymazáva a znova vytvára aplikácia. Držiteľov oprávnení môžete použiť na asistenciu pri migrácii zo systému System/36.

Nástroje bezpečnosti

Bezpečnostné nástroje môžete použiť, aby vám pomohli manažovať a monitorovať bezpečnostné prostredie na vašom systéme iSeries. Môžete tiež použiť nástroje užívateľského profilu, ktoré vám pomôžu:

- Zistiť, ktoré užívateľské profily majú štandardné heslá.
- Naplánovať nedostupnosť užívateľských profilov v určitom čase počas dňa a lebo týždňa.
- Naplánovať odstránenie užívateľského profilu po odchode zamestnanca.
- Zistiť, ktoré užívateľské profily majú zvláštne oprávnenia.
- Zistiť, kto si osvojuje oprávnenie na objekty v systéme.

Nástroje na zabezpečenie objektov môžete použiť na sledovanie verejných a súkromných oprávnení, ktoré súvisia s dôvernými objektmi. Tieto správy môžete pravidelne tlačiť (napríklad každý mesiac), čo vám pomôže zamerať vaše úsilie o bezpečnosť na aktuálne problémy. Správy môžete spúšťať len na zobrazenie zmien, ktoré prebehli od posledného spustenia správy.

Ďalšie nástroje poskytujú možnosť monitorovať:

- Spúšťacie programy
- Hodnoty, relevantné pre bezpečnosť v položkách komunikácií, opisy podsystémov, výstupné fronty, fronty úloh a opisy úloh.
- Zmenené alebo sfalšované programy

Teraz, keď už chápete dôležitosť bezpečnosti systému, pravdepodobne si budete chcieť pozrieť opis metódy plánovania, ktorú táto téma používa ako príklad.

Metóda plánovania základného zabezpečenia systému

Témy o plánovaní v tejto téme pristupujú k plánovaniu smerom zvonka dovnútra a od všeobecného ku konkrétnemu. Ak chcete napríklad plánovať užívateľské profily, musíte najprv porozmýšľať, čo má užívateľ vidieť (vonkajšia strana) a potom rozhodnúť, ako to urobiť (vnútorná strana). Najprv naplánujte systémové hodnoty a skupinové profily (všeobecné) a potom rozhodnite o výnimkách pre jednotlivých užívateľov (konkrétne). Kroky plánovania, uvedené v téme Plánovanie bezpečnosti užívateľov, sú navrhnuté tak, aby sa vykonávali v poradí. Poskytujú logickú postupnosť pre načrtnutie, ako máte naplánovať používanie vášho systému a pre rozhodovanie, ako ho máte zabezpečiť a prispôsobiť.

Pri plánovaní a navrhovaní bezpečnosti systému idete od základov, od najzákladnejších foriem zabezpečenia až po vybudovanie komplikovanejšieho zabezpečenia. Začnite s fyzickým zabezpečením vášho systému a prejdite na opis vašich aplikácií a systémových hodnôt. Nakoniec sa musíte postarať o bezpečnosť pre užívateľov a objekty vo vašom systéme.

Vo všetkých týchto témach, týkajúcich sa plánovania, sme uviedli príklady tohto prístupu a použili sme pritom vzorovú spoločnosť zo scenára - JKL Toys. Téma ″JKL Toy Company: Predstavenie vzorovej spoločnosti″ opisuje vzorovú spoločnosť, ktorá je použitá vo všetkých témach, týkajúcich sa plánovania.

Stručné opisy jednotlivých krokov a ich vzájomnú súvislosť nájdete v téme ″Kroky v procese plánovania″.

Príklad: Predstavenie spoločnosti JKL Toy Company

Použitie príkladov uľahčuje vysvetľovanie aj pochopenie vecí. Majúc toto na pamäti, táto téma používa ako príklad spoločnosť JKL Toy Company. Spoločnosť JKL Toy Company, malý, ale rýchlo rastúci výrobca hračiek, chce nastaviť bezpečnosť na systéme iSeries. Prezident spoločnosti, John Smith, chce nový systém iSeries na uľahčenie situácie spojenej s prudkým rastom spoločnosti JKL Toy Company.

John pridelil Sharon Jones, obchodnej manažérke, zodpovednosť správcu systému a správcu bezpečnosti. Sharon musí zabezpečiť, aby celá inštalácia, vrátane bezpečnosti, prebehla plynulo. Sharon verí v dôležitosť plánovania. Dnes je táto spoločnosť malá a väčšina jej zamestnancov má prístup k väčšine informácií. Sharon však vie, že v dôsledku rastu spoločnosti sa toto zmení. Obáva sa, či prvý raz urobí veci správne.

Spoločnosť JKL Toy Company plánuje najprv spustiť na svojom systéme nasledujúce aplikácie: Zákaznícke objednávky, Inventúra, Zmluvy a cenotvorba a Pohľadávky. Pri čítaní tém o plánovaní sa dozviete viac o tom, ako spoločnosť JKL Toy Company rieši bezpečnosť.

Téma ″Kroky v procese plánovania″ vysvetľuje jednotlivé kroky, ktoré musíte vykonať, keď plánujete zabezpečenie vášho systému.

Kroky v procese plánovania bezpečnosti

Nasledujúca tabuľka opisuje jednotlivé kroky v procese plánovania a súvislosť každého kroku so zvyškom tohto procesu.

Tabuľka 2. Kroky v procese plánovania bezpečnosti

Krok	Čo urobíte v tomto kroku	Ako tento krok súvisí s každým ďalším krokom
Plánovanie fyzického zabezpečenia	Opíšte, ako plánujete chrániť systémovú jednotku, zariadenia a zálohovacie médiá.	Väčšina týchto informácií závisí od zvyšku tohto procesu. Informácie o plánovaní fyzického zabezpečenia nezadávate do systému; niektoré z týchto informácií však potrebujete na plánovanie systémových hodnôt a zabezpečenia prostriedkov.
Plánovanie vašej aplikácie	Opíšte účel, hlavné ponuky a knižnice všetkých vašich aplikácií.	Poskytuje základ pre zvyšok procesu plánovania a pre vaše ďalšie rozhodovania o bezpečnosti. Tieto informácie nezadávate do systému.
Plánovanie vášho celkového prístupu	Rozhodnite sa, aký bude váš celkový prístup k bezpečnosti. Vyberte systémové hodnoty, ktoré podporujú tento prístup.	Na pomoc k určeniu vášho celkového prístupu použite informácie o plánovaní vašej aplikácie. Systémové hodnoty, ktoré vyberiete, budú mať vplyv na to, ako naplánujete užívateľské a skupinové profily.
Plánovanie skupín užívateľov	Rozhodnite sa, ako rozdelíte vašich užívateľov do skupín. Rozhodnite, aké charakteristiky budú mať jednotlivé skupiny a ako ich treba v systéme zadefinovať.	Pomocou opisu vašej aplikácie určite skupiny v systéme. Vami zadefinované skupiny užívateľov budú mať vplyv na to, ako naplánujete jednotlivých užívateľov vo vašom systéme.
Plánovanie individuálnych užívateľských profilov	Každého užívateľa systému zadeľte do skupiny. Zadefinujte každého užívateľa vrátane charakteristiky, ktorý sa odlišuje od zvyšku skupiny. Takýto užívateľ napríklad potrebuje iný prístup k aplikácii alebo knižnici ako zvyšok skupiny.	Jednotlivých užívateľov vám pomôžu zadefinovať informácie o plánovaní aplikácie a plánovaní skupiny užívateľov.
Plánovanie zabezpečenia prostriedkov	Rozhodnite, ktoré aplikácie majú byť dostupné pre každého vo vašom systéme. Ak potrebujete prístup k určitým aplikáciám obmedziť, rozhodnite, ktorí užívatelia alebo skupiny budú mať povolené ich používať.	Pri plánovaní zabezpečenia prostriedkov vám pomôžu informácie o plánovaní aplikácií a plánovaní skupinového profilu.
Plánovanie inštalácie vašich aplikácií	Rozhodnite, ako sa má vytvoriť vlastníctvo a verejné oprávnenie pre knižnice vašich aplikácií.	Inštaláciu vašich aplikácií naplánujte pomocou informácií o plánovaní zabezpečenia prostriedkov.

Proces plánovania zabezpečenia by ste mali začať naplánovaním bezpečnosti užívateľov.

Plánovanie bezpečnosti užívateľov

Plánovanie bezpečnosti užívateľov zahrňuje plánovanie všetkých oblastí, kde bezpečnosť ovplyvňuje užívateľov vo vašom systéme. Je nevyhnutné, aby ste opísali nasledujúce oblasti:

Fyzické zabezpečenie
Fyzická bezpečnosť zahŕňa ochranu vášho systému iSeries pred náhodným (alebo úmyselným) poškodením a krádežou. Okrem toho zahrňuje všetky vaše pracovné stanice, tlačiarne a úložné médiá. Kapitola ″Plánovanie fyzickej bezpečnosti″ obsahuje viac informácií o plánovaní fyzickej bezpečnosti, rizikách a odporúčania IBM.

Bezpečnosť aplikácií
Bezpečnosť aplikácií sa zaoberá aplikáciami, ktoré uchovávate vo vašom systéme a spôsobom ochrany týchto

aplikácií za súčasného povolenia prístupu užívateľov k nim. Téma ″Plánovanie bezpečnosti pre vaše aplikácie″ podrobne opisuje vaše aplikácie a ich názvové konvencie.

Celková bezpečnostná stratégia
Plánovanie vašej celkovej bezpečnosti zahrňuje vypracovanie bezpečnostného plánu, ktorý berie do úvahy vašu súčasnú situáciu aj plány do budúcnosti pre vašu firmu. Téma ″Plánovanie vašej celkovej bezpečnostnej stratégie″ poskytuje bližšie informácie o stanovení vašich bezpečnostných politík, úrovni bezpečnosti, zvažovaní hesiel a systémových hodnotách.

Bezpečnosť skupiny užívateľov
Skupina užívateľov je skupina, ktorá potrebuje používať rovnaké aplikácie rovnakým spôsobom. Plánovanie bezpečnosti skupiny užívateľov zahrňuje stanovenie pracovných skupín, ktoré plánujú používať systém a požiadavky týchto skupín na aplikácie. Téma ″Plánovanie skupín užívateľov″ poskytuje podrobné informácie o identifikovaní skupín užívateľov, plánovaní skupinových profilov, výbere systémových hodnôt a určení prostredia týchto užívateľov.

Bezpečnosť jednotlivých užívateľov
Po stanovení skupín užívateľov, ktoré potrebujete, môžete naplánovať individuálne užívateľské profily, ktoré potrebujete. Téma ″Plánovanie individuálnych užívateľských profilov″ poskytuje bližšie informácie o pomenovávaní užívateľov v systéme, určovaní zodpovedností jednotlivých užívateľov a výbere systémových hodnôt.

V týchto témach o plánovaní nájdete odkazy na plánovacie formuláre, ktoré môžete použiť na zaznamenávanie vašich rozhodnutí, týkajúcich sa plánovania.

Plánovanie fyzického zabezpečenia

Keď sa pripravujete na inštaláciu vášho servera iSeries, mali by ste si vytvoriť plán fyzickej bezpečnosti, kde zodpoviete na tieto otázky:

- Kde umiestnite vašu systémovú jednotku ?
- Kde umiestnite jednotlivé pracovné stanice ?
- Kde umiestnite tlačiarne ?
- Aké ďalšie vybavenie potrebujete, elektrické vedenie, telefónne linky, nábytok alebo skladové priestory ?
- Aké opatrenia vykonáte na ochranu vášho systému pred nepredvídateľnými udalosťami, akými je požiar alebo výpadky elektriny ?

Fyzické zabezpečenie musí byť súčasťou vášho plánu celkovej bezpečnosti. V závislosti od umiestnenia systému a jeho zariadení budete pravdepodobne musieť prijať zvláštne opatrenia na ich ochranu.

Na zaznamenanie vašich rozhodnutí o fyzickom zabezpečení vášho systému môžete použiť formulár Plánovanie fyzického zabezpečenia. Ak chcete mať istotu, že ste zahrnuli všetky aspekty fyzického zabezpečenia, pozrite si tieto témy:

- Fyzické zabezpečenie systémovej jednotky uvádza podrobnosti o zabezpečení samotného systému.
- Fyzické zabezpečenie systémovej dokumentácie a úložných médií obsahuje informácie o ochrane systémových dokumentov a vašich úložných médií.
- Fyzické zabezpečenie pracovných staníc hovorí o spôsoboch zabezpečenia pracovných staníc.
- Fyzické zabezpečenie tlačiarní a tlačového výstupu poskytuje podrobné informácie o fyzickej ochrane tlačiarní a ich výstupu.
- Plánovanie vašej bezpečnostnej politiky vysvetľuje, ako máte vypracovať inštrukcie pre užívateľov a bezpečnostnú politiku.

Každá systémová jednotka má ovládací panel na obsluhu počítača a na vykonávanie špeciálnych systémových operácií, napríklad zapnutia a vypnutia systému. Na zabránenie neoprávnenému používaniu týchto systémových operácií má každá systémová jednotka buď uzamykateľný vypínač alebo elektronický kľúč. Poskytujú istú ochranu vašej systémovej jednotky, ale uzamykateľný vypínač ani elektronický kľúč nenahrádzajú adekvátne fyzické zabezpečenie.

Fyzické zabezpečenie systémovej jednotky

Systém iSeries nevyžaduje miestnosť pre počítač so zvláštnym nastavením prostredia. Systémovú jednotku často nájdete v strede firmy, kde má k nej prístup mnoho ľudí. Zákazníci majú radi malé rozmery a jednoduchú údržbu servera iSeries; tieto vlastnosti však môžu tiež predstavovať bezpečnostné riziká. Napríklad jedna osoba môže systémovú jednotku ľahko odcudziť alebo z nej vybrať cenné komponenty.

Mali by ste prijať opatrenia na bezpečné umiestnenie vašej systémovej jednotky. Najlepším miestom je samostatná, uzamknutá miestnosť. A celkom nakoniec, systémová jednotka musí byť na mieste, ktoré možno mimo riadneho pracovného času uzamknúť.

Ohrozenia systémovej jednotky

Okrem odcudzenia systémovej jednotky alebo jej komponentov uvádzame niektoré ďalšie riziká dôsledku neprimeraného fyzického zabezpečenia vašej systémovej jednotky:

Neúmyselné prerušenie systémových operácií
Mnoho problémov so zabezpečením spôsobujú autorizovaní užívatelia systému. Predstavte si, že jedna z pracovných staníc vo vašom systéme sa uzamkne. Systémový operátor je na stretnutí mimo firmy. Znechutený užívateľ pracovnej stanice chodí okolo systémovej jednotky a rozmýšľa ″Možno by pomohlo, keby som stlačil toto tlačidlo.″ Toto tlačidlo by mohlo vypnúť alebo znova načítať systém v čase, keď beží veľa úloh. Potrebovali by ste niekoľko hodín na obnovu čiastočne aktualizovaných súborov. Ak chcete tejto situácii predísť, môžete použiť uzamykateľný vypínač systémovej jednotky.

Používanie funkcie DST (dedicated service tools) na obídenie bezpečnosti
Bezpečnosť neriadi servisné funkcie, vykonávané systémom, pretože softvér vášho systému pravdepodobne nepracuje správne, keď potrebujete vykonávať tieto funkcie. Skúsená osoba, ktorá pozná alebo uhádne ID užívateľa servisných nástrojov, môže váš systém značne poškodiť. O servisných nástrojoch sa dozviete viac v téme Servisné nástroje v Informačnom centre.

Odporúčania

- Ideálnym miestom pre systémovú jednotku je uzamknutá miestnosť. Ak ju neviete zabezpečiť, umiestnite vašu jednotku mimo dosahu cudzích osôb. Okrem toho vyberte miesto, kde ju budú zodpovední zamestnanci môcť monitorovať. Nasledujúce funkcie fyzického zabezpečenia vám môžu pomôcť chrániť váš systém pred náhodnou alebo úmyselnou manipuláciou:
- Použite elektronický kľúč alebo uzamykateľný vypínač:
  - Ak chcete váš systém spustiť bez použitia kľúča, operačný režim nastavte na Normal.
  - Ak máte v úmysle spustiť a zastaviť váš systém pomocou funkcie Automatic Power On/Off, operačný režim nastavte na Auto.
  - Kľúč vyberte a odložte ho na bezpečné miesto.
- Okamžite po nainštalovaní vášho systému a jeho použití servisnými technikmi zmeňte ID a heslo užívateľa servisných nástrojov (DST). Podrobnejšie vysvetlenie nájdete v téme Servisné nástroje v Informačnom centre.

Než naplánujete fyzické zabezpečenie systémovej dokumentácie a úložných médií, pravdepodobne si budete chcieť pozrieť príklad plánu zabezpečenia systémovej jednotky v spoločnosti JKL Toy Company.

Príklad: Formulár plánovania fyzického zabezpečenia spoločnosti JKL Toy—systémová jednotka: Nižšie je uvedený príklad časti formulára plánovania fyzického zabezpečenia pre systémovú jednotku, ktorý použila Sharon Jones pre svoj systém:

Tabuľka 3. Formulár plánovania fyzického zabezpečenia spoločnosti JKL Toy: príklad systémovej jednotky

Formulár plánovania fyzického zabezpečenia	
Pripravil: Sharon Jones	Dátum: 9/2/99
Systémová jednotka:	

Tabuľka 3. Formulár plánovania fyzického zabezpečenia spoločnosti JKL Toy: príklad systémovej jednotky (pokračovanie)

Opíšte vaše bezpečnostné opatrenia na ochranu systémovej jednotky (napríklad uzamknutá miestnosť):	Systémová jednotka je v účtovníckom priestore. Cez deň sú účtovníci vždy v tomto priestore a môžu dať pozor na systémovú jednotku. Účtovníci tiež zodpovedajú za malú hotovosť a dôležité záznamy. Mimo riadneho pracovného času je tento priestor uzamknutý.
Aká poloha uzamykateľného vypínača sa normálne používa?	Normálna
Kde sa necháva kľúč?	Malý trezor v Sharoninej kancelárii
Ďalšie poznámky týkajúce sa systémovej jednotky:	K systémovej jednotke bude ľahký prístup. Treba povedať užívateľom v účtovníckom priestore, že majú zaistiť, aby žiadni ľudia do jednotky nedovolene nezasahovali.

Po naplánovaní fyzického zabezpečenia systémovej jednotky môžete plánovať fyzické zabezpečenie pre systémovú dokumentáciu a úložné médiá.

Fyzické zabezpečenie systémovej dokumentácie a úložných médií

Ďalší aspekt vášho plánu fyzického zabezpečenia sa zaoberá uložením dôležitej systémovej dokumentácie a úložných médií. Systémová dokumentácia obsahuje informácie, ktoré spoločnosť IBM posiela so systémom, informácie o hesle, vaše plánovacie formuláre a všetky správy, ktoré systém generuje.

V závislosti od vášho systému môžu zálohovacie médiá zahrňovať pásky, disky CD-ROM, diskety alebo DVD. Systémovú dokumentáciu aj zálohovacie médiá by ste mali uložiť jednak v lokalite vašej firmy, jednak v ďalšej vzdialenej lokalite. V prípade katastrofy budete tieto informácie potrebovať na obnovu vášho systému. Nasledujúce informácie navrhujú spôsoby uloženia vašej systémovej dokumentácie a úložných médií. Po vybratí svojej metódy zaznamenajte vaše voľby do časti Zálohovacie médiá a dokumentácia vo formulári Plánovanie fyzického zabezpečenia.

Bezpečné uloženie systémovej dokumentácie

Pre prevádzku vášho systému sú veľmi dôležité heslá servisných nástrojov a správcu bezpečnosti. Tieto heslá by ste si mali zapísať a uložiť ich na bezpečnom a tajnom mieste. Okrem toho kópiu týchto hesiel uschovajte na mieste mimo firmy, pomôže vám pri obnove po katastrofe.

Zvážte uloženie aj ďalšej dôležitej systémovej dokumentácie, napríklad konfiguračných nastavení a vašich hlavných knižníc aplikácií, na mieste mimo vašej firmy, pomôže vám to pri obnove po katastrofe.

Bezpečné uloženie vašich úložných médií

Pri inštalácii vášho systému si naplánujte pravidelné ukladanie všetkých informácií v systéme na pásku alebo iné úložné médium. V prípade potreby vám tieto zálohy umožnia obnoviť váš systém. Tieto zálohy by ste mali uschovať aj na bezpečnom mieste mimo firmy.

Riziká

- Poškodenie zálohovacieho média: Ak vaše médiá so zálohami systému poškodili vandali alebo katastrofa, okrem tlačených správ nebudete môcť obnoviť informácie, ktoré boli v systéme.
- Odcudzenie zálohovacích médií alebo hesiel: Na vašich zálohovacích médiách máte možno uložené tajné firemné informácie. Skúsená osoba môže tieto informácie obnoviť na iný počítač a vytlačiť alebo ich spracovať.

Odporúčania

- Všetky heslá a zálohovacie médiá uložte do zamknutej, ohňovzdornej skrine.
- Kópie vašich zálohovacích médií odneste pravidelne, napríklad najmenej raz za týždeň, na bezpečné miesto mimo firmy.

Než naplánujete fyzické zabezpečenie vašich pracovných staníc, pravdepodobne si budete chcieť pozrieť príklad plánu ukladania systémovej dokumentácie spoločnosti JKL Toy Company.

Príklad: Formulár plánovania fyzického zabezpečenia spoločnosti JKL Toy—zálohovacie médiá a dokumentácia: Sharon Jones zo spoločnosti JKL Toy vyplnila časť formulára plánovania fyzického zabezpečenia pre zálohovacie médiá a dokumentáciu tak, ako to ukazuje nasledujúca tabuľka:

Tabuľka 4. Formulár plánovania fyzického zabezpečenia spoločnosti JKL Toy: príklad zálohovacích médií a dokumentácie

Formulár plánovania fyzického zabezpečenia	
Pripravil: Sharon Jones	Dátum: 9/2/99
Zálohovacie médiá a dokumentácia:	
Kde sú na vašom pracovisku uložené zálohovacie pásky?	Vo veľkom ohňovzdornom trezore.
Kde sú uložené zálohovacie pásky mimo vášho pracoviska?	V ohňovzdornom trezore v kancelárii hlavného účtovníka.
Kde sú uchovávané heslá správcu bezpečnosti, služieb a DST?	S bezpečnou kombináciou v kancelárii Johna Smitha.
Kde sa uchováva dôležitá systémová dokumentácia, ako napríklad sériové číslo a konfigurácia?	Vo veľkom trezore mimo pracoviska a v kancelárii nášho hlavného účtovníka.

Po naplánovaní zabezpečenia vášho úložného priestoru a dokumentácie môžete naplánovať fyzické zabezpečenie pre vaše pracovné stanice.

Plánovanie fyzického zabezpečenia pracovných staníc

Vo väčšine prípadov chcete, aby sa všetci užívatelia mohli prihlásiť na ktorúkoľvek dostupnú pracovnú stanicu a vykonávať všetky autorizované funkcie. Ak však máte pracovné stanice, ktoré sú buď príliš verejné alebo príliš súkromné, pravdepodobne budete chcieť prijať zvláštne preventívne opatrenia. Zvláštnu pozornosť vyžadujú napríklad pracovné stanice, ktoré môžu uchovať informácie a osobné počítače. Toto použite pri vyplňovaní Časti 2 (Fyzické zabezpečenie pracovných staníc a tlačiarní) formulára Plánovanie fyzického zabezpečenie.

Riziká, spojené s pracovnými stanicami

Použitie pracovnej stanice, umiestnenej na verejnom mieste, na neautorizované účely
Ak sa môžu užívatelia, ktorí nepatria do vašej spoločnosti, ľahko dostať na takéto miesta, je možné, že uvidia dôverné informácie. Ak užívateľ systému opustí pracovnú stanicu a ostane prihlásený, môže prísť niekto zvonka, kto nepatrí do vašej spoločnosti a dostať sa k dôverným informáciám.

Použitie pracovnej stanice, umiestnenej na súkromnom mieste, na neautorizované účely
Pracovná stanica, umiestnená na celkom súkromnom mieste, poskytuje narušiteľovi príležitosť stráviť dlhé hodiny nad pokusmi ako obísť vaše zabezpečenie bez toho, aby ho niekto uvidel.

Použitie funkcie prehrávania alebo programu prihlasovania na pracovnej stanici na obídenie bezpečnostných opatrení
Mnohé pracovné stanice majú funkciu nahrávania a prehrávania, ktorá umožňuje užívateľom ukladať často používané písané informácie a opakovať ich stlačením jedného klávesu. Keď používate osobný počítač ako pracovnú stanicu na systéme iSeries, môžete si napísať program na automatizáciu procesu prihlasovania. Pretože užívatelia často používajú proces prihlasovania, môžu sa rozhodnúť, že svoje užívateľské ID a heslá si uložia namiesto toho, aby ich písali pri každom prihlásení.

Odporúčania

Pri nastavovaní fyzického zabezpečenia pre pracovné stanice vezmite do úvahy tieto odporúčania:

- Ak je to možné, neumiestňujte pracovné stanice na príliš verejné alebo príliš súkromné miesta.
- Užívateľom systému zdôraznite dôležitosť odhlásenia pred opustením pracovnej stanice. Procedúry odhlasovania by ste mali zahrnúť do vašej bezpečnostnej politiky.

- Zdôraznite, že zaznamenanie hesla do pracovnej stanice alebo do programu PC narušuje bezpečnosť systému. Informácie o zaznamenávaní hesiel by ste mali zahrnúť do vašej bezpečnostnej politiky.
- Pomocou systémových hodnôt neaktívneho časovača (QINACTITV a QINACTMSGQ) prijmite opatrenia, ktoré zabránia užívateľom odchádzať od pracovných staníc na verejných miestach bez odhlásenia zo systému.
- Obmedzte funkcie, ktoré môžu užívatelia vykonávať na verejných pracovných staniciach tým, že oprávnite len užívateľov s obmedzeným oprávnením na tieto pracovné stanice.
- Užívateľom s bezpečnostným alebo servisným oprávnením zabráňte prihlasovať sa na súkromné pracovné stanice. Pomocou systémovej hodnoty QLMTSECOFR kontrolujte, kde sa užívateľ s týmito oprávneniami prihlasuje.
- Zabráňte užívateľom prihlasovať sa na viac ako jednu pracovnú stanicu v rovnakom čase. Na kontrolu, kde sa užívateľ prihlasuje, môžete použiť systémovú hodnotu, ktorá obmedzuje relácie zariadenia (QLMTDEVSSN).

Ak chcete tieto odporúčania uviesť do platnosti, podrobné informácie nájdete v témach Výber systémových hodnôt, ovplyvňujúcich prihlásenie″ a ″Plánovanie zabezpečenia prostriedkov pre pracovné stanice″.

Pre formulár Plánovanie fyzického zabezpečenia je potrebné identifikovať, ktoré pracovné stanice môžu znamenať riziko dôsledku ich fyzického umiestnenia. Pravdepodobne si budete chcieť pozrieť príklad, ako Sharon Jones plánovala fyzické zabezpečenie pracovných staníc v spoločnosti JKL Toy Company.

Po naplánovaní zabezpečenia pracovných staníc môžete naplánovať fyzické zabezpečenie tlačiarní a tlačového výstupu.

Fyzické zabezpečenie tlačiarní a tlačového výstupu

Keď sa raz informácie začnú tlačiť, systémová bezpečnosť nemôže určovať, kto ich uvidí. Ak chcete riziko, že niekto uvidí citlivé firemné informácie, znížiť na minimum, mali by ste tlačiarne a tlačový výstup zabezpečiť. Tak isto by ste mali vytvoriť politiku, ktorá sa zaoberá tlačou dôverných firemných informácií.

Riziká, spojené s tlačiarňami a tlačovým výstupom

Nasledujúce riziká sa môžu týkať situácie vo vašej firme. Sú to najbežnejšie bezpečnostné riziká, súvisiace s tlačiarňami a tlačovým výstupom. Musíte však preskúmať aj ďalšie riziká, ktoré by sa mohli týkať konkrétnej situácie vo vašej firme.

- Tlačiareň, umiestnená na verejne prístupnom mieste, môže neautorizovaným osobám poskytnúť prístup k dôverným informáciám.
- Informácie môže prezradiť aj tlačový výstup, ponechaný v priehradke.
- Vo vašom systéme je pravdepodobne len jedna alebo dve tlačiarne. Môžete potrebovať tlačiť cenné alebo dôverné informácie, napríklad mzdy, ktoré by zamestnanci vašej spoločnosti nemali vidieť.

Odporúčania

Nasledujúce odporúčania vám môžu pomôcť znížiť bezpečnostné riziká, spojené s tlačiarňami a ich výstupom.

- Užívateľom systému zdôraznite dôležitosť ochrany dôverného tlačového výstupu. Rozhodnutia o fyzickom zabezpečení, týkajúce sa tlačiarní, zahrňte do vašej bezpečnostnej politiky.
- Tlačiarne neumiestňujte na verejne prístupných miestach.
- Tlač vysoko dôverného výstupu si naplánujte a počas jeho tlače postavte k tlačiarni autorizovanú osobu.

Téma ″Plánovanie zabezpečenia tlačiarní a tlačového výstupu″ rozoberá návrhy narábania s dôverným tlačovým výstupom.

Než začnete plánovať vašu bezpečnostnú politiku, pravdepodobne si budete chcieť pozrieť príklad plánu zabezpečenia tlačiarní v spoločnosti JKL Toy Company.

Príklad: Formulár plánovania fyzického zabezpečenia spoločnosti JKL Toy—pracovná stanica a tlačiareň:
Nasleduje príklad 2. časti plánu fyzického zabezpečenia, ktorý použila Sharon Jones pre spoločnosť JKL Toy:

Tabuľka 5. Formulár plánovania fyzického zabezpečenia spoločnosti JKL Toy: príklad pracovnej stanice a tlačiarne

Formulár plánovania fyzického zabezpečenia			2. časť z 2
Fyzické zabezpečenie pracovných staníc a tlačiarní			
Názov pracovnej stanice alebo tlačiarne	Jej umiestnenie alebo opis	Bezpečnostná trhlina	Ochranné opatrenia, ktoré treba urobiť
DSP06	Nakladacie rampy	Príliš verejné	Automatické odhlásenie. Obmedziť funkcie, ktoré môžu byť vykonávané na pracovnej stanici.
DSP09	Pracovisko služieb zákazníkom	Príliš verejné	Automatické odhlásenie. Obmedziť funkcie, ktoré môžu byť vykonávané na pracovnej stanici.
RMT12	Vzdialená predajná kancelária	Príliš súkromné	Nedovoliť správcovi bezpečnosti sa tam prihlásiť.
PRT02	Učtáreň, blízko systémovej jednotky	Je možné vidieť citlivé informácie, napríklad cenníky	Určiť niekoho, aby sledoval tlačový výstup

Po vyplnení Formulára plánovania fyzického zabezpečenia pokračujte témou ″Plánovanie bezpečnostnej politiky.

Plánovanie vašej bezpečnostnej politiky

Možno zistíte, že na zdôraznenie vašich bezpečnostných politík, týkajúcich sa fyzického a systémového zabezpečenia, je užitočné rozoslať bezpečnostné pokyny všetkým vašim zamestnancom. Tie isté pokyny môžete dať novým užívateľom, ktorí sa pridajú do vášho systému neskôr.

Do týchto pokynov by ste mali zahrnúť niektoré všeobecné inštrukcie k ochrane bezpečnosti systému, napríklad odhlasovanie z pracovných staníc a nezdieľanie hesiel. Tieto pokyny by mali obsahovať aj informácie o vašich konkrétnych rozhodnutiach, týkajúcich sa bezpečnosti.

Pri čítaní týchto informácií o plánovaní si robte poznámky k tomu, čo by mali obsahovať vaše vlastné bezpečnostné pokyny. Pravdepodobne si budete chcieť robiť poznámky aj k vašej bezpečnostnej politike.

Sharon Jones zo spoločnosti JKL Toy Company si napríklad tieto poznámky k jej bezpečnostným pokynom robila počas plánovania fyzického zabezpečenia systému:

```
Nezabudnite zdôrazniť odhlásenie
pre nakladaciu rampu, zákaznícke služby
a vzdialenú obchodnú kanceláriu. Obchodníci budú sledovať systémovú jednotku.
```

Po vyplnení formulára Plánovanie fyzického zabezpečenia môžete začať plánovať bezpečnosť pre vaše aplikácie.

Plánovanie bezpečnosti vašich aplikácií

Ak chcete naplánovať správnu bezpečnosť pre vaše aplikácie, musíte vedieť:

- Ktoré informácie plánujete ukladať do systému ?
- Kto potrebuje prístup k týmto informáciám ?
- Aký druh prístupu užívatelia potrebujú ? Potrebujú informácie meniť alebo si ich len prezerať ?

Keď prechádzate týmito témami o plánovaní aplikácií, odpovedzte na prvú otázku - ktoré informácie plánujete ukladať do vášho systému. V ďalších témach rozhodnite, kto potrebuje tieto informácie a aký druh prístupu užívatelia potrebujú. Informácie o plánovaní aplikácií nezadávate do systému; budete ich však potrebovať pri nastavovaní bezpečnosti užívateľov a prostriedkov.

Čo je aplikácia ?

V prvom kroku plánovania bezpečnosti aplikácií musíte opísať aplikácie, ktoré plánujete spustiť vo vašom systéme. Aplikácia je skupina funkcií, ktoré logicky patria k sebe. Napríklad v spoločnosti JKL Toy Company je evidencia objednávok, expedovanie zákaziek a tlač faktúr súčasťou jednej aplikácie, nazývanej Spracovanie objednávok.

Na vašom systéme iSeries môžu zvyčajne bežať dva odlišné typy aplikácií:

- **Podnikové aplikácie**: Aplikácie, ktoré kupujete alebo vyvíjate na vykonávanie konkrétnych podnikových funkcií ako sú napríklad spracovanie objednávok alebo riadenie inventúr.
- **Špeciálne aplikácie**: Vami poskytnuté aplikácie, ktoré sa používajú v celej vašej spoločnosti na vykonávanie rozličných činností, ktoré sa výslovne netýkajú pracovného procesu.

Aké formuláre potrebujte ?

Pri plánovaní bezpečnosti vašich aplikácií vám pomôžu nasledujúce formuláre:

- Formulár Opis aplikácie
- Formulár Opis knižnice
- Formulár Názvové konvencie

Ak chcete tieto formuláre vytlačiť, kliknite vo vašom prehliadači na odkaz, vyberte pravý rámec a kliknite na ikonu **Print**.

Prečítanie nasledujúcich informácií vám pomôže vyplniť tieto plánovacie formuláre.

- Opísanie vašich aplikácií
- Opísanie názvových konvencií
- Opísanie informácií o knižnici
- Nakreslenie diagramu aplikácií

Opísanie vašich aplikácií

V tomto bode potrebujete zozbierať niektoré všeobecné informácie o každej vašej podnikovej aplikácii. Informácie o vašich aplikáciách pridajte do príslušných polí vo formulári Opis aplikácie tak, ako je uvedené ďalej. Tieto informácie môžete neskôr použiť ako pomôcku pri plánovaní skupín užívateľov a bezpečnosti aplikácií:

Názov aplikácie a skratka
: Dajte aplikácii krátky názov a skratku, ktorú môžete použiť na rýchle zapísanie do formulárov a na pomenovanie objektov, ktoré táto aplikácia používa.

Opisné informácie
: Stručne opíšte, čo táto aplikácia vykonáva.

Primárna ponuka a knižnica
: Identifikujte, ktorá ponuka je primárnou ponukou na prístup k aplikácii. Označte knižnicu, v ktorej je táto ponuka. Primárna ponuka zvyčajne vedie k ďalším ponukám s konkrétnymi funkciami aplikácií. Užívatelia radi vidia primárnu ponuku pre ich hlavnú aplikáciu okamžite po prihlásení do systému.

Úvodný program a knižnica
: Aplikácie občas spúšťajú úvodný program, ktorý pre užívateľa nastavuje prostredie alebo vykonáva kontrolu bezpečnosti. Ak má aplikácia úvodný program alebo program nastavenia, uveďte ho do formulára.

Knižnice aplikácií
: Každá aplikácia má zvyčajne pre svoje súbory hlavnú knižnicu. Zahrňte všetky knižnice, ktoré táto aplikácia používa, vrátane knižníc programov a knižníc, ktoré sú vlastníctvom iných aplikácií. Napríklad, aplikácia zákazníckych objednávok spoločnosti JKL Toy Company používa knižnicu inventára na získanie stavov a opisov položiek.

  Vzťah medzi knižnicami a aplikáciami môžete použiť na zistenie, kto potrebuje prístup do každej knižnice.

Hľadanie informácií o vašich aplikáciách

Ak ešte nepoznáte informácie, ktoré potrebujete o vašich aplikáciách, pravdepodobne sa budete musieť spojiť s vaším programátorom alebo s poskytovateľom vašich aplikácií.

Uvádzame metódy, ktorými môžete sami zozbierať tieto informácie, ak nemáte prístup k týmto informáciám o aplikácii, ktorá beží na vašom systéme.

- Užívatelia tejto aplikácie vám zrejme povedia názov primárnej ponuky a knižnice, alebo sa môžete pozerať, keď sa budú prihlasovať do systému.
- Ak užívatelia vidia aplikáciu okamžite po prihlásení, pozrite si pole **Úvodný program** v ich užívateľských profiloch. Toto pole obsahuje úvodný program k tejto aplikácii. Na zobrazenie úvodného programu môžete použiť príkaz DSPUSRPRF.
- Môžete si vypísať názvy a opisy všetkých knižníc vo vašom systéme. Použite DSPOBJD *ALL *LIB. Zobrazia sa všetky knižnice vo vašom systéme.
- Keď užívateľom beží aplikácia, môžete pozorovať aktívne úlohy. Na získanie podrobných informácií o interaktívnych úlohách použite príkaz WRKACTJOB (Work with Active Jobs) so strednou úrovňou pomoci. Zobrazte úlohy a pozrite si zoznamy knižníc aj zámky ich objektov, aby ste zistili, ktoré knižnice sa používajú.
- Dávkové úlohy v aplikácii môžete zobraziť pomocou príkazu WRKUSRJOB (Work with User Jobs).

Ak chcete mať istotu, že máte všetky informácie, potrebné k naplánovaniu bezpečnosti vašich aplikácií, musíte najprv vykonať nasledujúce úlohy:

- Pre všetky vaše podnikové aplikácie vyplňte formulár Opis aplikácie. Vyplňte celý formulár okrem časti požiadaviek na bezpečnosť. Túto časť použijete na plánovanie zabezpečenia prostriedkov pre aplikáciu tak, ako je opísané v téme ″Plánovanie zabezpečenia prostriedkov″.
- Ak je to vhodné, vypracujte pre každú špeciálnu aplikáciu formulár Opis aplikácie. Použitie tohto formulára vám pomôže určiť, ako poskytnúť prístup k aplikácii.

Poznámka: Príprava formulárov s opisom aplikácií pre špeciálne aplikácie od IBM, napríklad IBM Query for iSeries nie je povinná. Prístup ku knižniciam, používaný týmito aplikáciami, nevyžaduje žiadne zvláštne plánovanie. Pravdepodobne však zistíte, že zbieranie informácií a vypracovanie formulárov je užitočné.

Než prejdete k opísaniu názvových konvencií, pravdepodobne si budete chcieť pozrieť príklad formulára Opis aplikácie, ktorý používa spoločnosť JKL Toy Company.

Príklad: Formulár opisu aplikácií spoločnosti JKL Toy: Sharon Jones vytvorila zoznam všetkých aplikácií spoločnosti s ich skratkami na formulári opisu aplikácií. Stručne tiež opísala, ako užívatelia s tými aplikáciami pracujú.

Zákaznícke objednávky (CO)
Vkladajú, sledujú a posielajú objednávky. Tlačia faktúry.

Riadenie zásob (IC)
Riadia úrovne zásob pre dokončené produkty aj pre materiály. Spracúvajú všetky zmeny v zásobách.

Kontrakt a tvorba cien (CP)
Riadia špeciálnu tvorbu cien a kontrakty so zákazníkmi.

Pohľadávky (AC)
Sledujú aktuálne zostatky. Tlačia mesačné výkazy.

Nasledujúca tabuľka obsahuje opis aplikácie Zákaznícka objednávka vytvorený Sharon Jones. Tá pripravovala svoje formuláre systematicky, začínajúc jednou aplikáciou, a potom opísala ostatné.

Tabuľka 6. Formulár opisu aplikácií spoločnosti JKL Toy: príklad

Formulár opisu aplikácií	
Pripravil: Sharon Jones	Dátum: 9/3/99
Názov aplikácie: Zákaznícke objednávky	Skratka: CO

Tabuľka 6. Formulár opisu aplikácií spoločnosti JKL Toy: príklad (pokračovanie)

Stručný opis aplikácie:	Vkladá zákaznícke objednávky, sleduje ich pred odoslaním, odosiela objednávku a tlačí faktúry a prepravné doklady.
Názov primárnej ponuky: COMAIN	Knižnica: COPGMLIB
Názov úvodného programu: NA	Knižnica: NA
Vypíšte knižnice používané aplikáciou pre súbory aj pre programy: • CUSTLIB • ITEMLIB • CONTRACTS • COPGMLIB	
Definujte ciele zabezpečenia pre aplikáciu, napríklad či sú určité informácie dôverné:	

Okrem aplikácie Zákaznícka objednávka Sharon Jones pripravila aj formuláre opisu aplikácií pre tieto aplikácie v systéme spoločnosti JKL Toy:

- Riadenie zásob
- Kontrakty a tvorba cien
- Pohľadávky.

Ďalej môžete popísať názvové konvencie pre objekty vo vašom systéme.

Opísanie názvových konvencií

Ak viete, ako systém pomenováva objekty, môžete plánovať a monitorovať bezpečnosť, riešiť problémy a plánovať zálohovanie a obnovu. Väčšina aplikácií má pravidlá pre priraďovanie názvov k objektom, napríklad ku knižniciam, súborom a programom. Ak vaše aplikácie pochádzajú z rôznych zdrojov, každá z nich má pravdepodobne svoj vlastný jedinečný systém pomenovávania.

Do formulára Názvové konvencie určite zaznamenajte všetky názvové konvencie aplikácií a objektov. Vo formulári Názvové konvencie uveďte pravidlá, ktoré vaše aplikácie používajú pre pomenovávanie knižníc a súborov. Pravdepodobne budete chcieť použiť prázdne riadky pre iné názvové konvencie, napríklad pre ponuky a programy. Ak vaše aplikácie pochádzajú z rôznych zdrojov, každá z nich má pravdepodobne jedinečné názvové konvencie. Opíšte názvové konvencie pre každú aplikáciu. Pravdepodobne budete musieť vypracovať viac ako jeden formulár Názvové konvencie.

Než prejdete na opísanie informácií o knižnici, pravdepodobne si budete chcieť pozrieť príklad, ako Sharon použila názvové konvencie pre objekty v systéme spoločnosti JKL Toy Company.

Príklad: Formulár názvových konvencií spoločnosti JKL Toy: Nasledujúca tabuľka ukazuje názvové konvencie len pre knižnice a súbory. Bude tiež potrebné, aby ste popísali názvové konvencie pre ostatné typy objektov vo vašom systéme. Formulár názvových konvencií obsahuje viaceré bežné objekty; môžete mať však aj iné, ktoré bude potrebné pripraviť.

Tabuľka 7. Formulár názvových konvencií spoločnosti JKL Toy: príklad

Formulár názvových konvencií	
Pripravil: Sharon Jones	Dátum: 9/3/99
Typ objektu	**Pomenúvacie konvencie**
Knižnice	Knižnice obsahujúce súbory majú zmysluplné názvy, napríklad CONTRACTS alebo ITEMLIB. Knižnice programov používajú skratku aplikácie, za ktorou nasleduje PGMLIB, napríklad ICPGMLIB.

Tabuľka 7. Formulár názvových konvencií spoločnosti JKL Toy: príklad (pokračovanie)

Súbory	Hlavné súbory majú zmysluplné názvy, napríklad CUSTMAST pre zákaznícky hlavný súbor, alebo ITEMMAST pre hlavný súbor položiek. Ďalšie aplikačné súbory (používané z dôvodov, ktorým rozumejú len programátori), majú názvy pozostávajúce zo skratky aplikácie, za ktorou nasleduje FILE a číslo, napríklad ICFILE14.

Po vyplnení formulára názvových konvencií môžete začať opisovať knižničné informácie.

Opísanie informácií o knižnici

Po opísaní vašich názvových konvencií by ste mali opísať knižnice vo vašom systéme. Knižnice identifikujú a organizujú objekty vo vašom systéme. Umiestnenie podobných súborov spolu do jednej knižnice umožňuje užívateľom ľahko pristupovať k veľmi dôležitým aplikáciám a súborom. Môžete tiež prispôsobiť oprávnenia vašich užívateľov, aby mali prístup do niektorých knižníc, ale do žiadnych iných. Opíšte všetky knižnice, ktoré máte v systéme pre jednotlivé aplikácie. Pravdepodobne budete musieť vypracovať viac ako jeden formulár Opis knižnice.

Poznámka: Vyplňte iba opisné informácie o knižnici. Pri plánovaní zabezpečenia prostriedkov pre túto knižnicu vyplníte zvyšnú časť formulára Opis knižnice. Neskôr budete musieť pridať informácie o oprávneniach na knižnice. Podrobné informácie o vyplňovaní zvyšnej časti formulára Opis knižnice nájdete v téme ″Plánovanie bezpečnosti pre knižnice aplikácií″.

Skôr, než budete pokračovať, musíte vykonať nasledovné:

- Vo formulári Názvové konvencie vyplňte časti, týkajúce sa knižníc a súborov.
- Vo formulári Opis knižnice vyplňte opisné informácie pre každú knižnicu aplikácií.

Skôr, než nakreslíte diagram aplikácií, pravdepodobne si budete chcieť pozrieť príklad, ako Sharon Jones zo spoločnosti JKL Toy Company opísala knižnice.

Príklad: Formulár opisu knižnice spoločnosti JKL Toy: Nasledujúce dve tabuľky opisujú dve knižnice, ktoré používa aplikácia Zákaznícke objednávky v spoločnosti JKL Toy. Prvá tabuľka opisuje knižnicu obsahujúcu súbory a druhá opisuje knižnicu obsahujúcu programy.

Tabuľka 8. Formulár opisu knižnice spoločnosti JKL Toy: Príklad knižnice obsahujúcej súbory

Formulár opisu knižnice	
Pripravil: Sharon Jones	Dátum: 9/3/99
Názov knižnice: CUSTLIB	Opisný názov (text): Knižnica zákazníckych záznamov
Stručne opíšte funkciu tejto knižnice:	Obsahuje všetky zákaznícke súbory, vrátane objednávok a pohľadávok.

Tabuľka 9. Formulár opisu knižnice spoločnosti JKL Toy: Príklad knižnice obsahujúcej programy

Formulár opisu knižnice	
Pripravil: Sharon Jones	Dátum: 9/3/99
Názov knižnice: COPGMLIB	Opisný názov (text): Knižnica programov zákazníckych objednávok
Stručne opíšte funkciu tejto knižnice:	Obsahuje všetky programy pre aplikáciu zákazníckych objednávok.

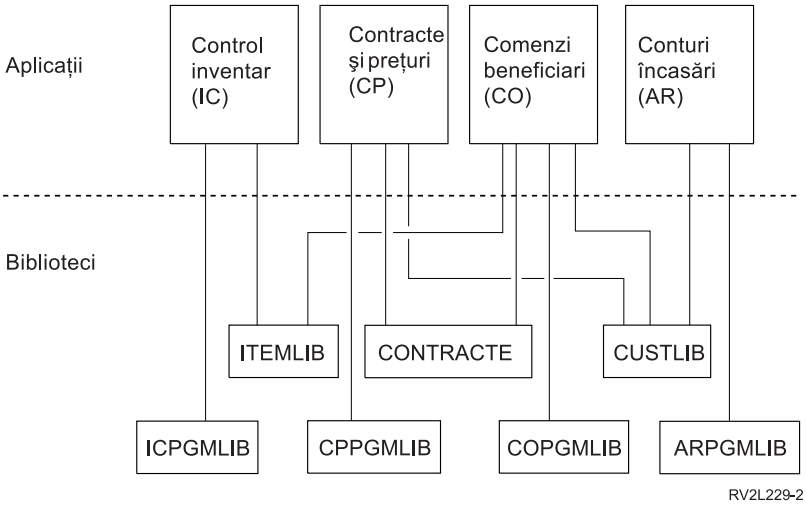
Po popísaní vašich knižníc by ste mali nakresliť aplikačný diagram vášho systému.

Nakreslenie diagramu aplikácií

Pri vypracovávaní formulárov Opis aplikácie a Opis knižnice pravdepodobne zistíte, že je užitočné nakresliť si diagram, ktorý znázorňuje vzťah medzi aplikáciami a knižnicami. Graf vám pomôže pri plánovaní skupín užívateľov aj zabezpečenia prostriedkov.

Nasledujúci obrázok znázorňuje diagram aplikácií a knižníc spoločnosti JKL Toy Company, ktorý nakreslila Sharon Jones:

Graf aplikácií a knižníc spoločnosti JKL Toy Company



Pri mnohých rozhodnutiach o bezpečnosti, ktoré potrebujete urobiť, vám pomôže zozbieranie informácií o vašich aplikáciách a knižniciach. Berte to ako možnosť dozvedieť sa viac o vašom systéme a aplikáciách.

Ak chcete mať istotu, že ste zozbierali potrebné informácie o aplikáciách, urobte nasledovné:
- Vyplňte formulár Opis aplikácie pre každú podnikovú aplikáciu vo vašom systéme.
- Voliteľne vypracujte formulár Opis aplikácie pre každú špeciálnu aplikáciu vo vašom systéme.
- Vo formulári Názvové konvencie vyplňte časti, týkajúce sa knižníc a súborov.
- Pre každú knižnicu aplikácií vypracujte formulár Opis knižnice.
- Nakreslite si diagram vzťahu medzi vašimi aplikáciami a knižnicami.

Po vyplnení týchto formulárov môžete začať plánovať vašu celkovú bezpečnostnú stratégiu.

Plánovanie vašej celkovej bezpečnostnej stratégie

Po naplánovaní bezpečnosti pre vaše aplikácie môžete začať s celkovou bezpečnostnou stratégiou. Najprv musíte urobiť rozhodnutia o celkovom prístupe k bezpečnosti vo vašom systéme. Keď robíte tieto rozhodnutia, zosúlaďte súčasné požiadavky vašej spoločnosti s požiadavkami pre budúcnosť.

Tieto informácie vám v procese plánovania pomôžu stanoviť vašu bezpečnostnú politiku a ciele. Tieto informácie môžete použiť aj ako pomôcku pri výbere základných systémových hodnôt, ktoré ovplyvňujú všetkých užívateľov vo vašom systéme.

Aké formuláre potrebujte ?

Na plánovanie pre vaše aplikácie použite formulár Výber systémových hodnôt.

Keď čítate tieto témy a chcete urobiť rozhodnutia o systémových hodnotách, mali by ste použiť vaše vyplnené formuláre Plán fyzického zabezpečenia a Opis aplikácie.

Pri plánovaní vašej bezpečnostnej stratégie vám pomôžu tieto témy:

- Vypracovanie bezpečnostnej politiky
- Výber vašej úrovne bezpečnosti
- Výber systémových hodnôt, ovplyvňujúcich prihlásenie
- Výber systémových hodnôt, ovplyvňujúcich heslá
- Použitie systémových hodnôt na prispôsobenie vášho systému

Vypracovanie vašej bezpečnostnej politiky

Skôr než začnete s plánovaním, vypracujte vyhlásenie vašej firemnej politiky, ktoré sa týka bezpečnosti vášho systému. Toto vyhlásenie je zmluvou medzi vami a manažmentom vašej spoločnosti. Pomáha vám rozhodovať a určovať, čo je dôležité. Vaša bezpečnostná politika by mala uvádzať, aký je váš celkový prístup a ktoré informácie, ktoré sú súčasťou majetku firmy, vyžadujú ochranu.

Každý systém by mal byť zabezpečený. Pre vašu bezpečnosť si môžete zvoliť jeden z týchto prístupov:

- **Prísny**: Niektorí odborníci to nazývajú bezpečnostnou schémou need-to-know. V prostredí prísnej bezpečnosti dajte užívateľom prístup len k tým informáciám a funkciám, ktoré potrebujú k vykonávaniu svojich úloh. Všetci ostatní sú vylúčení. Mnohí auditori odporúčajú tento prísny prístup.
- **Priemerný**: Priemerný prístup k bezpečnosti dáva užívateľom prístup k objektom na základe oprávnení, ktoré ste im pridelili.
- **Mierny**: V prostredí miernej bezpečnosti umožňujete všetkým oprávneným užívateľom prístup k väčšine objektov v systéme. Prístup obmedzte v prípadoch jedného oddelenia s konkrétnymi závažnými alebo dôvernými prostriedkami. Malá spoločnosť zvyčajne používa vo svojich systémoch mierny prístup.

Váš celkový prístup vám pomôže pri rozhodovaní o vašich konkrétnych požiadavkách na bezpečnosť. Prístup k bezpečnosti vášho systému musí byť v súlade s filozofiou prístupu k informáciám v celej vašej spoločnosti. Ak sa neviete rozhodnúť, ktorý prístup máte použiť, skúste toto:

- Pomocou vyplneného formulára Opis aplikácie určite, kto má alebo nemá mať prístup k týmto aplikáciám.
- Skontrolujte technológie, ktoré používate vo vašej spoločnosti. Ak napríklad plánujete pripojiť váš systém alebo sieť k Internetu, budete chcieť prostredie s reštriktívnejšou bezpečnosťou, aby ste váš systém chránili pred vonkajšími užívateľmi Internetu.
- Porozprávajte sa s ďalšími členmi vašej organizácie, napríklad s auditormi bezpečnosti, aby ste vedeli lepšie stanoviť vaše požiadavky na bezpečnosť.

Nezabudnite, že vašu politiku môžete kedykoľvek zmeniť. Väčšina spoločností zisťuje, že spolu s ich rastom rastie aj potreba prísnejšej bezpečnosti. Tieto informácie vám pomôžu nastaviť schému bezpečnosti, ktorá vám neskôr umožní zvýšiť bezpečnosť bez toho, aby ste museli urobiť veľa zmien alebo znova otestovať všetky vaše aplikácie.

Čo treba zabezpečiť

Okrem vyjadrenia vášho celkového prístupu k bezpečnosti vo vašej bezpečnostnej politike musíte identifikovať dôležité informácie, ktoré sú súčasťou majetku vašej spoločnosti. Váš bezpečnostný systém by mal byť navrhnutý tak, aby tieto informácie chránil. Na určenie závažných informácií, ktoré sú súčasťou majetku spoločnosti, môžete použiť niekoľko požiadaviek:

- **Dôvernosť**: Informácie, ktoré nie sú všeobecne dostupné pre užívateľov vo vašej spoločnosti. Výplatné listiny sú príkladom dôverných informácií.
- **Konkurencieschopnosť**: Informácie, ktoré vám dávajú výhodu oproti vašej konkurencii, napríklad špecifikácie produktov a vzorce.
- **Operácie**: Informácie vo vašom počítači, ktoré sú podstatné pre denné operácie vo vašom podniku, napríklad záznamy o zákazníkoch a stavy inventára.

Sharon Jones, správkyňa bezpečnosti a John Smith, prezident spoločnosti, spolu vypracovali vyhlásenie firemnej bezpečnostnej politiky. John Smith použil tieto poznámky na náčrt bezpečnostnej politiky pre spoločnosť JKL Toy Company. Pravdepodobne si budete chcieť pozrieť bezpečnostnú politiku, ktorú vedenie spoločnosti JKL Toy Company

po naplánovaní a nastavení bezpečnosti rozoslalo všetkým svojim zamestnancom. Pri prechádzaní týchto tém o plánovaní si nezabudnite urobiť poznámky, čo by ste chceli pridať do vašej bezpečnostnej politiky.

Tabuľka 10. Bezpečnostná politika spoločnosti JKL Toy Company: príklad

Celkový prístup
Mierny: Väčšina užívateľov potrebuje mať prístup k väčšine informácií.

Závažné informácie
- Zmluvy a špeciálne ceny
- Výplatná listina
- Záznamy o zákazníkoch a inventári sú dostupné len pre zamestnancov spoločnosti.

Všeobecné pravidlá
- Každý užívateľ systému bude mať užívateľský profil. Užívateľ nemôže zdieľať profily ani heslá.
- Užívatelia musia meniť svoje heslá každých 60 dní.

Po tom, ako si urobíte poznámky, týkajúce sa vašej bezpečnostnej politiky, si môžete zvoliť úroveň vašej bezpečnosti.

Výber vašej úrovne bezpečnosti

Systémová hodnota QSECURITY vám umožňuje určiť, nakoľko chcete mať váš systém zabezpečený. Aby ste pochopili, ako úrovne bezpečnosti pracujú, predstavte si váš systém ako budovu, do ktorej chcú ľudia vstúpiť.

Úroveň 20: Bezpečnosť hesla
Ak vyberiete úroveň 20, máte určitú ochranu bezpečnosti. Stráž pri vchode do budovy vás požiada o preukázanie totožnosti a tajné heslo. Do budovy smú vstúpiť len ľudia, ktorí splnia obe podmienky. Keď už sú však ľudia vnútri, môžu vojsť kamkoľvek a môžu robiť čo chcú.

Ak niekto náhodne začuje tajné heslo a pomocou neho sa dostane dovnútra okolo stráže pri vchode, nie ste chránený.

Úroveň 30: Bezpečnosť hesla a prostriedku
Úroveň 30 vám poskytuje všetko, čo ste mali na úrovni 20 a navyše môžete určovať, kto sa dostane do určitých častí vašej budovy a čo tam bude robiť. Niektoré časti vašej budovy môžete označiť ako verejné, kým ďalšie sú chránené strážami pri vchodoch.

Ľuďom, majúcim prístup do zakázaných častí, môžete povoliť robiť, čo chcú, alebo môžete vyžadovať, aby svoje žiadosti o informácie predložili autorizovaným informátorom (programom). Votrelec, ktorý sa dostane dovnútra použitím hesla niekoho iného, sa ešte stále môže dostať okolo vnútorných stráží do chránených častí

Úroveň 40: Ochrana integrity
Úroveň 40 vám poskytuje všetku ochranu úrovne 30, ale systém overuje prístup užívateľa. Stráže pri vchodoch vo vnútri budovy kontrolujú heslá a protokolujú všetkých užívateľov, ktorí vstupujú do miestnosti.

Úroveň 50: Rozšírená ochrana integrity
Na úrovni 50 stráže uplatňujú ešte prísnejšiu skupinu pravidiel na zabránenie vstupu užívateľom so špeciálnymi znalosťami cez zakázané dvere overením identity každého, kto vstupuje.

Odporúčania

iSeries sa dodáva s úrovňou bezpečnosti 40. Úroveň bezpečnosti 40 je najlepšou voľbou pre väčšinu inštalácií, či už je vaša bezpečnostná politika prísna, priemerná alebo mierna. Ak si vyberiete mierny prístup, k väčšine prostriedkov vo vašom systéme môžete nastaviť verejný prístup. Ak použijete úroveň bezpečnosti 40 od samotného začiatku, v budúcnosti budete bez potreby vykonania mnohých zmien pružnejší pri zvyšovaní bezpečnosti vášho systému.

Ak kupujete aplikačné programy, konzultujte s vaším poskytovateľom aplikácií, aby ste mali istotu, že tieto programy boli otestované na úrovni 40. Niektoré aplikácie používajú operácie, ktoré na úrovni bezpečnosti 40 spôsobujú chyby.

Ak neboli vaše aplikácie otestované na úrovni 40 alebo 50, začnite s úrovňou 30. Pomocou funkcie auditovacieho žurnálu zistite, či vaše aplikácie zaznamenávajú zlyhania oprávnení. Ak nezaznamenávajú, môžete prejsť na úroveň 40 alebo 50.

Úroveň bezpečnosti 50 zabraňuje udalostiam, ku ktorým vo väčšine systémov zvyčajne nedochádza. Systém vykonáva dodatočné kontroly vždy, keď sa vo vašom systéme spúšťajú programy. Tieto dodatočné kontroly môžu mať negatívny účinok na výkon.

Po zadaní vášho výberu úrovne bezpečnosti do formulára Výber systémových hodnôt môžete vybrať systémové hodnoty, ktoré majú vplyv na prihlásenie.

Výber systémových hodnôt, ovplyvňujúcich prihlásenie

Po vybratí vašej úrovne bezpečnosti môžete pomocou systémových hodnôt prispôsobiť to, čo užívatelia vidia na obrazovkách a aká je ich interakcia so systémom. Tieto systémové hodnoty si budete musieť naplánovať a na zaznamenanie vašich výberov budete musieť použiť formulár Výber systémových hodnôt.

Nižšie uvedená tabuľka opisuje systémové hodnoty, použité v tejto téme.

Tabuľka 11. Systémové hodnoty iSeries a ich opisy

Systémová hodnota	Opis
QMAXSIGN	Obmedzuje počet opakovaných pokusov o prihlásenie.
QMAXSGNACN	Špecifikuje akciu, ktorú systém vykonáva v prípade dosiahnutia počtu opakovaných pokusov o prihlásenie.
QLMTDEVSSN	Určuje, či sa užívateľ môže prihlásiť s rovnakým užívateľským profilom na viac ako jednu pracovnú stanicu.
QINACTITV	Určuje, kedy systém zasahuje na neaktívnych úlohách.
QINACTMSGQ	Určuje akciu, ktorú systém vykonáva v prípade, že interaktívna úloha je neaktívna počas doby, špecifikovanej systémovou hodnotou QINACTITV.
QDSCJOBITV	Určuje, či a kedy systém ukončuje úlohu, ktorá bola dočasne odpojená.
QLMTSECOFR	Správcu bezpečnosti, ktorý má oprávnenie na všetky objekty v systéme, obmedzuje na konkrétne zariadenia.

Obmedzenie počtu pokusov o prihlásenie (QMAXSIGN a QMAXSGNACN): Dve systémové hodnoty určujú, koľkokrát sa môže užívateľ pokúsiť prihlásiť do vášho systému a kroky, ktoré systém vykoná po dosiahnutí určeného limitu.

Systémová hodnota QMAXSIGN (maximálny počet pokusov o prihlásenie) obmedzuje počet opakovaných nesprávnych pokusov o prihlásenie, ktoré systém povoľuje predtým, než zasiahne. Nesprávny pokus o prihlásenie znamená, že niekto sa pokúša použiť určitý užívateľský profil buď s neplatným heslom alebo s nesprávnym oprávnením na pracovnú stanicu.

Systémová hodnota QMAXSGNACN (kroky, vykonané pri dosiahnutí maximálneho počtu pokusov o prihlásenie) špecifikuje, čo robí systém v prípade, ak sa niekto pokúša prihlásiť príliš veľakrát za sebou. Možnými hodnotami sú:

1 Zabrániť všetkým ďalším pokusom o prihlásenie v prípade zariadenia. Hovorí sa tomu deaktivovanie zariadenia. Na toto zariadenie sa nemôže nikto prihlásiť, kým oprávnená osoba toto zariadenie neaktivuje príkazom WRKCFGSTS. Táto voľba zvyčajne nie je dostatočnou ochranou, najmä ak sa pokusy o prihlásenie do vášho systému robia z osobného počítača alebo zo vzdialeného systému.

Zariadenie môže znova sprístupniť systémový operátor alebo ktokoľvek s oprávnením *USE na toto zariadenie.

2 Zabrániť všetkým ďalším pokusom o prihlásenie v prípade užívateľského profilu. Hovorí sa tomu

deaktivovanie užívateľského profilu. S týmto profilom sa nikto nemôže prihlásiť, kým ho oprávnená osoba neaktivuje príkazom CHGUSRPRF (Change User Profile).

Aby ste mohli aktivovať užívateľský profil (zmeniť stav), musíte byť správcom bezpečnosti s oprávnením na používanie tohto profilu.

3 Deaktivovať užívateľský profil aj zariadenie.

Riziká a odporúčania

Niektorí záškodníci sa zaoberajú tým, že hádajú heslá a dokážu vniknúť do systémov. Obmedzením počtu vami povolených pokusov o prihlásenie obmedzíte ich možnosti hádať.

Systémová hodnota QMAXSIGN (maximálny počet neplatných prihlásení) určuje, koľko pokusov o prihlásenie povolíte. Nastavte ju dostatočne vysoko, aby ste užívateľov neznechutili. Nastavte ju dostatočne nízko, aby ste užívateľov odradili od neopatrného písania a predišli tak šanci potenciálneho votrelca veľakrát sa pokúšať uhádnuť heslo. Pre maximálny počet pokusov o prihlásenie by ste mali túto hodnotu nastaviť na 3 až 5.

Odporúčaná hodnota QMAXSGNACN (kroky, vykonané pri dosiahnutí maximálneho počtu pokusov o prihlásenie) je 3, aj keď deaktivovanie zariadenia aj užívateľského profilu môže užívateľom systému spôsobiť problémy. Pracovná stanica, umiestnená na súkromnom mieste, môže dať votrelcovi príležitosť vyskúšať veľa rozličných kombinácií užívateľského profilu a hesla. Ak váš systém nemá pracovné stanice, ktoré znamenajú riziko z dôvodu svojho umiestnenia, dostatočnou ochranou bude pravdepodobne len deaktivovanie užívateľského profilu.

Skontrolujte váš vyplnený formulár Fyzické zabezpečenie. Ak máte pracovné stanice vo vzdialených lokalitách alebo máte vzdialených užívateľov (užívatelia, ktorí pristupujú na váš systém prostredníctvom telefónnych liniek alebo pripojení VPN), pravdepodobne budete chcieť prihlasovania prísnejšie obmedziť. Nezabudnite do Časti 2 formulára Výber systémových hodnôt pridať vaše voľby pre systémové hodnoty QMAXSIGN a QMAXSGNACN.

Než vyberiete systémové hodnoty, ktoré obmedzujú užívateľov na používanie jednej pracovnej stanice v rovnakom čase, pravdepodobne budete považovať za užitočné pozrieť si príklad, ktorý demonštruje, ako tieto systémové hodnoty spolupracujú na obmedzení pokusov o prihlasovanie.

Príklad: Obmedzenie pokusov o prihlásenie: Sharon Jones obmedzila počet pokusov o prihlásenie na 3 (QMAXSIGN je 3) a rozhodla sa v prípade prekročenia tohto obmedzenia profil aj zariadenie vypnúť (QMAXSGNACN je 3). Pozrite sa, čo sa môže stať pri dosiahnutí týchto hodnôt:

1. Roger dvakrát nesprávne napíše svoje heslo.
2. Po druhom pokuse dostane varovnú správu, že ďalší nesprávny pokus o prihlásenie vypne jeho užívateľský profil.
3. Znova sa pomýli.
4. Systém jeho profil vypne a pracovná stanica už nezobrazuje prihlasovaciu obrazovku. Ak sa Roger pokúsi prihlásiť na inú pracovnú stanicu, dostane chybovú správu.
5. Teraz musí požiadať Sharon o aktivovanie jeho profilu, aby sa mohol znova pokúsiť o prihlásenie. Sharon alebo systémový operátor musí sprístupniť aj Rogerovu pracovnú stanicu. Ak si Roger nepamätá svoje heslo, Sharon mu môže prideliť heslo dočasné, ktoré musí Roger pri ďalšom prihlásení zmeniť.

Nižšie si môžete pozrieť systémovú hodnotu, ktorá obmedzuje užívateľov na používanie jednej pracovnej stanice v rovnakom čase.

Obmedzenie užívateľov na používanie jednej pracovnej stanice v rovnakom čase: Systémová hodnota QLMTDEVSSN (obmedzenie relácií zariadenia) určuje, či rovnaký užívateľ môže byť prihlásený na viac ako jednu pracovnú stanicu v rovnakom čase. Možné hodnoty sú:

0 Systém povoľuje neobmedzenému počtu užívateľov, aby boli prihlásení v rovnakom čase s rovnakým užívateľským profilom.

1 Užívateľský profil sa môže používať naraz len na jednom zariadení. Užívateľ môže mať na jednom zariadení naraz viac relácií.

Riziká a odporúčania

Povolenie užívateľom prihlasovať sa len na jednu pracovnú stanicu v rovnakom čase zvyšuje úroveň bezpečnostných návykov. Uvoľnené bezpečnostné návyky predstavujú ohrozenie bezpečnosti:

- Ak obmedzíte užívateľov na jedno zariadenie, odradíte ich od zdieľania užívateľských ID a hesiel. Ak užívatelia zdieľajú užívateľské ID, stratíte kontrolu aj zodpovednosť. Už nebudete môcť povedať, kto a čo v systéme naozaj robí.
- Užívatelia sa nesmú zabudnúť odhlásiť z jednej pracovnej stanice skôr, než sa presunú na inú. Pracovné stanice, z ktorých sa užívateľ neodhlásil a pritom sa nepoužívajú, predstavujú ohrozenie bezpečnosti.

Odporúčané nastavenie pre systémovú hodnotu QLMTDEVSSN je 1, čo obmedzuje užívateľov na používanie jedného zariadenia. Každému užívateľovi systému pridelte jedinečné užívateľské ID a heslo s príslušnými oprávneniami a obmedzte ho na používanie len jednej pracovnej stanice v rovnakom čase. Vašu voľbu pre systémovú hodnotu QLMTDEVSSN nezabudnite pridať do Časti 2 formulára Výber systémových hodnôt.

Potom môžete začať plánovať systémové hodnoty pre neaktívne úlohy.

Plánovanie systémových hodnôt pre neaktívne úlohy: Tri systémové hodnoty pracujú spolu, aby určili, aké kroky systém podnikne v prípade, že sa užívateľ zabudne odhlásiť z pracovnej stanice.

Interval uplynutia času, vyhradeného pre neaktívnu úlohu (QINACTITV)
Systémová hodnota QINACTITV určuje, či systém vykonáva nejaké kroky, ak je obrazovka prihlásená, ale po určitú dobu je neaktívna.

Poznámka: **Neaktívny** znamená, že užívateľ nestlačil kláves Enter alebo funkčný kláves v rámci stanoveného časového intervalu.

Front správ neaktívnych úloh (QINACTMSGQ)
Vaše nastavenie pre systémovú hodnotu QINACTMSGQ určuje, čo urobí systém v prípade, že časovému limitu, ktorý stanovíte v systémovej hodnote QINACTITV, skončí platnosť. Ak vyberiete ENDJOB, systém ukončí každú úlohu, ktorá je neaktívna dlhšie ako interval uplynutia vyhradeného času, ktorý ste vybrali pre systémovú hodnotu QINACTITV. Ak vyberiete DSCJOB, systém neaktívnu úlohu odpojí. Ak stanovíte názov frontu správ, systém vyšle do tohto frontu varovnú správu, ak je úloha pridlho neaktívna.

Keď systém **odpojí** úlohu na pracovnej stanici, dočasne ju preruší. Na pracovnej stanici znova naskočí prihlasovacia obrazovka. Odpojená úloha sa obnoví, keď sa na tú istú pracovnú stanicu znova prihlási ten istý užívateľ.

Interval uplynutia času, vyhradeného pre odpojenú úlohu (QDSCJOBITV)
Systémová hodnota QDSCJOBITV určuje, či a kedy systém skončí dočasne odpojenú úlohu. Úlohy môžu byť odpojené automaticky systémom ako výsledok systémových hodnôt QINACTITV a QINACTMSGQ. Užívatelia môžu tiež požadovať, aby boli ich úlohy dočasne odhlásené (odpojené) pomocou voľby v ponuke Operačného asistenta alebo príkazom DSCJOB (Disconnect Job).

Riziká a odporúčania

Ak sa Sharon zabudne pred odchodom odhlásiť z pracovnej stanice, John môže k tejto pracovnej stanici prísť a použiť ktorúkoľvek funkciu, ktorú môže Sharon vykonávať v systéme.

Neaktívne obrazovky by ste mali riadiť najmä z dvoch dôvodov:

- Máte prísne bezpečnostné prostredie s dôvernými informáciami, uloženými vo vašom systéme.
- Pracovné stanice máte umiestnené na miestach, kde sa k nim ľahko dostanú osoby, ktoré nie sú zamestnané vo vašej spoločnosti.

Bežné pracovné úlohy často prerušia užívateľov pri ich pracovných staniciach. Využite spôsob, akým tieto tri systémové hodnoty spolupracujú, aby ste umožnili bežné prerušenia práce a bezpečnosť vášho systému by pritom ostala chránená.

Na zníženie týchto rizík IBM odporúča spoločné používanie systémových hodnôt QINACTITV, QINACTMSGQ a QDSCJOBITV, aby sa umožnili normálne prerušenia práce a zároveň chránila bezpečnosť vášho systému.

Interval uplynutia času, vyhradeného pre neaktívnu úlohu (QINACTITV): Interval nastavte tak, aby bol dostatočne krátky na to, aby užívateľ neriskoval odchod od pracovnej stanice a nenechal ju bez dozoru, ale nie tak krátky, že by užívateľom spôsobil problémy. Odporúčané nastavenie je 30 minút. Ak je úloha neaktívna 30 minút, systém vykoná kroky, špecifikované vo fronte správ neaktívnych úloh.

Front správ neaktívnych úloh (QINACTMSGQ): Vyberte odpojenie úlohy. Systém odpojí každú úlohu, neaktívnu počas časového úseku, špecifikovaného v intervale uplynutia času, vyhradeného pre neaktívnu úlohu. Systém preruší úlohu a odhlási pracovnú stanicu. Keď sa znova prihlási ten istý užívateľ, úloha bude pokračovať od miesta, kde bola prerušená.

Toto je pre užívateľov pohodlnejšie, pretože systém ich úlohy neukončí, ale len preruší. Odpojenie neaktívnej úlohy poskytuje vášmu systému toľko ochrany ako jej ukončenie.

Poznámka: Niektoré úlohy systém nemôže odpojiť. Ak systém nemôže odpojiť neaktívnu úlohu, namiesto odpojenia ju ukončí. Toto môže zapríčiniť stratu informácií. Zvážte nastavenie QINACTMSGQ, aby ste mohli posielať správy do frontu správ systémového operátora.

Interval uplynutia času, vyhradeného pre odpojenú úlohu(QDSCJOBITV): Odporučte užívateľom, aby sa dočasne odhlásili zo systému, ak sa potrebujú od svojich pracovných staníc vzdialiť len na chvíľku a pokiaľ musia na dlhšiu dobu prerušiť prácu, odporučte im, aby ju ukončili a odhlásili sa.

Pomocou systémovej hodnoty QDSCJOBITV ukončite odpojené úlohy skôr, než váš systém spustí nočné spracovanie, napríklad Automatické čistenie. Nastavte túto hodnotu na dostatočne dlhú, aby sa väčšinu pracovného dňa mohli užívatelia vracať k pracovnej stanici, ale dostatočne krátku na to, aby sa úlohy ukončili pred spustením nočného spracovania. Zvoľte 300 minút (päť hodín), ktoré poskytnú nočnému spracovaniu dosť času na dokončenie bez toho, aby bolo narušované úlohou užívateľa.

Poznámka: Aby sa predišlo pokusu dvoch užívateľov meniť rovnaké informácie v rovnakom čase, systém **uzamkne** záznam pred jeho aktualizáciou. Všetky uzamknutia na prostriedkoch ostanú v platnosti, keď systém odpojí úlohu užívateľa. V závislosti od návrhu vašej aplikácie a počtu užívateľov v systéme môžu uzamknutia zapríčiniť vo vašom systéme problémy s výkonom. Poraďte sa s vaším programátorom alebo poskytovateľom aplikácií, aby ste zistili, či uzamknutie môže mať vplyv na výkon.

Pravdepodobne si budete chcieť pozrieť príklad, ako tieto systémové hodnoty spolupracujú, aby ste mohli spracovávať neaktívne úlohy vo vašom systéme.

Po zaznamenaní vašich rozhodnutí o neaktívnych úlohách do formulára Výber systémových hodnôt môžete rozhodnúť, ako obmedziť miesta, kde sa správca bezpečnosti môže prihlásiť.

Príklad: Spracovanie neaktívnych úloh so systémovými hodnotami QINACTITV, QINACTMSGQ a QDSCJOBITV: Povedzme, že ste nastavili interval uplynutia vyhradeného času neaktívnej úlohy (QINACTITV) na 30 minút. Systém odpojí neaktívne úlohy (QINACTMSGQ je DSCJOB). Interval uplynutia vyhradeného času odpojenej úlohy (QDSCJOBITV) je 300 minút (5 hodín). Napríklad ak sa Sharon zabudne odhlásiť o 9:30, systém odpojí jej úlohu o 10:00 a ukončí úlohu o 15:00.

Pridajte svoje voľby pre systémové hodnoty QINACTITV, QINACTMSGQ a QDSCJOBITV v 2. časti formulára Výber systémových hodnôt.

Keď zaznamenáte svoje rozhodnutia pre neaktívne úlohy na formulár výberu systémových hodnôt, môžete sa rozhodnúť, ako obmedzíte, kde sa môže prihlásiť správca bezpečnosti.

Obmedzenie miest, kde sa môže správca bezpečnosti prihlásiť: Užívateľov s oprávnením na zmenu bezpečnosti a riadenie objektov budete pravdepodobne chcieť obmedziť na určité pracovné stanice. Týmto užívateľom to zabraňuje

prihlasovať sa bez vášho vedomia na pracovné stanice na vzdialených miestach. Môžete to urobiť pomocou systémovej hodnoty QLMTSECOFR (obmedzenie správcu bezpečnosti). Ak systémovú hodnotu QLMTSECOFR nastavíte na 1, užívatelia so zvláštnym oprávnením na všetky objekty (*ALLOBJ) alebo so zvláštnym servisným oprávnením (*SERVICE) sa môžu prihlasovať len na tú konzolu alebo ďalšie pracovné stanice, ktoré vy určíte.

Systémová hodnota QLMTSECOFR obmedzuje prihlasovanie správcu bezpečnosti, užívateľov s oprávnením na všetky objekty v systéme a servisných technikov na túto konzolu. Príkazom GRTOBJAUT (Grant Object Authority) môžete týmto užívateľom umožniť prístup na ďalšie zariadenia.

Poznámka: Aby systémová hodnota QLMTSECOFR pracovala, úroveň bezpečnosti vášho systému musí byť 30 alebo vyššia.

Riziká a odporúčania

Systémovú hodnotu QLMTSECOFR by ste mali nastaviť na 1. Ak ktosi náhodou začuje alebo uhádne heslo osoby s profilom správcu bezpečnosti, musí tiež dostať prístup k zariadeniu, ktoré mu umožní sa prihlásiť.

Po vyplnení vašich volieb pre QLMTSECOFR v časti 2 formulára Výber systémových hodnôt, môžete vybrať systémové hodnoty, ktoré sa týkajú hesiel.

Výber systémových hodnôt, ovplyvňujúcich heslá

Užívateľom by ste mali povoliť priradiť svoje vlastné heslá namiesto toho, aby im heslá prideľoval správca bezpečnosti. Keď si užívatelia vytvoria svoje vlastné heslá, zvyčajne si ich nemusia zapisovať. Je tendencia uchovávať zapísané heslá na viditeľných miestach, čím predstavujú bezpečnostné riziko.

Tip na vytváranie hesiel

Vaši užívatelia môžu mať problém s vymyslením dobrého hesla. Navrhnite im túto techniku: Ako pomôcku pri vytvorení vášho hesla, ktoré je ťažké uhádnuť, použite ľahko zapamätateľnú vetu. Napríklad po dovolenke môžete použiť vetu ″4.júla bolo pekné počasie″ na vytvorenie hesla 4JBPP.

Niektoré systémové hodnoty regulujú heslá. Môžete určiť, ako často musia užívatelia meniť svoje heslá. Rovnako môžete vytvoriť mnoho pravidiel na zabránenie použitiu hesiel, ktoré je ľahké uhádnuť. Mnohé z týchto systémových hodnôt sú dôležité pre veľké organizácie. Niekoľko ich je dôležitých pre každého.

Užívatelia si môžu priradiť svoje vlastné heslá použitím voľby z ponuky ASSIST alebo príkazom CHGPWD (Change Password). Keď užívatelia menia svoje vlastné heslá, systém nové heslo skontroluje porovnaním so systémovými hodnotami tohto hesla. Ak užívateľ zmení heslo príkazom CHGUSRPRF, systém nové heslo neskontroluje so systémovými hodnotami bezpečnosti.

Poznámka: Ak ste nastavili ktorúkoľvek zo systémových hodnôt hesla, systém nedovolí, aby sa nové heslo zhodovalo s názvom užívateľského profilu, iba ak by ste na nastavenie hesla použili príkaz CHGUSRPRF.

Nižšie uvedená tabuľka znázorňuje systémové hodnoty, ovplyvňujúce heslá a ich definície:

Tabuľka 12. Systémové hodnoty iSeries súvisiace s heslom

Systémová hodnota	Opis
QPWDEXPITV	Vyžaduje, aby užívatelia po určenej dobe zmenili svoje heslá.
QPWDMAXLEN	Umožňuje vám uviesť maximálnu dĺžku hesiel v znakoch.
QPWDMINLEN	Umožňuje vám uviesť minimálnu dĺžku hesiel v znakoch.
QPWDRQDDIF	Zabraňuje užívateľom používať striedavo dve rozličné heslá.

Podrobnejšie informácie o týchto systémových hodnotách, súvisiacich s heslami, nájdete v nasledujúcich témach:

- Stanovenie doby platnosti hesla

- Stanovenie dĺžky hesiel
- Obmedzenie používania duplicitných hesiel

V príkazovom riadku CL zadajte WRKSYSVAL *SEC a pozrite si online informácie o systémových hodnotách, začínajúcich znakmi QPWD.

Stanovenie doby platnosti hesla: Systémová hodnota QPWDEXPITV stanovuje, ako často musia užívatelia meniť svoje heslá.

Systém užívateľov upozorní, keď sa blíži čas ukončenia platnosti ich hesiel. Ak heslu skončí platnosť, systém vyzve užívateľa, aby svoje heslo pri ďalšom prihlásení zmenil.

Odporúčania

Užívateľ by mal svoje heslo pravidelne meniť. Odrádza to od zdieľania hesiel s ďalšími užívateľmi systému. Rovnako, ak by sa neoprávnený užívateľ dozvedel heslo inej osoby, toto heslo bude fungovať len krátku dobu. Interval zmeny hesla nastavte dosť dlhý na to, aby ste užívateľov nepodráždili, ale dosť krátky na poskytnutie kvalitnej bezpečnosti. Ak sa týmto problémom chcete vyhnúť, tento interval nastavte na 45 až 60 dní.

Po zadaní vašej voľby pre systémovú hodnotu QPWDEXPITV do Časti 2 vášho formulára Výber systémových hodnôt môžete stanoviť dĺžku hesiel.

Stanovenie dĺžky hesiel: Niektorí užívatelia neradi píšu. Ak ich necháte, zvolia si heslo, ktoré tvorí jedno písmeno alebo svoje iniciály. Krátke heslá však nanešťastie zvyšujú šancu votrelcov uhádnuť tieto heslá. Systémová hodnota QPWDMINLEN vám umožňuje stanoviť minimálnu požadovanú dĺžku pre všetky heslá vo vašom systéme.

Ak váš systém komunikuje s inými systémami, užívatelia si môžu medzi dvomi počítačmi vymieňať heslá. Niektoré metódy komunikácie obmedzujú dĺžku hesla na maximálne 8 znakov. Systémová hodnota QPWDMAXLEN vám umožňuje stanoviť maximálnu dĺžku hesiel.

Odporúčania

Minimálnu dĺžku vašich hesiel stanovte na 6 znakov. Tým sa vylúči používanie iniciál a užívateľov to povzbudí, aby boli trocha tvorivejší pri vyberaní hesiel. Ak váš systém komunikuje s inými systémami, maximálnu dĺžku vašich hesiel stanovte na 8 znakov.

Po zadaní vašich volieb pre systémové hodnoty QPWDMINLEN a QPWDMAXLEN do Časti 2 vášho formulára Výber systémových hodnôt sa môžete rozhodnúť, nakoľko máte obmedziť používanie duplicitných hesiel.

Obmedzenie používania duplicitných hesiel: Príkaz CHGPWD (Change Password) vyžaduje, aby sa nové heslo odlišovalo od hesla starého. Užívatelia však môžu striedavo používať dve odlišné heslá, pokiaľ im v tom nezabránite pomocou systémovej hodnoty QPWDRQDDIF. Nižšie uvedená tabuľka znázorňuje voľby pre systémovú hodnotu QPWDRQDDIF:

Tabuľka 13. Hodnoty pre systémovú hodnotu QPDRQDDIF

Hodnota	Počet hesiel, skontrolovaných na duplicitu
0	0 Duplicitné heslá sú povolené.
1	32
2	24
3	18
4	12
5	10
6	8
7	6
8	4

Odporúčania

Ak chcete vyžadovať, aby heslá boli rok jedinečné, použite interval ukončenia platnosti hesla a hodnoty duplicitného hesla. Napríklad, ak platnosť hesiel končí po 60 dňoch, pre systémovú hodnotu QPWDRQDDIF vyberte hodnotu 7.

Po zadaní vašej voľby pre systémovú hodnotu QPWDRQDDIF do Časti 2 vášho formulára Výber systémových hodnôt sa môžete rozhodnúť, ako máte systémové hodnoty použiť na prispôsobenie vášho systému.

Použitie systémových hodnôt na prispôsobenie vášho systému

Server iSeries používa systémové hodnoty a sieťové atribúty na riadenie mnohých iných aktivít než bezpečnosti. Systémoví a aplikační programátori používajú väčšinu týchto systémových hodnôt a atribútov. Správca bezpečnosti by mal na prispôsobenie vášho systému stanoviť niekoľko systémových hodnôt a sieťových atribútov.

Pomenovanie vášho systému

Na priradenie názvu vášmu systému použite sieťový atribút SYSNAME. Názov systému sa zobrazuje v pravom hornom rohu vašej prihlasovacej obrazovky a v systémových správach. Používa sa tiež, keď váš systém komunikuje s iným systémom, alebo s osobnými počítačmi pomocou iSeries Access for Windows.

Pri komunikácii vášho systému s inými systémami alebo s osobnými počítačmi názov systému identifikuje a odlišuje váš systém od iných systémov v sieti. Počítače pri každej komunikácii striedajú názvy systému. Keď raz priradíte systému názov, nemali by ste ho meniť, pretože jeho zmena ovplyvňuje ďalšie systémy vo vašej sieti.

Odporúčania

Vyberte pre váš systém zmysluplný a jedinečný názov. Aj keď v súčasnosti s inými počítačmi nekomunikujete, môže k tomu dôjsť v budúcnosti. Ak je váš systém súčasťou siete, správca siete vám pravdepodobne povie, aký názov systému máte použiť.

Sharon Jones v spoločnosti JKL Toy Company napríklad rozhodla dať systému názov JKLTOY.

Zobrazenie času a dátumu vo vašom systéme

Keď váš systém tlačí alebo zobrazuje dátum, môžete stanoviť postupnosť, v ktorej sa zobrazí rok, mesiac a deň. Tak isto môžete špecifikovať znaky, ktoré má váš systém použiť medzi rokom (R), mesiacom (M) a dňom (D).

Formát dátumu určuje systémová hodnota QDATFMT. Nasledujúci diagram znázorňuje všetky možnosti, ako systém tlačí dátum 16. jún 2000:

Tabuľka 14. QDATFMT (Formáty systémového dátumu)

Vaša voľba	Opis	Výsledok
RMD	Rok, Mesiac, Deň	00/06/16
MDR	Mesiac, Deň, Rok	06/16/00
DMR	Deň, Mesiac, Rok	16/06/00
JUL	Juliánsky dátum	00/168

Poznámka: Tieto príklady používajú ako oddeľovač dátumu lomku (/).

Systémová hodnota QDATSEP určuje, aké znaky systém používa medzi rokom, mesiacom a dňom. Nižšie uvedená tabuľka znázorňuje vaše voľby. Na špecifikovanie vašej voľby použite číslo:

Tabuľka 15. QDATSEP (Oddeľovač systémového dátumu)

Oddeľovací znak	Hodnota QDATSEP	Výsledok
/ (lomka)	1	16/06/00

Tabuľka 15. QDATSEP (Oddeľovač systémového dátumu) (pokračovanie)

Oddeľovací znak	Hodnota QDATSEP	Výsledok
- (pomlčka)	2	16-06-00
. (bodka)	3	16.06.00
, (čiarka)	4	16,06,00
(prázdny znak)	5	16 06 00

Poznámka: Vyššie uvedené príklady používajú formát DMR.

Systémová hodnota QTIMSEP určuje, ktoré znaky systém používa pri zobrazovaní času na oddeľovanie hodín, minút a sekúnd. Na špecifikovanie vašej voľby použite číslo. Nižšie uvedená tabuľka znázorňuje, aký formát by mal čas 10:30 predpoludním použitím jednotlivých hodnôt:

Tabuľka 16. QTIMSEP (Oddeľovač systémového času)

Oddeľovací znak	QTIMSEP	Výsledok
: (dvojbodka)	1	10:30:00
. (bodka)	2	10.30.00
, (čiarka)	3	10,30,00
(prázdny znak)	4	10 30 00

Rozhodnutie, ako pomenovať vaše systémové zariadenia

Váš systém automaticky konfiguruje všetky nové pracovné stanice a tlačiarne, ktoré k nemu pripájate. Systém dáva každému novému zariadeniu názov. Systémová hodnota QDEVNAMING určuje, ako sa tieto názvy priraďujú. Nižšie uvedený diagram znázorňuje, aký názov dá systém tretej pracovnej stanici a druhej tlačiarni, pripojenej k vášmu systému:

Tabuľka 17. Pomenovanie systémového zariadenia

Vaša voľba	Formát názvu	Názov pracovnej stanice	Názov tlačiarne
1	iSeries	DSP03	PRT02
2	S/36	W3	P2
3	Adresa zariadenia	DSP010003	PRT010002

Poznámka: Vo vyššie uvedenom príklade sú pracovná stanica a tlačiareň pripojené k prvému káblu.

Odporúčania

Používajte názvové konvencie iSeries, pokiaľ nepoužívate softvér, ktorý vyžaduje pomenúvanie S/36. Názvy iSeries pre obrazovkové stanice a tlačiarne sú praktickejšie ako názvy, ktoré používajú adresu zariadenia. Názvy pracovných staníc a tlačiarní sa zobrazujú na niektorých obrazovkách Operačného asistenta. Názvy tlačiarní sa používajú aj na riadenie tlačového výstupu.

Po nakonfigurovaní nového zariadenia systémom zadajte príkazom CHGDEVDSP (Change Display Device) alebo príkazom CHGDEVPRT (Change Printer Device) zmysluplný opis tohto zariadenia. Do opisu zahrňte fyzickú adresu aj umiestnenie tohto zariadenia, napríklad *Kancelária Johna Smitha, linka 1 adresa 6*.

Výber vašej systémovej tlačiarne

Na priradenie vašej systémovej tlačiarne použite systémovú hodnotu QPRTDEV. Táto systémová hodnota, užívateľský profil a opis úlohy určujú tlačiareň, ktorú používa úloha. Ak užívateľský profil alebo opis úlohy nešpecifikuje inú tlačiareň, úloha používa systémovú tlačiareň.

Odporúčania

Za normálnych okolností by systémová tlačiareň mala byť najrýchlejšou tlačiarňou vo vašom systéme. Systémovú tlačiareň používajte pre dlhé správy a systémový výstup.

Poznámka: Až do nainštalovania a nakonfigurovania vášho systému nebudete poznať názvy vašich tlačiarní. Teraz si urobte poznámky o umiestnení vašej systémovej tlačiarne. Názov tlačiarne vyplňte neskôr.

Povolenie zobrazenia dokončeného tlačového výstupu

Systém poskytuje užívateľom možnosť nájsť ich tlačový výstup. Obrazovka Work with Printer Output zobrazuje celý výstup, ktorý sa aktuálne tlačí alebo čaká na tlač. Užívateľom môžete umožniť aj pozrieť sa na zoznam dokončeného tlačového výstupu. Táto obrazovka ukazuje, kedy a na ktorej tlačiarni sa výstup tlačí. Môže to byť užitočné pri lokalizovaní stratených správ.

Funkcia analyzovania úlohy a systémová hodnota QACGLVL vám umožňujú zobraziť dokončený tlačový výstup. Voľba *PRINT v systémovej hodnote QACGLVL umožňuje uloženie informácií o dokončenom tlačovom výstupe.

Odporúčania

Ukladanie informácií o dokončenom tlačovom výstupe zaberá priestor vo vašom systéme. Ak si myslíte, že vaši užívatelia nebudú tlačiť veľa správ, pravdepodobne nebudete musieť túto funkciu poskytnúť. Do formulára Výber systémových hodnôt zadajte NIE. Táto hodnota nastavuje úroveň analyzovania úlohy na *NONE.

- Skontrolujte, či ste napísali vyhlásenie bezpečnostnej politiky pre vašu vlastnú spoločnosť podobne, ako ho vypracovali Sharon Jones a John Smith v príklade spoločnosti JKL Toy Company.
- Skontrolujte, či ste do formulára Výber systémových hodnôt zadali vaše voľby systémových hodnôt.
- Urobte si poznámky k tomu, čo by ste chceli zahrnúť do vášho vyhlásenia o bezpečnosti.

Po zadaní všetkých volieb vášho systému do formulára Výber systémových hodnôt a napísaní bezpečnostnej politiky môžete naplánovať skupiny užívateľov.

Príklad: Bezpečnostná politika spoločnosti JKL Toy: Nasledujúce oznámenie objasňuje bezpečnostnú stratégiu, ktorú John Smith, prezident spoločnosti JKL Toy, poslal svojim zamestnancom. Použil poznámky, ktoré si spolu so Sharon urobil, aby mohol vytvoriť toto bezpečnostné oznámenie.

Tabuľka 18. Príklad: Bezpečnostné oznámenie spoločnosti JKL Toy

Od: John Smith, prezident

Tabuľka 18. Príklad: Bezpečnostné oznámenie spoločnosti JKL Toy (pokračovanie)

Spoločnosť JKL Toy

Komu: Všetkým zamestnancom Spoločnosť JKL Toy

Predmet: Zabezpečenie nového systému

Všetci ste sa zúčastnili na informačnom stretnutí o našom novom systéme. Tí, ktorí budú tento systém používať, sa začali školiť a budúci týždeň začnú spracovávať zákaznícke objednávky. Očakávame, že tento systém sa rýchlo stane kľúčovým pre úspech nášho podniku.

Chcem zopakovať naše rozhodnutia a stratégie týkajúce sa bezpečnosti a zdôrazniť ich dôležitosť. Tieto stratégie boli navrhnuté pre ochranu informácií, ktoré sú pre náš podnik kľúčové.

- Za bezpečnosť nového systému zodpovedá Sharon Jones. Pomáhať jej bude Ken Harrison. Obráťte sa na nich, ak budete mať akékoľvek otázky alebo podozrenie, že sa vyskytli problémy zabezpečenia.
- Naše rozhodnutia o tom, kto môže vykonávať funkcie v systéme, sú založené na našich súčasných stratégiách týkajúcich sa informácií. Uvediem príklad:
  - Informácie o kontraktoch a zvláštnych cenách sú považované za dôverné. Nikdy by sa nemali prezrádzať nikomu mimo spoločnosti.
  - Iba učtáreň môže stanovovať a meniť úverové limity pre našich zákazníkov.
- Každý, kto potrebuje systém používať, dostane ID užívateľa a heslo. Bude sa vyžadovať, aby ste si svoje heslo zmenili po prvom prihlásení sa do systému, a potom po každých 60 dňoch. Vyberte si heslo, ktoré si dokážete zapamätať, ale nie také, ktoré je očividné. Formulár, ktorý dostanete s vaším ID užívateľa, obsahuje určité návrhy na vytváranie hesiel.
- *Nezdieľajte svoje heslo s nikým iným.*. Chceme, aby ste v systéme mohli robiť všetko, čo je nutné pre vašu prácu. Ak potrebujete prístup k informáciám, obráťte sa na Sharon alebo na Kena. Ak svoje heslo zabudnete, Sharon alebo Ken vám môžu ihneď nastaviť nové. Nemal by byť žiaden dôvod, aby sa niekto prihlasoval s ID užívateľa a heslom niekoho iného.
- Možno ste sa naučili používať na vašej pracovnej stanici funkciu záznamu a reprodukcie na uloženie toho, čo ste napísali. *Nepoužívajte* ju na uloženie svojho hesla.
- Nenechávajte svoju pracovnú stanicu prihlásenú, keď nie ste na svojom pracovnom mieste. Počas školenia ste sa naučili dočasne odhlásiť pracovnú stanicu. Používajte túto funkciu, ak potrebujete odísť z vášho pracovného miesta na krátky čas. Ak budete preč dlhší čas, ukončite prácu a použite normálne odhlásenie.

  Odhlásiť sa, keď odchádzate od svojej pracovnej stanice, je zvlášť dôležité na miestach, ktoré sú dostupné verejnosti, ako je napríklad nakladacia rampa, priestor služieb zákazníkom a vzdialené predajné kancelárie.
- AJ keď systémová jednotka je veľmi robustná, chráňte ju pred nárazmi a neklaďte na ňu veci. Ovládacie panely na jednotke sú za normálnych okolností deaktivované, ale, prosím, nedotýkajte sa ich. Pracovníci učtárne sú zodpovední za zaistenie, aby nikto nedovolene nezasahoval do systémovej jednotky.

Pamätajte na to, že náš nový systém má všetky naše úlohy uľahčovať a zvyšovať výkon nášho podniku. Naše bezpečnostné stratégie by vám mali pomáhať, nie vám prekážať. Ak budete mať akékoľvek otázky alebo vám bude niečo robiť starosti, neváhajte a obráťte sa na Sharon, Kena alebo na mňa.

Po vytvorení konceptu vašej bezpečnostnej politiky môžete začať s plánovaním skupín užívateľov.

Plánovanie skupín užívateľov

Prvý krok v procese plánovania, rozhodnutie o vašej bezpečnostnej stratégii, je niečo podobné ako zavedenie firemnej politiky. Teraz môžete začať plánovať skupiny užívateľov, čo je niečo ako rozhodnutie o politike oddelenia.

Čo je skupina užívateľov ?

Skupina užívateľov je presne to, čo naznačuje jej názov: je to skupina užívateľov, ktorí potrebujú používať rovnaké aplikácie rovnakým spôsobom. Skupinu užívateľov zvyčajne tvoria užívatelia, ktorí pracujú v tom istom oddelení a majú podobné pracovné zaradenie. Zadefinujte skupinu užívateľov vytvorením skupinového profilu.

Ako funguje skupinový profil ?

Skupinový profil slúži v systéme dvom účelom:

- **Bezpečnostný nástroj**: Skupinový profil umožňuje jednoduchý spôsob organizovania užívateľov, ktorí môžu používať určité objekty vo vašom systéme (oprávnenia na objekt). Oprávnenia na objekt môžete zadefinovať pre celú skupinu a nie pre každého člena skupiny zvlášť.
- **Nástroj prispôsobenia**: Skupinový profil môžete používať ako vzor pre vytváranie individuálnych užívateľských profilov. Väčšina užívateľov, ktorí patria do rovnakej skupiny, majú rovnaké požiadavky na prispôsobenie, napríklad na úvodnú ponuku a štandardnú tlačiareň. Týchto užívateľov môžete zadefinovať v skupinovom profile a skopírovať ich do jednotlivých užívateľských profilov.

Skupinové profily vám uľahčujú zachovávať jednoduchú a konzistentnú schému pre bezpečnosť aj prispôsobenie.

Aké formuláre potrebujte ?

K plánovaniu vašich skupín užívateľov potrebujete tieto formuláre:

- Formulár Identifikácia skupiny užívateľov
- Formulár Opis skupiny užívateľov

Poznámka: Pre každú skupinu užívateľov, ktorú budete mať vo vašom systéme, budete potrebovať jeden formulár Opis skupiny užívateľov.

Pri vyplňovaní týchto formulárov vám pomôže, ak si prečítate tieto témy:

- Identifikovanie skupín užívateľov.
- Plánovanie skupinových profilov.
- Výber hodnôt, ovplyvňujúcich prihlásenie.
- Výber hodnôt, obmedzujúcich, čo smie užívateľ robiť.
- Výber hodnôt, nastavujúcich prostredie užívateľa.

Identifikovanie skupín užívateľov

Keď plánujete vaše skupiny užívateľov, musíte najprv identifikovať skupiny užívateľov vo vašom systéme. Umožní vám to naplánovať prístupy k prostriedkom, ktoré tieto skupiny potrebujú. Skúste použiť jednoduchý spôsob identifikácie vašich skupín užívateľov. Berte do úvahy oddelenia alebo pracovné skupiny, ktoré budú používať systém. Pozrite si tabuľku vašich aplikácií, ktorú ste si už predtým vyplnili. Pozrite sa, či medzi pracovnými skupinami a aplikáciami existuje prirodzený vzťah:

- Viete identifikovať primárnu aplikáciu pre každú pracovnú skupinu ?
- Viete, ktoré aplikácie jednotlivé skupiny potrebujú ? Ktoré aplikácie nepotrebujú ?
- Viete, ktorá skupina bude vlastniť informácie v každej knižnici aplikácií ?

Ak viete na tieto otázky odpovedať ″Áno″, môžete začať plánovať vaše skupiny užívateľov. Ak ste však odpovedali ″občas″ alebo ″možno″, identifikovať vaše skupiny užívateľov vám asi pomôže použitie systematického prístupu.

Pravdepodobne si budete chcieť pozrieť príklad použitia tohto prístupu na identifikáciu skupín užívateľov.

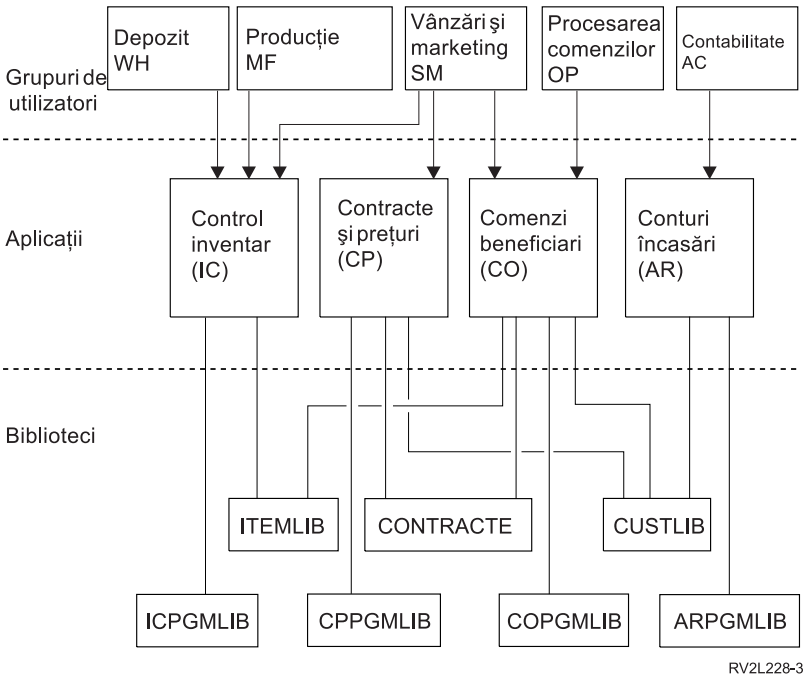
Poznámka: Ak užívateľov urobíte členmi len jedného skupinového profilu, zjednoduší to riadenie vašej bezpečnosti. Niektoré situácie však môžu profitovať z toho, ak užívatelia patria do viac ako jedného skupinového profilu.

Je zvyčajne jednoduchšie manažovať užívateľov, ktorí patria do viac ako jedného skupinového profilu, než udeľovať veľa súkromných oprávnení individuálnym užívateľským profilom.

Príklad: Identifikovanie skupín užívateľov: Ak sa vzťah medzi pracovnými skupinami a aplikáciami zdá byť komplikovaný alebo nejasný, vyjasniť ho môže použitie maticovej techniky ako je formulár Identifikácia skupiny užívateľov. Keď užívateľov systému a ich požiadavky na aplikácie plánujete v matici, mali by sa vám zjaviť podobné

vzory. Sharon Jones okrem vyplnenia formulára Identifikácia skupín užívateľov použila svoj diagram aplikácií na identifikovanie skupín užívateľov, ktoré potrebovali prístup k týmto aplikáciám.

Nižšie znázornená ilustrácia ukazuje diagram aplikácií spoločnosti JKL Toy Company.



Ak je váš prístup k bezpečnosti mierny, na označenie, že užívateľ potrebuje aplikáciu, použite znak X. Ak je váš prístup k bezpečnosti prísny, musíte vziať do úvahy, ako užívatelia používajú aplikácie. Namiesto vloženia znaku X do matice použite znak V (view - prezerať), ak sa niekto chce len pozrieť na informácie v aplikácii. Ak potrebuje niekto robiť zmeny v týchto informáciách, použite znak C (change - zmeniť). Ak má niekto primárnu zodpovednosť za tieto informácie, použite znak O (owner - vlastník).

Napríklad v spoločnosti JKL Toy Company rôzne skupiny potrebujú aplikáciu Cenotvorba a Zmluvy:

- Obchodné a marketingové oddelenie určuje ceny a vypracováva zákaznícke zmluvy. Toto oddelenie *vlastní* informácie o cenotvorbe a zmluvách.
- Oddelenie zákazníckych objednávok nepriamo mení informácie v zmluvách. Pri spracovávaní objednávok sa objemy v zmluve menia. Toto oddelenie musí *meniť* cenové informácie a informácie v zmluvách.
- Pracovníci, ktorí spracovávajú objednávky, musia vidieť informácie o úverovom limite, aby si mohli naplánovať svoju prácu, tieto informácie však nemajú povolené meniť. Potrebujú si *prezrieť* súbor úverového limitu.

Tabuľka 19. Formulár Identifikácia skupiny užívateľov, ktorý používa spoločnosť JKL Toy Company: príklad

Formulár Identifikácia skupiny užívateľov					
Vypracovala: Sharon Jones		Dátum: 9/2/99			
		Potrebný prístup k aplikáciám			
Meno užívateľa	Oddelenie	APP: CO	APP: IC	APP: PC	APP: AR
Ken H.	OP (Order Processing - Spracovanie objednávok)	O	C	C	C
Karen R.	OP (Order Processing - Spracovanie objednávok)	O	C	C	C
Kris T.	AC (Accounting - Účtovníctvo)	V		V	O
Sandy J.	AC (Accounting - Účtovníctvo)	V	C	V	O

Tabuľka 19. Formulár Identifikácia skupiny užívateľov, ktorý používa spoločnosť JKL Toy Company: príklad (pokračovanie)

Peter D.	AC (Accounting - Účtovníctvo)	C		V	O
Ray W.	WH (Warehouse - Sklad)	V	O	V	
Rose Q.	WH (Warehouse - Sklad)	V	O	V	
Roger T.	SM (Sales and Marketing - Obchod a marketing)	C	C	O	C
Sharon J.	MG (Managers - manažéri)	C	C	C	C

Poznámka:

- Ak je vaše bezpečnostné prostredie *Mierne*, na označenie, ktoré aplikácie užívatelia potrebujú, použite znak X.
- Ak je vaše bezpečnostné prostredie *Priemerné*, na označenie, ktorí užívatelia a na ktoré aplikácie budú mať oprávnenie, použite znak A.
- Ak je vaše bezpečnostné prostredie *Prísne*, pravdepodobne budete musieť použiť znaky C (change - zmeniť), V (view - prezerať) a O (owner - vlastník), aby ste mohli určiť, *ako* sa tieto aplikácie majú používať.

Sharon Jones si pri vypracovaní matice urobila niekoľko poznámok o svojich rozhodnutiach:

- Spracovanie objednávok a účtovníctvo si navzájom poskytujú zálohovanie. V súčasnosti vyžadujú podobné aplikácie. Mali by však byť osobitnými skupinami, pretože v budúcnosti budú z dôvodu svojho nárastu viac špecializované.
- Napriek tomu, že oddeleniu spracovania objednávok nepovoľujeme meniť inventár alebo zmluvy priamo, stavy položiek a zmlúv sa automaticky menia pri vytváraní a vybavovaní objednávok. Stane sa to neskôr problematikou, týkajúcou sa bezpečnosti ?
- Pracovníci obchodného a marketingového oddelenia sú zapojení do všetkých častí obchodu a do každej aplikácie. Stanovujú ceny a opisy položiek. Etablujú nových zákazníkov, hoci úverové limity stanovuje účtovníctvo. Sú zodpovední za stanovenie všetkých zmluvných podmienok a cien.

Rozhodnite, aké majú byť skupiny vašich užívateľov. Ak potrebujete pomôcku pri vašom rozhodovaní, vyplňte formulár Identifikácia skupiny užívateľov.

Po pridaní vašich užívateľov do formulára Identifikácia skupiny užívateľov môžete naplánovať skupinový profil.

Plánovanie skupinového profilu

Po identifikácii vašich skupín užívateľov môžete začať plánovať profil pre každú skupinu. Mnohé z vašich rozhodnutí majú vplyv na bezpečnosť aj na prispôsobenie. Napríklad, ak stanovíte úvodnú ponuku, užívateľa môžete obmedziť len na túto ponuku. Takisto však zabezpečujete, aby užívateľ po prihlásení videl správnu ponuku.

Ako príklad vypracujte pre jednu skupinu formulár Opis skupiny užívateľov. Po dokončení prvého formulára sa vráťte a vyplňte formuláre pre ďalšie skupiny, ktoré potrebujete.

Bezpečnosť a prispôsobovanie iSeries sú navrhnuté, aby boli veľmi flexibilné. Metóda plánovania v tejto téme poskytuje správny spôsob navrhnutia opisov skupinových profilov a úloh, váš programátor alebo poskytovateľ aplikácií môže však odporučiť inú metódu.

Pomenovávanie skupinových profilov

Vzhľadom na to, že skupinový profil funguje ako zvláštny typ užívateľského profilu, pravdepodobne budete chcieť skupinové profily ľahko identifikovať v zoznamoch a na obrazovkách. Musíte im priradiť zvláštne názvy. Ak chcete, aby sa vaše skupinové profily zobrazovali v zoznamoch spolu, mali by začínať rovnakými znakmi, napríklad GRP (v prípade skupiny) alebo DPT (v prípade oddelenia). Pri pomenovávaní skupín užívateľov sa riaďte týmito inštrukciami:

- Názvy skupín užívateľov sa môžu skladať z najviac 10 znakov.
- Názov môže obsahovať písmená, číslice a zvláštne znaky: znak mriežky (#), dolára ($), podčiarkovníka (_) a zavináča (@).

- Názov nesmie začínať číslicou.

Poznámka: Systém priradí každému skupinovému profilu identifikačné číslo skupiny (*gid*). Zvyčajne môžete nechať systém vygenerovať *gid*. Ak váš systém používate v sieti, pravdepodobne budete musieť skupinovým profilom priradiť konkrétne gid. Poraďte sa s vaším správcom siete, či musíte priradiť gid.

Váš systém pomenovávania skupinových profilov by ste mali pridať do príslušného poľa vo formulári Názvové konvencie. Sharon Jones napríklad zvolila DPT ako názvovú konvenciu pre skupinové profily. Vyplnila príslušnú časť formulára Názvové konvencie.

Tabuľka 20. Formulár Názvové konvencie, ktorý používa spoločnosť JKL Toy Company: Príklad skupinového profilu

Typ objektu	Názvová konvencia
Skupinové profily	Použite znaky DPT, za ktorými nasleduje skratka oddelenia. Textovým opisom skupinového profilu by mal byť názov tohto oddelenia.

Určenie, ktoré aplikácie a knižnice skupina užívateľov potrebuje

Pokiaľ ste to ešte neurobili, pridajte vaše skupiny užívateľov do diagramu aplikácií a knižníc, ktorý už máte nakreslený. Tento vizuálny obraz vám pomôže pri rozhodovaní o požiadavkách každej skupiny na prostriedky a aplikácie.

V Časti 1 formulára Opis skupiny užívateľov označte primárnu aplikáciu skupiny, čo je aplikácia, ktorú táto skupina používa najčastejšie. Uveďte ďalšie aplikácie, ktoré táto skupina potrebuje.

Pozrite sa do svojich formulárov Opis aplikácie a na diagram aplikácií, aby ste videli knižnice, ktoré jednotlivé skupiny potrebujú. S vaším programátorom alebo poskytovateľom aplikácií pohľadajte najlepší spôsob poskytnutia prístupu k týmto knižniciam. Väčšina aplikácií používa jednu z týchto techník:

- Aplikácia obsahuje knižnice, ktoré sú na užívateľovom úvodnom zozname knižníc.
- Aplikácia spúšťa nastavovací program, ktorý umiestňuje tieto knižnice do užívateľovho zoznamu knižníc.
- Knižnice nemusia byť v zozname knižníc. Knižnicu vždy špecifikujú aplikačné programy.

Systém používa zoznam knižníc na vyhľadávanie súborov a programov, ktoré potrebujete, keď spúšťate aplikácie. **Zoznam knižníc** je zoznam knižníc, v ktorom systém vyhľadáva objekty, potrebné pre užívateľa. Má dve časti:

1. **Systémová časť**: Je špecifikovaná v systémovej hodnote QSYSLIBL, systémová časť sa používa pre knižnice OS/400. Štandard pre túto systémovú hodnotu netreba meniť.
2. **Užívateľská časť**: Systémová hodnota QUSRLIBL poskytuje užívateľskú časť zoznamu knižníc. Užívateľov opis úlohy špecifikuje úvodný zoznam knižníc alebo príkazy po prihlásení užívateľa. Ak máte úvodný zoznam knižníc, tento nahrádza systémovú hodnotu QUSRLIBL. Knižnice aplikácií by mali byť zahrnuté do užívateľskej časti zoznamu knižníc.

Použitie opisu úlohy

Keď sa užívateľ prihlási do systému, užívateľov opis úlohy definuje mnohé charakteristiky tejto úlohy, vrátane toho, ako táto úloha tlačí, ako sa spúšťajú dávkové úlohy a úvodný zoznam knižníc. Váš systém sa dodáva s opisom úlohy, ktorý má názov QDFTJOBD a ktorý môžete použiť pri vytváraní užívateľských profilov. QDFTJOBD však špecifikuje systémovú hodnotu QUSRLIBL ako úvodný zoznam knižníc. Ak chcete, aby rôzne skupiny užívateľov mali pri prihlásení prístup k rôznym knižniciam, mali by ste pre každú skupinu vytvoriť jedinečné opisy úlohy.

Do formulára Opis skupiny užívateľov uveďte každú knižnicu, ktorú skupina potrebuje. Ak má byť knižnica zahrnutá do úvodného zoznamu knižníc v opise úlohy tejto skupiny, do formulára zaznačte názov každej knižnice.

Než začnete vyberať hodnoty, ovplyvňujúce prihlásenie, pravdepodobne si budete chcieť pozrieť príklad, ako Sharon Jones opísala skupiny užívateľov v spoločnosti JKL Toy Company.

Príklad: Formulár opisu skupiny užívateľov spoločnosti JKL Toy: Prvá tabuľka ukazuje 1. časť formulára Opis skupiny užívateľov, ktorý Sharon Jones pripravila pre oddelenie odbytu a marketingu. Všimnite si, že nezahrnula knižnice CONTRACTS a CPPGMLIB do úvodného zoznamu knižníc skupiny. Aplikácia ich automaticky pridá do zoznamu knižníc namiesto ich začlenenia do úvodného zoznamu knižníc DPTSM. Keď užívateľ aplikáciu ukončí, systém tieto knižnice odstráni zo zoznamu knižníc. Tým sa týmto knižniciam poskytne dodatočné zabezpečenie, pretože môžete do nich uskutočňovať prístup len prostredníctvom aplikačných programov.

Tabuľka 21. Formulár opisu skupiny užívateľov spoločnosti JKL Toy: Príklad opisných informácií

Formulár opisu skupiny užívateľov	1. časť z 2
Pripravil: Sharon Jones	Dátum: 9/5/99
Názov skupinového profilu: DPTSM Opis skupiny: Oddelenie odbytu a marketingu	
Primárna aplikácia pre skupinu: Kontrakty a tvorba cien Výpis ostatných aplikácií potrebných pre skupinu: Zásoby (pre zadanie opisov položiek a cien), Zákaznícke objednávky	
Urobte výpis každej knižnice, ktorú skupina potrebuje. Označte (✓) každú knižnicu, ktorá by mala byť v úvodnom zozname knižníc pre skupinu: • ✓CUSTLIB • ✓ITEMLIB • ✓COPGMLIB • ✓ICPGMLIB • CPPGMLIB • CONTRACTS	

Okrem toho Sharon spustila aj formulár opisu skupiny užívateľov pre sklad.

Tabuľka 22. Formulár opisu skupiny užívateľov: Opisné informácie

Formulár opisu skupiny užívateľov	1. časť z 2
Pripravil: Sharon Jones	Dátum: 9/5/99
Názov skupinového profilu: DPTWH Opis skupiny: Sklad	
Primárna aplikácia pre skupinu: Riadenie zásob Výpis ostatných aplikácií potrebných pre skupinu: žiadne	
Urobte výpis každej knižnice, ktorú skupina potrebuje. Umiestnite značku zaškrtnutia (✓) pred každú knižnicu, ktorá by mala byť v úvodnom zozname knižníc pre skupinu: • ✓ITEMLIB • ✓ICPGMLIB	

Po vyplnení 1. časti formulára opisu skupiny užívateľov môžete začať s výberom hodnôt, ktoré ovplyvňujú prihlásenie.

Výber hodnôt, ovplyvňujúcich prihlásenie

Po naplánovaní skupinových profilov vo vašom systéme musíte vybrať systémové hodnoty, ktoré ovplyvňujú prihlásenie. Svoje voľby zadajte do Časti 2 formulára Opis skupiny užívateľov. Nezabudnite, že vyberáte hodnoty, ktoré sa budú kopírovať na vytvorenie individuálnych profilov pre členov skupiny. Začnite zadaním názvu skupinového profilu, ktorý ste vybrali a stručným opisom (Textovým) pre túto skupinu.

Ak váš systém správne prispôsobíte, užívatelia budú na prihlasovacej obrazovke zadávať už len svoje užívateľské ID a heslá. Ich užívateľské profily poskytujú ďalšie prihlasovacie hodnoty.

Heslo

Heslo pre skupinový profil nastavte na *NONE. Tým sa zabráni, aby sa ktokoľvek prihlasoval pomocou skupinového profilu. Neskôr, keď kopírujete skupinový profil na vytvorenie individuálnych užívateľských profilov, nastavte heslo pre každého užívateľa.

Úvodný program a úvodná procedúra

Úvodný program užívateľa, nazývaný aj **prihlasovací program**, beží predtým, než systém zobrazí prvú ponuku. Názov tohto programu a jeho knižnice uveďte v skupinovom profile, aj keď je táto knižnica súčasťou úvodného zoznamu knižníc. Uvedením oboch týchto hodnôt zabezpečíte, že systém spustí správny program a vy sa nemusíte starať o zmeny v zozname knižníc.

Úvodný program alebo procedúra sa používa z jedného z týchto dôvodov:

- Niektoré aplikácie používajú úvodný program na nastavenie prostredia aplikácie.
- Chcete, aby užívateľ používal len jeden program a nikdy nevidel ponuku. Napríklad v spoločnosti JKL Toy Company užívatelia, ktorí používajú pracovnú stanicu na nakladacej rampe, môžu používať len program na prijímanie tovaru. Zabraňuje to ohrozeniu bezpečnosti pracovnej stanice, umiestnenej na verejnom mieste.

Nastavenie poľa **Obmedziť schopnosti** pre užívateľa na hodnotu *YES alebo *PARTIAL zabraňuje užívateľovi meniť úvodný program na prihlasovacej obrazovke.

Poraďte sa s vaším programátorom, či vaše aplikácie vyžadujú úvodný program alebo procedúru.

Úvodná ponuka a knižnica úvodných ponúk

Úvodná ponuka, nazývaná aj **prvá ponuka**, je prvá ponuka, ktorá sa užívateľovi zobrazí po prihlásení. Predtým, než sa objaví úvodná ponuka, beží úvodný program. Ak úvodný program ukáže akékoľvek obrazovky, užívateľ uvidí tieto obrazovky predtým, než systém ukáže úvodnú ponuku.

Bežne by úvodná ponuka pre skupinu mala byť primárnou ponukou hlavnej aplikácie tejto skupiny. Uveďte názov ponuky a jej knižnice.

Ak pole **Obmedziť schopnosti** nastavíte pre užívateľa na hodnotu *YES, tento užívateľ nemá povolené meniť úvodnú ponuku na prihlasovacej obrazovke. Ak pole *Obmedziť schopnosti* nastavíte pre užívateľa na hodnotu *PARTIAL, tomuto užívateľovi povolíte meniť úvodnú ponuku na prihlasovacej obrazovke.

Aktuálna knižnica

Aktuálnej knižnici sa hovorí aj **štandardná knižnica**. Ak špecifikujete pre užívateľa aktuálnu knižnicu, stane sa všeličo:

- Ak užívateľ vytvára akékoľvek objekty, napríklad dotazovacie programy, systém umiestni tieto objekty do aktuálnej knižnice, pokiaľ užívateľ neurčí inú knižnicu.
- Systém automaticky pridáva aktuálnu knižnicu do užívateľskej časti zoznamu knižníc. Možno ju zahrnúť do úvodného zoznamu knižníc v opise úlohy, ale nie je to nutné.
- Aktuálna knižnica sa stane prvou knižnicou v užívateľskej časti zoznamu knižníc. Systém vyhľadáva v aktuálnej knižnici súbory a programy pred prehľadaním knižníc v zozname knižníc užívateľa.
- Ak nevyhradíte pre užívateľa aktuálnu knižnicu, systém priradí knižnicu QGPL (všeobecný účel).

Odporúčania

Aktuálne knižnica je obzvlášť dôležitá, keď plánujete používať licenčný program IBM Query for iSeries alebo iný podobný program. Použite jeden z týchto prístupov:

- Vytvorte knižnicu, ktorú bude zdieľať každý zo skupiny. Do tejto knižnice uložte všetky dotazovacie programy a súbory pre túto skupinu. Dajte jej rovnaký názov ako má skupinový profil a urobte z nej aktuálnu knižnicu pre túto skupinu.
- Každému užívateľovi, ktorý plánuje používať program Query, dajte osobnú knižnicu. Tejto knižnici dajte rovnaký názov ako má užívateľský profil. Túto knižnicu špecifikujte ako aktuálnu knižnicu v individuálnych profiloch členov skupiny, nie v skupinovom profile.

V Časti 2 formulára Opis užívateľa vyplňte vaše voľby pre polia, ovplyvňujúce prihlásenie.

Po vybratí hodnôt, ovplyvňujúcich prihlásenie, môžete vybrať hodnoty, ktoré obmedzujú, čo smie užívateľ robiť.

Výber hodnôt, obmedzujúcich, čo smie užívateľ robiť

Po zadaní vašich volieb pre hodnoty, ovplyvňujúce prihlásenie, do Časti 2 formulára Opis skupiny užívateľov by ste mali zvážiť, že obmedzíte, čo smie užívateľ v systéme robiť. Pravdepodobne budete chcieť obmedziť, čo smú užívatelia robiť, z niekoľkých dôvodov:

- Užívateľom chcete zabrániť v používaní príkazov CL. Mohlo by ich to zvádzať na experimentovanie a neúmyselne by mohli všeličo poškodiť.
- Užívateľov chcete obmedziť na konkrétne aplikácie a funkcie.
- Užívateľom treba poskytnúť jednoduché prostredie, kde ich nebudú mýliť nepotrebné voľby.

Čo všetko môžu vaši užívatelia robiť, určujú mnohé faktory:

- Návrh aplikácie
- Systémové hodnoty
- Zabezpečenie prostriedkov
- Skupinové profily
- Užívateľské profily
- Opisy úloh

Dve polia v skupinovom alebo užívateľskom profile, **Obmedziť schopnosti** a **Trieda užívateľa**, určujú, nakoľko smie užívateľ prekročiť vaše rozhodnutia.

Obmedziť schopnosti

Pole **Obmedziť schopnosti** sa nazýva **Obmedzené používanie príkazového riadka**. Môžete obmedziť, či smú užívatelia meniť hodnoty na prihlasovacej obrazovke, zadávať príkazy a meniť svoj program, obsluhujúci kláves Attention. Môžete zvoliť prísne obmedzenia (*YES), priemerné obmedzenia (*PARTIAL) alebo žiadne obmedzenia (*NO). Nasledujúca tabuľka zobrazuje, čo každá z týchto hodnôt povoľuje:

Tabuľka 23. Funkcie, povolené pre hodnoty obmedzenia schopností

Hodnota obmedzenia schopností	Meniť úvodný program	Meniť úvodnú ponuku	Meniť aktuálnu knižnicu	Meniť program upozornenia	Zadávať príkazy
*YES	Nie	Nie	Nie	Nie	Niektoré[1]
*PARTIAL	Nie	Áno	Nie	Nie	Áno
*NO	Áno	Áno	Áno	Áno	Áno

1 Povolené sú tieto príkazy: SIGNOFF, SNDMSG, DSPMSG, DSPJOB, DSPJOBLOG a STRPCO. Užívateľ nemôže používať kláves F9 na zobrazenie príkazového riadka zo žiadnej ponuky alebo obrazovky Operačného asistenta.

Trieda užívateľa

Trieda užívateľa, nazývaná aj **typ užívateľa**, určuje, ktoré voľby uvidí užívateľ v ponukách Operačného asistenta a systému. Určuje tiež, ktoré systémové funkcie smie užívateľ vykonávať, pokiaľ neuvediete oprávnenia v poli **Zvláštne oprávnenie**.

Odporúčania pre obmedzené schopnosti a triedu užívateľa

Väčšina užívateľov nepotrebuje alebo nechce prístup k príkazom CL alebo k systémovým funkciám. Obrazovky Operačného asistenta poskytujú užívateľom dostatok informácií o ich vlastnej práci a kontrolu nad ňou. Tieto odporúčania umožňujú užívateľom prístup len k tým systémovým prostriedkom, ktoré potrebujú na vykonávanie svojich úloh:

- V každom skupinovom profile nastavte pole **Obmedziť schopnosti** na hodnotu *YES. Pole *Trieda užívateľa* nastavte na hodnotu *USER.
- Tieto špecifikácie vynechajte v prípade jednotlivých užívateľov, ktorí potrebujú systémové funkcie.
- Skontrolujte, či vaše ponuky umožňujú užívateľom v prípade potreby pohybovať sa medzi aplikáciami.

Po zadaní vašich volieb pre triedu užívateľa a obmedzenie schopností do Časti 2 formulára Opis skupiny užívateľov môžete vybrať hodnoty, nastavujúce prostredie užívateľa.

Výber hodnôt, nastavujúcich prostredie užívateľa

Po zadaní vašich volieb pre obmedzenie, čo smú vaši užívatelia v systéme robiť, do Časti 2 formulára Opis skupiny užívateľov môžete vybrať hodnoty na určenie operačného prostredia užívateľa. Mnohé polia v užívateľskom profile určujú operačné prostredie užívateľa: akú tlačiareň treba používať, kam treba posielať správy, s akou prioritou majú bežať úlohy. Pre mnohé z týchto polí sa odporúča štandardné nastavenie. V nasledujúcich odsekoch je opísaných niekoľko polí.

- **Opis úlohy a knižnica opisov úlohy**: Tieto polia v profile hovoria systému, ktorý opis úlohy treba použiť, keď sa užívateľ prihlási. Opis úlohy obsahuje úvodný zoznam knižníc. Každá skupina užívateľov by mala mať opis úlohy s rovnakým názvom ako má skupinový profil. Opisy úloh sa zvyčajne ukladajú do knižnice QGPL.
- **Tlačové zariadenie a výstupný front**: Každý tlačový výstup, vytvorený užívateľom, ide na tlačové zariadenie, uvedené v profile, pokiaľ ho konkrétna tlačová úloha nepošle na inú tlačiareň. Členovia skupiny užívateľov sú zvyčajne umiestnení spolu a zdieľajú rovnakú tlačiareň. Túto tlačiareň môžete špecifikovať v skupinovom profile a skopírovať ju do každého individuálneho užívateľského profilu. Tlačovému zariadeniu užívateľa sa hovorí aj **štandardná tlačiareň**.

  Než sa tlačový výstup vytlačí, nachádza sa vo výstupnom fronte. Každé tlačové zariadenie má zvyčajne svoj vlastný výstupný front s rovnakým názvom. Pre tento výstupný front môžete špecifikovať hodnotu *DEV, aby ste systému oznámili, že má použiť výstupný front tohto tlačového zariadenia.

  Vo formulári Opis skupiny užívateľov vyplňte polia názvu opisu úlohy a jeho knižnice a polia štandardnej tlačiarne a výstupného frontu.
- **Nastavenie prostredia Operačného asistenta**: Pri dodaní vášho systému je ponuka Operačného asistenta pre každého užívateľa programom, obsluhujúcim kláves Attention. Stlačením klávesu Attention uvidia užívatelia ponuku Operačného asistenta (ASSIST). Ak vaše aplikačné programy už používajú iný program, obsluhujúci kláves Attention, mali by ste vašim užívateľom poskytnúť inú metódu, pomocou ktorej sa dostanú k ponuke Operačného asistenta:
  - Ponuku Operačného asistenta pridajte ako voľbu z vašich hlavných ponúk aplikácií pomocou príkazu GO ASSIST alebo CALL QEZAST.
  - Nechajte užívateľov zadať príkaz GO ASSIST z príkazového riadka.

Ak je pole **Obmedziť schopnosti** nastavené v užívateľskom profile na hodnotu *YES, užívateľ nemôže na zobrazenie ponuky použiť príkaz GO. Užívateľom Operačného asistenta musíte poskytnúť metódu, ktorou pristúpia k ponuke ASSIST.

Pravdepodobne si budete chcieť pozrieť príklad, ktoré hodnoty vybrala Sharon Jones pre formulár Opis skupiny užívateľov v prípade spoločnosti JKL Toy Company.

Na vykonanie týchto krokov plánovania by ste mali:

- Pre každú skupinu užívateľov vo vašej spoločnosti vyplniť formulár Opis skupiny užívateľov .
- Vo formulári Názvové konvencie opísať, ako pomenovávate vaše skupiny užívateľov.
- Do vášho diagramu aplikácií a knižníc pridať skupiny užívateľov.

Po vykonaní týchto úloh môžete začať plánovať individuálne užívateľské profily.

Príklad: Formulár opisu skupiny užívateľov spoločnosti JKL Toy—2. časť: Sharon Jones si urobila niekoľko poznámok o oddeleniach odbytu a marketingu a skladu, keď pripravovala formulár opisu skupiny užívateľov pre pracovníkov odbytu a marketingu.

- Personál odbytu a marketingu bude vo veľkej miere používať IBM Query for iSeries. Každý užívateľ by mal mať súkromnú knižnicu. Sklad môže mať jednu skupinovú knižnicu.
- Ľudia zo skladu, ktorí pracujú na príjmovom termináli, budú potrebovať úvodný program namiesto úvodnej ponuky.

Sharon pripravila 2. časť formulára opisu skupiny užívateľov pre dve oddelenia.

Tabuľka 24. Formulár opisu skupiny užívateľov spoločnosti JKL Toy: Príklad oddelenia odbytu a marketingu

Názov poľa	**Odporúčaná hodnota**	**Vaša voľba**
Názov skupinového profilu (Užívateľ)		DSTSM
Heslo	*NONE	*NONE
Užívateľská trieda (Typ užívateľa)	*USER	*USER
Aktuálna knižnica (Štandardná knižnica)	*rovnaké ako názov skupinového profilu*	(ponechať prázdne v skupine; vyplniť pre jednotlivé profily)
Úvodný volaný program (Prihlasovací program)		
Knižnica úvodného programu		
Úvodná ponuka (Prvá ponuka)		CPMAIN
Knižnica úvodnej ponuky		CPMAINLIB
Obmedziť schopnosti (Obmedziť používanie príkazového riadka)	*YES	*PARTIAL
Text (Užívateľský opis)		Odbyt a marketing
Opis úlohy	*rovnaké ako názov skupinového profilu*	DPTSM
Knižnica opisu úlohy		QGPL
Názov skupinového profilu (Skupina užívateľov)	*NONE[1]	*NONE
Tlačové zariadenie (štandardná tlačiareň)		PRT03
Výstupný front	*DEV	*DEV

Tabuľka 25. Formulár opisu skupiny užívateľov spoločnosti JKL Toy: Príklad skladového oddelenia

Názov poľa	**Odporúčaná hodnota**	**Vaša voľba**
Názov skupinového profilu (Užívateľ)		DPTWH
Heslo	*NONE	*NONE
Užívateľská trieda (Typ užívateľa)	*USER	*USER
Špeciálne prostredie		
Aktuálna knižnica (Štandardná knižnica)	*rovnaké ako názov skupinového profilu*	DPTWH
Úvodný volaný program (Prihlasovací program)		

Tabuľka 25. Formulár opisu skupiny užívateľov spoločnosti JKL Toy: Príklad skladového oddelenia (pokračovanie)

Názov poľa	Odporúčaná hodnota	Vaša voľba
Knižnica úvodného programu		
Úvodná ponuka (Prvá ponuka)		ICMAIN
Knižnica úvodnej ponuky		ICPGMLIB
Obmedziť schopnosti (Obmedziť používanie príkazového riadka)	*YES	*YES
Text (Užívateľský opis)		Skladové oddelenie
Opis úlohy	*rovnaké ako názov skupinového profilu*	DPTWH
Knižnica opisu úlohy		QGPL
Názov skupinového profilu (Skupina užívateľov)	*NONE[1]	*NONE
Tlačové zariadenie (štandardná tlačiareň)		PRT04
Výstupný front	*DEV	*DEV
1 Názov skupinového profilu musí byť *NONE pre skupinový profil. Skupinový profil nemôže byť členom ďalšej skupiny.		

Teraz môžete začať s plánovaním jednotlivých užívateľských profilov.

Plánovanie individuálnych užívateľských profilov

Keď už ste rozhodli o vašej celkovej bezpečnostnej stratégii a naplánovali ste skupiny užívateľov, môžete začať plánovať individuálne užívateľské profily.

Aké formuláre potrebujte ?

Na plánovanie individuálnych užívateľských profilov použite tieto formuláre:

- Formulár Individuálny užívateľský profil
- Formulár Systémové zodpovednosti

Budete musieť použiť aj informácie v týchto vyplnených formulároch:

- Formulár Definícia skupiny užívateľov
- Formulár Názvové konvencie
- Graf vašich aplikácií

Pomenovávanie skupinových profilov

Názov vášho užívateľského profilu znamená to, ako vás systém identifikuje. Názov vášho užívateľského profilu zadajte v poli **User ID** na prihlasovacej obrazovke. Všetky úlohy, ktoré vykonávate a tlačový výstup, ktorý vytvárate, sa priraďujú k názvu vášho užívateľského profilu.

Pri rozhodovaní, ako pomenujete užívateľské profily, berte do úvahy nasledovné:

- Názov užívateľského profilu sa môže skladať z najviac 10 znakov. Niektoré metódy komunikácie obmedzujú dĺžku užívateľského ID na 8 znakov.
- Názov užívateľského profilu môže obsahovať písmená, číslice a zvláštne znaky: znak mriežky (#), dolára ($), podčiarkovníka (_) a zavináča (@). Nesmie začínať číslicou alebo podčiarkovníkom (_).
- V názve užívateľského profilu systém nerozlišuje medzi veľkými a malými písmenami. Ak zadáte malé abecedné znaky, systém ich preloží do veľkých znakov.

- Obrazovky a zoznamy, ktoré používate na manažovanie užívateľských profilov, zobrazujú tieto užívateľské profily v abecednom poradí podľa názvu užívateľského profilu.
- Všetky profily, dodané spoločnosťou IBM, začínajú písmenom Q. Ak chcete vaše profily držať oddelene od profilov, dodaných spoločnosťou IBM, neprirađujte názvy užívateľských profilov, ktoré začínajú písmenom Q.

Odporúčania

Jednou z techník priraďovania názvov užívateľských profilov je použitie prvých 7 znakov priezviska, za ktorými nasleduje prvý znak krstného mena. Sharon použila pre užívateľské profily v spoločnosti JKL Toy Company nižšie uvedené názvové konvencie:

Tabuľka 26. Formulár Názvové konvencie, ktorý používa spoločnosť JKL Toy Company: Príklad užívateľských profilov

Meno užívateľa	Názov užívateľského profilu
Anderson, George	ANDERSOG
Anderson, Roger	ANDERSOR
Jones, Sharon	JONESS

Pomocou tejto metódy sú názvy užívateľských profilov ľahko zapamätateľné. Aj vaše zoznamy a obrazovky sú abecedne zotriedené podľa priezviska.

Napríklad Sharon Jones zo spoločnosti JKL Toy Company plánuje používať túto techniku pomenovávania. Vo formulári Názvové konvencie vyplnila príslušnú časť.

Tabuľka 27. Formulár Názvové konvencie, ktorý používa spoločnosť JKL Toy Company: Príklad užívateľských profilov

Typ objektu	Názvová konvencia
Užívateľské profily	Použite prvých 7 znakov priezviska užívateľa, za ktorými bude nasledovať prvý znak jeho krstného mena. Opisy užívateľského profilu budú: priezvisko, krstné meno.

Vo formulári Názvové konvencie opíšte, ako plánujete pomenovať užívateľské profily, potom môžete určiť, kto má byť zodpovedný za systémové funkcie a vybrať hodnoty pre každého užívateľa.

Stanovenie osoby, ktorá bude zodpovedná za systémové funkcie

Keď plánujete individuálne užívateľské profily, musíte najprv stanoviť zodpovednosti jednotlivcov v systéme. Ak chcete váš systém udržiavať v efektívnej prevádzke, potrebujete užívateľov na pravidelné vykonávanie rôznych funkcií manažovania a údržby. Ľudia, ktorí vykonávajú tieto úlohy, potrebujú oprávnenie na spúšťanie príkazov a vykonávanie systémových funkcií.

V téme Výber hodnôt, obmedzujúcich, čo smie užívateľ robiť sa hovorilo o tom, ako polia **Trieda užívateľa** a **Obmedziť schopnosti** riadia systémové funkcie, do ktorých má užívateľ prístup. Bežne by ste väčšine užívateľov nemali povoliť vykonávať systémové funkcie (triedu užívateľa nastavte na hodnotu *USER a obmedzenie schopností na hodnotu *PARTIAL alebo *YES). Niektorí užívatelia však potrebujú ďalšie oprávnenie, aby mohli udržiavať váš systém v efektívnej prevádzke.

Nižšie uvedená tabuľka uvádza niektoré dôležité úlohy manažovania systému. Určuje aj triedu užívateľa a zvláštne oprávnenia, ktoré môžete priradiť užívateľom s týmito úlohami. Tento zoznam vám pomôže určiť, ktorí užívatelia vo vašom systéme potrebujú zvláštne oprávnenia. Nie je však určený ako kompletný nástroj plánovania pre prevádzku a údržbu vášho systému. Táto tabuľka uvádza triedu užívateľa a zvláštne oprávnenia, ktoré fungujú s väčšinou systémov. Pravdepodobne budete musieť priradiť iné oprávnenia v závislosti od vášho systému.

Keď priradíte triedu užívateľa inú ako hodnota *USER v profile, užívateľ automaticky dostane na vykonávanie systémových funkcií určitú skupinu zvláštnych oprávnení. Užívateľovi môžete priradiť zvláštne oprávnenia, ktoré sa odlišujú od oprávnení, ktoré špecifikujete v poli triedy užívateľa, ale pravdepodobne to nebude potrebné.

Tabuľka 28. Systémová zodpovednosť, Trieda užívateľa a Zvláštne oprávnenie

Systémová funkcia[1]	Opis	Požadovaná trieda užívateľa[2]	Požadované zvláštne oprávnenie[3]
Systémové operácie	Manažovať tlačový výstup, odpovedať na systémové správy, monitorovať pravidelné operácie, vykonávať IPL (initial program load - úvodné zavedenie programu).	*SYSOPR	*JOBCTL
Údržba systému	Vykonávať funkcie údržby systému, akými sú vytváranie rozvrhu automatického čistenia a monitorovanie používania disku.	*SYSOPR	*JOBCTL
Zálohovanie systému	Pravidelne ukladať knižnice aplikácií, systémové knižnice a bezpečnostné informácie. Podrobné informácie o týchto funkciách nájdete v téme Zálohovanie a obnova v Informačnom centre.	*SYSOPR	*SAVSYS
Správa profilov	Pridávať nové užívateľské profily, udržiavať existujúce profily.	*SECADM	*SECADM
Správa zabezpečenia prostriedkov	Udržiavať oprávnenia na objekty v systéme.	*SECOFR	*ALLOBJ
Údržba programov	V knižniciach, dodaných spoločnosťou IBM, používať pravidelné zmeny programov (PTF). Vykonáva zmeny vo vašich knižniciach aplikácií.	*SECOFR	*ALLOBJ
Bezpečnostný audit	Nastaviť funkciu bezpečnostného auditu. Určiť, ktoré udalosti, užívatelia a objekty sa majú auditovať.		*AUDIT [4]
Konfigurácia systému	Pridávať, meniť a odstraňovať zariadenia z vášho systému.		*IOSYSCFG[5]

1 Pre užívateľov s týmito úlohami nastavte pole Obmedziť schopnosti na hodnotu *NO.

2 Je to minimálna požadovaná trieda užívateľa. Trieda užívateľa poskytuje oprávnenie na používanie príkazov a ponukových volieb, potrebných na vykonávanie funkcie. V závislosti od bezpečnosti vášho prostriedku sa môže vyžadovať aj ďalšie oprávnenie na objekt.

3 Toto mimoriadne zvláštne oprávnenie sa vyžaduje pre zodpovednosti za úlohy. Trieda užívateľa môže udeliť ďalšie zvláštne oprávnenia.

4 Zvláštne oprávnenie *AUDIT nemá zodpovedajúcu triedu užívateľa. Trieda užívateľa *SECOFR zahrňuje zvláštne oprávnenie *AUDIT. Váš auditor však pravdepodobne nepotrebuje ďalšie schopnosti triedy užívateľa *SECOFR. Pre každého individuálneho užívateľa, ktorý potrebuje riadiť auditovanie vo vašom systéme, by ste mali špecifikovať zvláštne oprávnenie *AUDIT.

5 Zvláštne oprávnenie *IOSYSCFG nemá zodpovedajúcu triedu užívateľa. Trieda užívateľa *SECOFR zahrňuje zvláštne oprávnenie *IOSYSCFG. Zvláštne oprávnenie *IOSYSCFG by ste mali špecifikovať len pre jednotlivcov, ktorí potrebujú nakonfigurovať váš systém. Títo jednotlivci môžu vytvárať linky, radiče a zariadenia alebo konfigurovať TCP/IP. Užívateľ, ktorý konfiguruje váš systém, však pravdepodobne nepotrebuje ďalšie schopnosti triedy užívateľa *SECOFR.

Odporúčania

Na plánovanie osôb, ktoré majú vykonávať systémové funkcie, použite vyššie uvedenú tabuľku. Na manažovanie bezpečnosti systému by ste mali vyhradiť minimálne dvoch užívateľov a na manažovanie operácií a zálohovania dvoch ďalších.

Ako nástroj pre manažovanie a auditovanie vášho systému použite formulár Systémové zodpovednosti. Sledujte každého, kto má zvláštne oprávnenie vo vašom systéme a načo ho potrebuje.

Než vyberiete hodnoty pre jednotlivých užívateľov, pravdepodobne si budete chcieť pozrieť príklad, ako Sharon Jones určila zodpovednosť užívateľov.

Príklad: Formulár systémovej zodpovednosti spoločnosti JKL Toy: Nasleduje príklad formulára systémovej zodpovednosti, ktorý vyplnila Sharon Jones:

Tabuľka 29. Formulár systémovej zodpovednosti spoločnosti JKL Toy: príklad

Kto je váš primárny správca bezpečnosti? Sharon Jones Kto je váš záložný správca bezpečnosti?Ken Harrison			
Názov profilu	Meno užívateľa	Trieda	Poznámky
JONESS	Sharon Jones	*SECOFR	Sharon je primárnym správcom bezpečnosti a správcom systému.
HARRISOK	Ken Harrison	*SECOFR	Ken je záloha Sharon vo funkcii celkového správcu systému.
JOHNSONS	Sandy Johnson	*SYSOPR	Sandy má primárnu zodpovednosť za systémové operácie a zálohovanie.
ROGERSK	Karen Rogers	*SYSOPR	Karen bude pomáhať Sandy s operáciami a zálohovaním.
WILLISR	Rose Willis	*SYSOPR	Rose bude obsluhovať systém počas druhej smeny.

Po vyplnení formulára systémovej zodpovednosti môžete začať vyberať hodnoty pre každého užívateľa.

Výber hodnôt pre jednotlivých užívateľov

Po určení zodpovedností užívateľov vo vašom systéme môžete pre jednotlivých užívateľov začať vyberať hodnoty. Najviac práce ste urobili pri plánovaní skupinových profilov ako vzorov pre individuálne užívateľské profily. Pomocou formulára Individuálny užívateľský profil zaraďte každého užívateľa do správnej skupiny a zadefinujte, čím sa tento užívateľ odlišuje od ostatných v skupine. Ako príklad by ste mali pre jednu skupinu užívateľov vyplniť formulár Individuálny užívateľský profil, potom sa vrátiť a formuláre Individuálny užívateľský profil vypracovať pre všetky ďalšie skupiny užívateľov.

V hornej časti formulára Individuálny užívateľský profil vyplňte názov skupinového profilu a ďalšie opisné informácie.

Príklad: Opisné informácie formulára Individuálny užívateľský profil, ktorý používa spoločnosť JKL Toy Company

Pozrite sa, ako Sharon Jones vyplnila hornú časť formulára Individuálny užívateľský profil.

Tabuľka 30. Formulár Individuálny užívateľský profil, ktorý používa spoločnosť JKL Toy Company: Príklad opisných informácií

Formulár Individuálny užívateľský profil		
Vypracovala: Sharon Jones		Dátum: 9/5/99
Názvy skupinových profilov: DPTOP		
Vlastníci vytvorených objektov:	Skupinové oprávnenie na vytvorené objekty:	
Typ skupinového oprávnenia:		

Určenie hodnôt pre členov skupiny

Vo vašom formulári Individuálny užívateľský profil napíšte názov profilu a opis (meno užívateľa) každého člena skupiny. V nižšie uvedených odsekoch sa uvádza, ako sa určujú ďalšie hodnoty pre každého člena skupiny.

Nezabudnite, že skupinový profil je vzor pre individuálne užívateľské profily. Vo formulári Individuálny užívateľský profil musíte špecifikovať len to, čo sa odlišuje od skupiny.

- **Priradenie hesiel**: Najjednoduchším spôsobom priradenia úvodných hesiel užívateľom je vytvoriť rovnaké heslo ako je názov profilu. Potom môžete vyžadovať, aby sa heslo zmenilo pri prvom prihlásení užívateľa tým, že tomuto heslu nastavíte ukončenie platnosti. V téme Nastavenie ukončenia platnosti hesla sa dozviete, ako to urobiť automaticky, keď kopírujete skupinový profil. Ak to zamýšľate urobiť, nemusíte heslá uvádzať do formulára Individuálny užívateľský profil.
- **Trieda užívateľa a obmedzenie schopností**: Vo vašom formulári Systémové zodpovednosti si pozrite, ktorí členovia každej skupiny potrebujú inú hodnotu pre polia **Trieda užívateľa** a **Obmedziť schopnosti**. Vo formulári Individuálny užívateľský profil vyplňte príslušné informácie pre každého, kto potrebuje iné hodnoty ako skupinový profil.
- **Špecifikovanie ďalších hodnôt**: Skontrolujte, či konkrétny užívateľ potrebuje hodnoty, ktoré sa odlišujú od hodnôt, špecifikovaných pre skupinu vo formulári Opis skupiny užívateľov. Vo formulári Opis skupiny užívateľov sú polia **Trieda užívateľa** a **Obmedziť schopnosti** uvedené v hornej časti, pretože ich hodnoty sa môžu pre niektorých členov skupiny často odlišovať. Uveďte všetky ďalšie polia, ktoré sa odlišujú pre členov skupiny, s ktorými pracujete.

Na dokončenie tohto kroku plánovania musíte:
- Vyplniť váš formulár Výber systémových hodnôt.
- Vo vašom formulári Názvové konvencie opísať, ako plánujete pomenovať užívateľské profily .
- Vypracovať formulár Individuálny užívateľský profil pre každú skupinu užívateľov vo vašej spoločnosti.

Než naplánujete zabezpečenie prostriedkov, pravdepodobne si budete chcieť pozrieť príklad informácií, ktoré Sharon použila v prípade jednotlivých užívateľov.

Príklad: Formulár jednotlivého užívateľského profilu spoločnosti JKL Toy: Ľudia, ktorí v spoločnosti JKL pracujú na nakladacej rampe, môžu spúšťať len jeden program. Sharon obmedzila týchto užívateľov na malý počet funkcií, pretože pracujú v priestore, kde má verejnosť ľahký prístup k ich pracovným staniciam. Členovia skladového oddelenia majú úvodný program a nemajú žiadnu úvodnú ponuku. Oddelenie spracovania objednávok má dve lokálne tlačiarne a jednu tlačiareň vo vzdialenej predajnej kancelárii. Preto Sharon priradila niektorým užívateľom inú tlačiareň než skupine.

Nižšie je formulár jednotlivého užívateľského profilu, ktorý Sharon Jones vyplnila pre oddelenie skladu a spracovania objednávok v spoločnosti JKL Toy. Všimnite si, že polia vyplnila len ak boli odlišné od hodnôt v skupinovom profile.

Tabuľka 31. Formulár jednotlivého užívateľského profilu spoločnosti JKL Toy: príklad skladového oddelenia

Názvy skupinových profilov: DPTWH					
Vytvorte položku pre každého člena skupiny:					
Užívateľský profil	**Text (opis)**	**Užívateľská trieda**	**Obmedziť schopnosť**	**Úvodný program/ knižnica**	**Úvodná ponuka/ knižnica**
WILLISR	Willis, Rose	*SYSOPR	*NO		
WAGNERR	Wagner, Ray			ICRCPT/ICPGMLIB	žiadne
AMESJ	Ames, Janice			ICRCPT/ICPGMLIB	žiadne
FOSSJ	Foss, Julie				
WOODBURC	Woodburt, Carol				

Tabuľka 32. Formulár jednotlivého užívateľského profilu: Príklad oddelenia spracovania objednávok

Názvy skupinových profilov: DPTOP				
Vytvorte položku pre každého člena skupiny:				
Užívateľský profil	**Text (opis)**	**Užívateľská trieda**	**Obmedziť schopnosť**	**Tlačové zariadenie**
HARRISOK	Harrison, Ken	*SECOFR	*NO	PRT05
RICHARDK	Richards, Karen			
UNGERJ	Unger, Jeff			PRT04

Tabuľka 32. Formulár jednotlivého užívateľského profilu: Príklad oddelenia spracovania objednávok (pokračovanie)

BELLB	Bell, Brad			PRT04

Ďalej môžete začať plánovať zabezpečenie prostriedkov.

Plánovanie zabezpečenia prostriedkov

Keď už ste dokončili proces plánovania užívateľov vo vašom systéme, môžete naplánovať zabezpečenie prostriedkov, ktoré chráni objekty v tomto systéme. V téme Nastavenie zabezpečenia″ sa dozviete, ako máte nastaviť zabezpečenie prostriedkov vo vašom systéme.

Systémové hodnoty a užívateľské profily určujú, kto má prístup do vášho systému a bránia prihlasovaniu neoprávnených užívateľov. Zabezpečenie prostriedkov riadi akcie, ktoré môžu oprávnení užívatelia systému vykonávať po svojom úspešnom prihlásení. Zabezpečenie prostriedkov podporuje ochranu hlavných cieľov bezpečnosti vo vašom systéme:

- Dôvernosť informácií
- Presnosť informácií, aby sa predišlo neautorizovaným zmenám
- Dostupnosť informácií, aby sa predišlo náhodnému alebo úmyselnému poškodeniu

Zabezpečenie prostriedkov môžete naplánovať rôznym spôsobom, v závislosti od toho, či vaša spoločnosť vyvíja aplikácie alebo či ich kupuje. V prípade aplikácií, ktoré vyvíjate, by ste mali počas procesu navrhovania aplikácií programátorovi odovzdať požiadavky na bezpečnosť informácií. Ak aplikácie kupujete, musíte stanoviť vaše požiadavky na bezpečnosť a zosúladiť ich so spôsobom, akým váš poskytovateľ vaše aplikácie navrhol. Techniky, ktoré sú tu opísané, by vám mali pomôcť v oboch prípadoch.

Táto téma poskytuje základný prístup k plánovaniu zabezpečenia prostriedkov. Zoznamuje vás s hlavnými technikami a ukazuje, ako ich môžete používať. Metódy, ktoré sú tu opísané, nemusia fungovať pre každú spoločnosť a každú aplikáciu. Keď plánujete zabezpečenie prostriedkov, konzultujte s vaším programátorom alebo poskytovateľom aplikácií.

Pri plánovaní zabezpečenia prostriedkov vám pomôžu tieto témy:

- Stanovenie cieľov pre zabezpečenie vašich prostriedkov
- Pochopenie typov oprávnení
- Plánovanie bezpečnosti pre knižnice aplikácií
- Určenie vlastníctva knižníc a objektov
- Zoskupovanie objektov
- Ochrana tlačového výstupu
- Ochrana pracovných staníc
- Súhrn odporúčaní pre zabezpečenie prostriedkov
- Plánovanie inštalácie vašich aplikácií

Aké formuláre potrebujte ?

Urobte si kópie nasledujúcich formulárov a vyplňte ich tak, ako sa dočítate v tejto téme. Prejdite celým procesom s jednou aplikáciou a tento proces potom zopakujte pre každú ďalšiu aplikáciu.

Tabuľka 33. Plánovacie formuláre, potrebné k plánovaniu zabezpečenia prostriedkov

Názov formulára	**Potrebný počet kópií**
Formulár Autorizačný zoznam	Niekoľko
Formulár Bezpečnosť tlačového výstupu a pracovných staníc	Jedna

Do nasledujúcich formulárov pridajte informácie, s ktorými ste predtým pracovali:

Tabuľka 34. Plánovacie formuláre, ktoré sa zmenia

Názov formulára	**Vypracovaný v**
Formulár Opis knižnice	Opísanie informácií o knižnici
Formulár Opis skupiny užívateľov	Plánovanie skupinových profilov

Pozrite si tieto formuláre, ktoré ste predtým vypracovali:

Tabuľka 35. Plánovacie formuláre, potrebné k vykonaniu zabezpečenia prostriedkov

Názov formulára	**Vypracovaný v:**
Formulár Opis knižnice	Nakreslenie diagramu aplikácií a Identifikovanie skupín užívateľov
Formulár Opis aplikácie	Opísanie informácií o aplikácii
Formulár Individuálny užívateľský profil	Výber hodnôt pre jednotlivých užívateľov
Formulár Identifikácia skupiny užívateľov	Identifikovanie skupín užívateľov
Formulár Systémové zodpovednosti	Stanovenie osoby, ktorá bude zodpovedná za systémové funkcie
Formulár Plánovanie fyzického zabezpečenia	Plánovanie fyzického zabezpečenia

Stanovenie cieľov pre zabezpečenie vašich prostriedkov

Aby ste mohli začať plánovať zabezpečenie prostriedkov, musíte najprv poznať vaše ciele. iSeries poskytuje flexibilnú implementáciu bezpečnosti prostriedkov. Veľmi dôležité prostriedky vám umožňuje chrániť presne takým spôsobom, ako sami chcete. Zabezpečenie prostriedkov však prináša pre vaše aplikácie aj ďalšiu réžiu. Napríklad, zakaždým keď aplikácia potrebuje nejaký objekt, systém musí skontrolovať oprávnenie užívateľa na tento objekt. Vašu požiadavku na dôvernosť musíte porovnať s nákladmi na výkon. Keď rozhodujete o zabezpečení prostriedkov, porovnajte význam zabezpečenia s nákladmi naň.

Ak chcete zabrániť zníženiu výkonnosti vašich aplikácií v dôsledku zabezpečenia prostriedkov, dodržujte nasledujúce pokyny.

- Vaša schéma zabezpečenia prostriedkov musí byť jednoduchá.
- Zabezpečte len tie objekty, ktoré zabezpečiť potrebujete.
- Zabezpečenie prostriedkov použite ako doplnok a nie ako náhradu ďalších nástrojov na ochranu informácií, akými sú:
  - Obmedzenie prístupu užívateľov ku konkrétnym ponukám a aplikáciám.
  - Zabránenie užívateľom zadávať príkazy (obmedzené schopnosti v užívateľských profiloch).

Plánovanie zabezpečenia prostriedkov začnite zadefinovaním vašich cieľov. Vaše ciele zabezpečenia môžete zadefinovať buď vo formulári Opis aplikácie alebo vo formulári Opis knižnice.

Formulár, ktorý použijete, závisí od organizácie vašich informácií v knižniciach.

Predtým, než si pozriete typy oprávnení, ktoré môžete použiť na zabezpečenie prostriedkov, si pravdepodobne budete chcieť pozrieť príklad cieľov zabezpečenia spoločnosti JKL Toy Company.

Príklad: Bezpečnostné ciele spoločnosti JKL Toy

Sharon Jones v spoločnosti JKL Toy použila formulár opisu knižnice na opis bezpečnostných požiadaviek pre knižnicu zákazníckych záznamov (CUSTLIB):

Tabuľka 36. Formulár opisu knižnice spoločnosti JKL Toy: Príklad bezpečnostných cieľov

Formulár opisu knižnice	1. časť z 2

Tabuľka 36. Formulár opisu knižnice spoločnosti JKL Toy: Príklad bezpečnostných cieľov (pokračovanie)

Definujte ciele zabezpečenia pre knižnicu, napríklad či sú určité informácie dôverné:	V súčasnosti má každý v spoločnosti povolené prezerať si zákaznícke informácie a zákaznícke objednávky. Kvôli ochrane presnosti informácií by sme mali obmedziť, komu bude povolené meniť ich.

Sharon použila formulár opisu aplikácií pre aplikáciu Kontrakty a tvorba cien na opis bezpečnostných cieľov pre celú aplikáciu.

Tabuľka 37. Formulár opisu aplikácií spoločnosti JKL Toy: Príklad bezpečnostných cieľov

Formulár opisu aplikácií	1. časť z 2
Definujte ciele zabezpečenia pre knižnicu, napríklad či sú určité informácie dôverné:	Informácie o kontraktoch a zvláštnych cenách sú dôverné. Iba málo užívateľov má oprávnenie pozerať si ich a meniť ich: • Personál odbytu a marketingu a všetci riadiaci pracovníci potrebujú vytvárať, meniť a analyzovať kontrakty. Potrebujú používať súbory aj programy. • Personál spracovania objednávok mení kontrakty a vidí ceny nepriamo pri vkladaní a odosielaní objednávok. Nemá povolené pozerať si kontrakty a ceny s výnimkou prípadov, keď vkladá alebo mení objednávku.

Zapíšte si bezpečnostné ciele pre vašu aplikáciu buď do formulára opisu aplikácií alebo do formulára opisu knižnice. Potom si môžete pozrieť typy oprávnení, ktoré môžete použiť pri plánovaní zabezpečenia prostriedkov.

Pochopenie typov oprávnení

Po stanovení cieľov pre zabezpečenie vašich prostriedkov a zaznamenaní vašich rozhodnutí do formulára Opis knižnice môžete začať plánovať typy oprávnení. Zabezpečenie prostriedkov definuje, ako majú užívatelia pristupovať k objektom v systéme.

Oprávnenie znamená spôsob, akým je osoba oprávnená používať objekt. Môžete mať napríklad oprávnenie prezerať alebo meniť informácie v systéme. Systém poskytuje niekoľko rozličných typov oprávnení. IBM zoskupuje tieto typy oprávnení do kategórií, nazývaných **systémom definované oprávnenia**, ktoré vyhovujú potrebám väčšiny užívateľov. Nižšie uvedená tabuľka uvádza tieto kategórie a ich použitie na zabezpečenie súborov a programov.

Poznámka: Pri plánovaní oprávnení si pozrite nižšie uvedené tabuľky.

Tabuľka 38. Systémom definované oprávnenia

Názov oprávnenia	Operácie, povolené pre súbory	Operácie, nepovolené pre súbory	Operácie, povolené pre programy	Operácie, nepovolené pre programy
*USE	Zobrazenie informácií v súbore.	Zmena alebo vymazanie všetkých informácií v súbore. Vymazanie súboru.	Spustenie programu.	Zmena alebo vymazanie programu.
*CHANGE	Zobrazenie, zmena a vymazanie záznamov v súbore.	Vymazanie alebo vyčistenie celého súboru.	Zmena opisu programu.	Zmena alebo vymazanie programu.
*ALL	Vytvorenie a vymazanie súboru. Pridanie, zmena a vymazanie záznamov v súbore. Oprávnenie ďalších osôb na používanie súboru.	Žiadne	Vytvorenie, zmena a vymazanie programu. Oprávnenie ďalších osôb na používanie programu.	Zmena vlastníka programu, ak program schváli oprávnenie.

Tabuľka 38. Systémom definované oprávnenia (pokračovanie)

Názov oprávnenia	Operácie, povolené pre súbory	Operácie, nepovolené pre súbory	Operácie, povolené pre programy	Operácie, nepovolené pre programy
*EXCLUDE[1]	Žiadne	Akýkoľvek prístup k súboru.	Žiadne	Akýkoľvek prístup k programu.
1 *EXCLUDE nahrádza všetky oprávnenia, ktoré udeľujete verejnosti alebo prostredníctvom skupinového profilu.				

Vysvetlenie, ako oprávnenie na objekt a oprávnenie na knižnicu pracujú spolu

Ak chcete navrhnúť jednoduché zabezpečenie prostriedkov, skúste naplánovať bezpečnosť pre všetky knižnice. K tomu potrebujete pochopiť, ako sa systémom definované oprávnenia používajú pre knižnice, čo ukazuje nižšie uvedená tabuľka:

Tabuľka 39. Systémom definované oprávnenia pre knižnice

Názov oprávnenia	Povolené operácie	Nepovolené operácie
*USE	• V prípade objektov v knižnici každá operácia, povolená oprávnením na konkrétny objekt. • V prípade knižníc zobrazenie opisných informácií.	• Pridanie nových objektov do knižnice. • Zmena opisu knižnice. • Vymazanie knižnice.
*CHANGE	• V prípade objektov v knižnici každá operácia, povolená oprávnením na konkrétny objekt. • Pridanie nových objektov do knižnice. • Zmena opisu knižnice.	• Vymazanie knižnice.
*ALL	• Všetko povolené so zmenou. • Vymazanie knižnice. • Oprávnenie ďalších osôb na knižnicu.	• Žiadne

Potrebujete tiež pochopiť, ako knižnica a oprávnenie na objekt pracujú spolu. Nižšie uvedená tabuľka uvádza príklady oprávnení, vyžadovaných pre objekt aj pre knižnicu:

Tabuľka 40. Ako oprávnenie na knižnicu a oprávnenie na objekt pracujú spolu

Typ objektu	Operácie	Potrebné oprávnenie na objekt	Potrebné oprávnenie na knižnicu
Súbor	Zmena údajov	*CHANGE	*USE
Súbor	Vymazanie súboru	*ALL	*USE
Súbor	Vytvorenie súboru	*ALL	*CHANGE
Program	Spustenie programu	*USE	*USE
Program	Zmena (opakované kompilovanie) programu	*ALL	*CHANGE
Program	Vymazanie programu	*ALL	*USE

Oprávnenie na adresár je podobné oprávneniu na knižnicu. Aby ste mohli pristúpiť k objektu, potrebujete oprávnenie na všetky adresáre v názve cesty k tomuto objektu.

Teraz môžete začať plánovať bezpečnosť pre knižnice aplikácií.

Plánovanie bezpečnosti pre knižnice aplikácií

Po stanovení cieľov pre zabezpečenie vašich prostriedkov môžete začať plánovať bezpečnosť pre knižnice aplikácií. Podľa procesu, ktorý je tu opísaný, vyberte jednu z vašich knižníc aplikácií, s ktorou chcete pracovať. Ak váš systém uchováva súbory a programy v osobitných knižniciach, vyberte knižnicu, ktorá obsahuje súbory. Keď túto tému skončíte, zopakujte uvedené kroky pre zvyšné knižnice aplikácií.

Prezrite si informácie, ktoré ste zozbierali o vašich aplikáciách a knižniciach:

- Formulár Opis aplikácie
- Formulár Opis knižnice
- Formulár Opis skupiny užívateľov pre všetky skupiny, ktoré potrebujú knižnicu
- Váš diagram aplikácií, knižníc a skupín užívateľov

Pouvažujte, ktoré skupiny potrebujú informácie v knižnici, načo ich potrebujú a čo s nimi potrebujú urobiť.

Zistenie obsahu knižnice

Knižnice aplikácií obsahujú dôležité súbory aplikácií. Môžu obsahovať aj iné objekty, z ktorých väčšina sú programovacie nástroje, zabezpečujúce správny chod aplikácie, akými sú:

- Pracovné súbory
- Dátové oblasti a fronty správ
- Programy
- Súbory správ
- Príkazy
- Výstupné fronty

Väčšina objektov, s výnimkou súborov a výstupných frontov, nepredstavuje ohrozenie bezpečnosti. Zvyčajne obsahujú malé množstvo údajov aplikácie, často vo formáte, ktorý je mimo programov ťažko zrozumiteľný. Príkazom Display Library si môžete vypísať názvy a opisy všetkých objektov v knižnici. Napríklad vypísanie obsahu knižnice CONTRACTS: DSPLIB LIB(CONTRACTS) OUTPUT(*PRINT)

Ďalej sa budete musieť rozhodnúť, aké verejné oprávnenie chcete mať pre knižnice aplikácií a knižnice programov.

Rozhodnutie o verejnom oprávnení na knižnice aplikácií

Na účely zabezpečenia prostriedkov **verejný** znamená ktokoľvek, komu dáte oprávnenie na prihlásenie do vášho systému. **Verejné oprávnenie** povoľuje užívateľovi prístup k objektu, ak nemáte iný, konkrétnejší prístup. Okrem rozhodnutia o verejnom oprávnení na objekty, ktoré sú už v knižnici, môžete špecifikovať verejné oprávnenie na všetky nové objekty, pridané neskôr do tejto knižnice. Použite na to parameter **CRTAUT (Create Authority)**. Verejné oprávnenie na objekty v knižnici a oprávnenie na vytvorenie knižnice pre nové objekty by malo byť spravidla rovnaké.

Systémová hodnota QCRTAUT (Create Authority) určuje celosystémové verejné oprávnenie na nové objekty. IBM dodáva systémovú hodnotu QCRTAUT nastavenú na *CHANGE. Systémovú hodnotu QCRTAUT nemeňte, pretože ju používajú mnohé systémové funkcie. Ak v parametri CRTAUT (Create Authority) knižnice aplikácií uvediete hodnotu *SYSVAL, použije systémovú hodnotu QCRTAUT (*CHANGE).

Z dôvodu jednoduchosti aj dobrého výkonu používajte verejné oprávnenie čo možno najviac. Ak chcete určiť, aké má byť verejné oprávnenie na knižnicu, položte si nasledujúce otázky:

- Majú mať všetci v spoločnosti prístup k väčšine informácií v tejto knižnici ?
- Aký druh prístupu by mali užívatelia mať k väčšine informácií v tejto knižnici ?

Sústreďte sa na rozhodnutia pre väčšinu užívateľov a väčšinu informácií. Neskôr sa dozviete, ako vyriešite výnimky. Plánovanie zabezpečenia prostriedkov je často zdĺhavý proces. Môžete zistiť, že po zvážení požiadaviek na konkrétne

objekty potrebujete vykonať zmeny vo verejnom oprávnení. Vyskúšajte niektoré kombinácie verejného a súkromného oprávnenia na objekty aj na knižnice predtým, než vyberiete oprávnenie, ktoré spĺňa vaše požiadavky na bezpečnosť a výkon.

Zabezpečenie primeraného oprávnenia

Oprávnenie *CHANGE na objekty a oprávnenie *USE na knižnice sú primerané pre väčšinu funkcií aplikácií. Vášmu programátorovi alebo poskytovateľovi aplikácií musíte však položiť niekoľko otázok, aby ste zistili, či určité funkcie aplikácií vyžadujú väčšie oprávnenie:

- Vymazávajú sa v knižnici počas spracovania nejaké súbory alebo iné objekty ? Čistia sa nejaké súbory ? Pridávajú sa do nejakých súborov členy ? Vymazanie objektu, vyčistenie súboru alebo pridanie člena súboru vyžaduje oprávnenie *ALL na tento objekt.
- Vytvárajú sa v knižnici počas spracovania nejaké súbory alebo iné objekty ? Vytvorenie objektu vyžaduje oprávnenie *CHANGE na túto knižnicu.

Než rozhodnete o verejnom oprávnení na knižnice programov, pravdepodobne si budete chcieť pozrieť príklad, ako sa Sharon rozhodla v prípade oprávnení na objekty.

Príklad: Formulár opisu knižnice spoločnosti JKL Toy:

Sharon Jones si pozrela bezpečnostné ciele pre knižnicu zákazníckych záznamov, ako aj informácie o aplikáciách a oddeleniach, ktoré používajú zákaznícke informácie. Urobila si poznámky o svojich záveroch:

- Každé oddelenie, s výnimkou skladového a výrobného oddelenia, potrebuje meniť zákaznícke informácie.
- Všetci užívatelia v skladovom a výrobnom oddelení majú užívateľské profily s položkou Obmedziť schopnosti (Áno) a majú obmedzené určité ponuky alebo programy. Ich ponuky im umožňujú prezerať si zákaznícke informácie, ale nie meniť ich.
- Verejné oprávnenie pre objekty v knižnici zákazníckych záznamov môže byť nastavené na *CHANGE. Obmedzenia ponúk zabraňujú neoprávneným užívateľom meniť zákaznícke informácie. Malo by sa to však znovu zhodnotiť, keď sa neskôr do systému pridajú ďalšie oddelenia.

Toto je príklad voľnejšieho prístupu k informáciám. V tomto prípade sa výnimky spracovávajú prostredníctvom užívateľských profilov, a nie pomocou obmedzení oprávnení. Sharon vyplnila časť formulára opisu knižnice, ktorá sa týka verejného oprávnenia, pre knižnicu zákazníckych záznamov (CUSTLIB).

Tabuľka 41. Formulár opisu knižnice spoločnosti JKL Toy—1. časť: Príklad zákazníckych záznamov

Názov knižnice: CUSTLIB	Opisný názov (text): Zákaznícke záznamy
Verejné oprávnenie pre knižnicu:	*USE
Verejné oprávnenie pre objekty v knižnici:	*CHANGE
Verejné oprávnenie pre nové objekty (CRTAUT):	*CHANGE

Sharon Jones zistila, že niektoré dočasné súbory v knižnici zákazníckych záznamov sú vymazávané počas spracovania aplikácie pohľadávok na konci mesiaca. Rozhodla sa radšej spracovať oprávnenie pre tie súbory jednotlivo, než aby podstúpila riziko, že by ďalšie objekty v knižnici mohli byť náhodne vymazané. Pre všetky ostatné činnosti spracovania je oprávnenie *CHANGE dostatočné.

I keď spracovanie na konci mesiaca spúšťa iba niekoľko užívateľov, Sharon si nemyslela, že by dočasné súbory predstavovali nejaké bezpečnostné riziko. Rozhodla sa dať tým súborom verejné oprávnenie *ALL namiesto poskytnutia toho oprávnenia len užívateľom, ktorí spúšťajú spracovanie na konci mesiaca. Nasledujúca tabuľka ukazuje druhú časť formulára opisu knižnice pre knižnicu zákazníckych záznamov:

Tabuľka 42. Formulár opisu knižnice spoločnosti JKL Toy—2. časť: Príklad zákazníckych záznamov

Vypíšte špecifické oprávnenia pre knižničné objekty

Tabuľka 42. Formulár opisu knižnice spoločnosti JKL Toy—2. časť: Príklad zákazníckych záznamov (pokračovanie)

Skupinový profil alebo užívateľský profil	Názov objektu	Typ objektu	Potrebné oprávnenie	Autorizačný zoznam
PUBLIC	ARFILE01	*FILE	*ALL	
PUBLIC	ARFILE02	*FILE	*ALL	
PUBLIC	ARFILE03	*FILE	*ALL	

Teraz môžete rozhodnúť o verejnom oprávnení pre knižnice programov, ktoré chcete mať.

Rozhodnutie o verejnom oprávnení na knižnice programov

Aplikačné programy sa často uchovávajú v osobitnej knižnici oddelene od súborov a iných objektov. Nevyžaduje sa, aby ste pre aplikácie používali osobitnú knižnicu, ale mnohí programátori používajú túto techniku pri navrhovaní aplikácií. Ak má vaša aplikácia osobitné knižnice programov, musíte rozhodnúť o verejnom oprávnení na tieto knižnice. Ak chcete úspešne spustiť programy, ale v knižniciach programov sú pravdepodobne iné objekty, ktoré vyžadujú ďalšie oprávnenie, na knižnicu aj na programy v tejto knižnici môžete použiť oprávnenie *USE. Položte vášmu programátorovi niekoľko otázok:

- Používa aplikácia na komunikáciu medzi programami dátové oblasti alebo fronty správ ? Sú v knižnici programov ? Oprávnenie *CHANGE na objekt sa vyžaduje na spracovávanie dátových oblastí a frontov správ.
- Vymazávajú sa v knižnici programov počas spracovania nejaké objekty, napríklad dátové oblasti ? Na vymazanie objektu sa vyžaduje oprávnenie *ALL na objekt .
- Vytvárajú sa v knižnici programov počas spracovania nejaké objekty, napríklad dátové oblasti ? Na vytvorenie všetkých nových objektov v tejto knižnici sa vyžaduje oprávnenie *CHANGE na knižnicu.

Vyplňte všetky informácie o zabezpečení prostriedkov v oboch častiach formulára Opis knižnice okrem stĺpca vlastníka knižnice a autorizačného zoznamu. Potom môžete určiť vlastníctvo knižníc a objektov.

Pravdepodobne si budete chcieť pozrieť nasledujúce dva príklady, ako Sharon Jones určila oprávnenie na knižnice programov. V prvom príklade Sharon rozhodla, že pre knižnicu programu Zákaznícke objednávky postačuje nie veľmi prísny prístup. Druhý príklad ukazuje prísnejší prístup, ktorý Sharon použila pre knižnicu programu Pohľadávky.

Príklad: Formulár opisu knižnice spoločnosti JKL Toy—nereštriktívny prístup: Sharon Jones preskúmala knižnicu programov zákazníckych objednávok a urobila si tieto poznámky:

- Jeden front správ, COMSGQ01, sa používa na komunikáciu medzi programami.
- Front správ sa vyprázdňuje, ale nikdy sa nevymazáva. Oprávnenie *CHANGE je pre front správ dostatočné.

Sharon sa rozhodla poskytnúť oprávnenie *USE všetkým objektom v knižnici programov a definovať front správ COMSGQ01 osobitne. Dve nasledujúce tabuľky ukazujú jej formulár opisu knižnice pre knižnicu COPGMLIB:

Tabuľka 43. Formulár opisu knižnice spoločnosti JKL Toy: Príklad knižnice programov

Formulár opisu knižnice	**1. časť z 2**
Názov knižnice: COPGMLIB	Opisný názov (text): Knižnica programov zákazníckych objednávok
Verejné oprávnenie pre knižnicu: *USE Verejné oprávnenie pre objekty v knižnici: *USE Verejné oprávnenie pre nové objekty (CRTAUT): *USE Vlastník knižnice:	

Tabuľka 44. Formulár opisu knižnice spoločnosti JKL Toy: Príklad knižnice programov

Formulár opisu knižnice				**2. časť z 2**
Vypíšte oprávnenia pre jednotlivé objekty v knižnici				
Skupinový profil alebo užívateľský profil	Názov objektu	Typ objektu	Potrebné oprávnenie	Autorizačné zoznamy
PUBLIC	COMSGQ01	*MSGQ	*CHANGE	

Používanie oprávnenia pre program na riadenie prístupu

I keď väčšina užívateľov v spoločnosti JKL Toy má dovolené meniť zákaznícke informácie, iba málo užívateľov má dovolené určovať úverové limity pre zákazníkov. Úverové limity sa ukladajú do hlavného zákazníckeho súboru (CUSTMAS), ale menia sa osobitným programom ARPGM12 v ARPGMLIB. Sharon môže ten program obmedziť, aby sa neoprávneným užívateľom zabránilo meniť úverové limity. Nasledujúce tabuľky ukazujú formulár opisu knižnice pre ARPGMLIB:

Tabuľka 45. Formulár opisu knižnice spoločnosti JKL Toy: Príklad jednotlivého oprávnenia

Formulár opisu knižnice	**1. časť z 2**
Názov knižnice: ARPGMLIB	Opisný názov (text): Knižnica programov pohľadávok
Verejné oprávnenie pre knižnicu: *USE Verejné oprávnenie pre objekty v knižnici: *USE Verejné oprávnenie pre nové objekty (CRTAUT): *USE Vlastník knižnice:	

Tabuľka 46. Formulár opisu knižnice spoločnosti JKL Toy: Príklad jednotlivého oprávnenia

Formulár opisu knižnice				**2. časť z 2**
Vypíšte oprávnenia pre jednotlivé objekty v knižnici				
Skupinový profil alebo užívateľský profil	Názov objektu	Typ objektu	Potrebné oprávnenie	Autorizačné zoznamy
PUBLIC	ARPGM12	*PGM	*EXCLUDE	
JACOBS	ARPGM12	*PGM	*USE	
DAVISP	ARPGM12	*PGM	*USE	
SMITHJ	ARPGM12	*PGM	*USE	

Možno si budete chcieť pozrieť reštriktívny príklad, ktorý používa prevzaté oprávnenie, skôr než začnete určovať vlastníctvo knižníc a objektov.

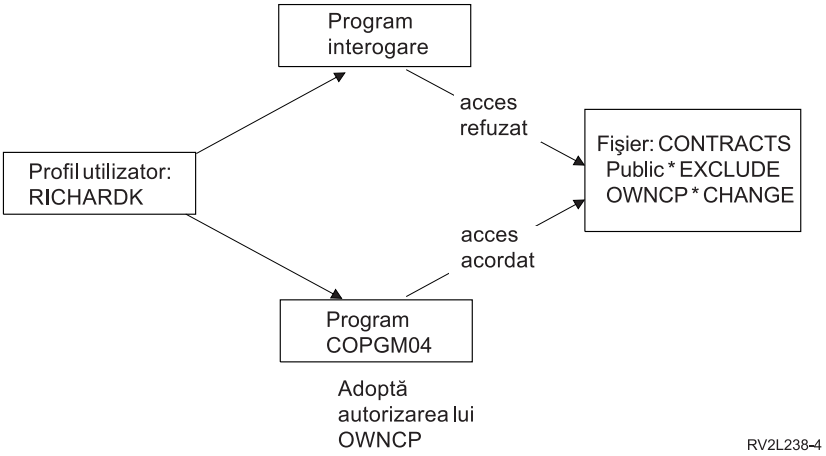
Príklad: Formulár opisu knižnice spoločnosti JKL Toy—reštriktívny prístup: Doterajšie príklady ukazovali voľnejší prístup k zabezpečeniu, pri ktorom väčšina užívateľov mala prístup k informáciám v knižnici. Informácie o kontraktoch a tvorbe cien sú v spoločnosti JKL Toy považované za dôverné a vyžadujú si reštriktívny prístup. Našťastie, tieto informácie sú uložené v osobitnej knižnici. Programy na aktualizovanie kontraktov a tvorby cien sú tiež v špeciálnej knižnici.

Sharon si pozrela bezpečnostné ciele pre aplikáciu Kontrakty a tvorba cien (pozrite si Určenie cieľov vášho zabezpečenia prostriedkov). Pozrela si tiež formulár opisu aplikácií a formuláre opisu knižnice. Sharon si uvedomovala, že bude ťažké dosiahnuť bezpečnostné ciele pre aplikáciu. Urobila si nejaké poznámky a rozobrala tento problém s poskytovateľom aplikácie:

- Personál odbytu a marketingu a riadiaci pracovníci potrebujú vytvárať a meniť kontrakty. Potrebujú používať súbory aj programy.
- Personál spracovania objednávok mení kontrakty a vidí ceny nepriamo pri vkladaní a odosielaní objednávok, ale nemá dovolené prezerať si kontrakty a ceny žiadnym iným spôsobom. Budú však používať Query na vytvorenie svojich správ o zákazníkoch a objednávkach. Ak by dostali oprávnenie pre súbory kontraktov a tvorby cien, mohli by vytvárať dotazové programy na ich prezeranie alebo tlačenie.

Poskytovateľ aplikácií pre spoločnosť JKL navrhol použitie bezpečnostnej funkcie prevzatého oprávnenia pre vyriešenie tohto problému. **Prevzaté oprávnenie** umožňuje užívateľovi prevziať oprávnenie vlastníka programu za behu programu. Užívateľ nemusí mať oprávnenie pre objekt.

Nasledujúci diagram ukazuje príklad, ako funguje prevzaté oprávnenie. Karen Richardsová (RICHARDK) z oddelenia spracovania objednávok bežne nemá oprávnenie používať súbor Kontrakty. Keď však vkladá objednávky, musí kontrolovať a aktualizovať zostatky kontraktov. Program vkladania objednávok, ktorý pracuje so zostatkami kontraktov (COPGM04), prevezme oprávnenie profilu OWNCP. Keď Karen spúšťa program COPGM04, má oprávnenie používať súbor kontraktov:



V téme ″Určenie vlastníctva knižníc a objektov″ nájdete podrobnosti o vlastníctve objektov. Váš poskytovateľ aplikácií alebo programátor môže zadať, že program prevezme oprávnenie vlastníka, pri vytvorení (kompilácii) programu, alebo môže programátor zadať prevzaté oprávnenie pomocou príkazu CHGPGM (Change Program). Pred použitím tejto techniky sa uistite, že rozumiete všetkým funkciám programu.

Sharon sa rozhodla použiť funkciu prevzatého oprávnenia, aby poskytla užívateľom mimo oddelenia odbytu a marketingu prístup k súborom kontraktov a tvorby cien. Okrem toho určila, že prístup *CHANGE je dostatočný pre všetky objekty používané aplikáciou Kontrakty a tvorba cien. Nasledujúce tabuľky ukazujú formulár opisu knižnice pre knižnicu Kontrakty:

Tabuľka 47. Formulár opisu knižnice spoločnosti JKL Toy: Príklad reštriktívneho oprávnenia

Formulár opisu knižnice	**1. časť z 2**
Názov knižnice: CONTRACTS	Opisný názov (text): Knižnica kontraktov a tvorby cien
Verejné oprávnenie pre knižnicu: *EXCLUDE Verejné oprávnenie pre objekty v knižnici: *CHANGE Verejné oprávnenie pre nové objekty (CRTAUT): *CHANGE Vlastník knižnice:	

Tabuľka 48. Formulár opisu knižnice spoločnosti JKL Toy: Príklad reštriktívneho oprávnenia

Formulár opisu knižnice				**2. časť z 2**
Vypíšte oprávnenia pre jednotlivé objekty v knižnici				
Skupinový profil alebo užívateľský profil	Názov objektu	Typ objektu	Potrebné oprávnenie	Autorizačné zoznamy
DPTSM	CONTRACTS	*LIB	*USE	
DPTMG	CONTRACTS	*LIB	*USE	

Nemusíte obmedziť oprávnenie pre objekty v knižnici, pretože obmedzíte prístup k samotnej knižnici. Sharon tiež poskytla oprávnenie riadiacim pracovníkom a oddeleniu odbytu a marketingu. Použila skupinové oprávnenie namiesto poskytnutia oprávnenia každému jednotlivcovi v oddeleniach.

Poznámka: Skúsený programátor, ktorý má prístup do knižnice, môže dokázať udržať prístup k objektom v knižnici aj keď ste zrušili oprávnenie ku knižnici. Ak knižnica obsahuje objekty s vysokými bezpečnostnými požiadavkami, obmedzte objekty a knižnicu pre úplnú ochranu.

Možno si budete chcieť pozrieť nereštriktívny príklad, ktorý používa verejné oprávnenie, skôr než začnete určovať vlastníctvo knižníc a objektov.

Určenie vlastníctva knižníc a objektov

Po naplánovaní bezpečnosti pre knižnice aplikácií môžete rozhodnúť o vlastníctve knižníc a objektov. Každý objekt má pri jeho vytvorení priradeného vlastníka. Vlastník objektu má automaticky na tento objekt kompletné oprávnenie, zahrňujúce možnosť oprávniť ďalších užívateľov na používanie tohto objektu, jeho zmenu alebo jeho vymazanie. Správca bezpečnosti môže tieto funkcie vykonávať v prípade každého objektu v systéme.

Systém používa profil vlastníka objektu na sledovanie, kto má oprávnenie na tento objekt. Systém vykonáva túto funkciu interne. Toto nesmie mať priamy vplyv na užívateľský profil. Ak však vlastníctvo objektu nenaplánujete správne, niektoré užívateľské profily môžu veľmi narásť.

Keď systém ukladá nejaký objekt, spolu s ním ukladá aj názov profilu vlastníka. Systém túto informáciu používa v prípade, že tento objekt obnovuje. Ak profil vlastníka obnoveného objektu v systéme nie je, systém prenesie vlastníctvo na profil, dodaný spoločnosťou IBM, ktorý má názov QDFTOWN.

Odporúčania

Nižšie uvedené odporúčania platia pre mnohé ale nie pre všetky situácie. Po prečítaní týchto odporúčaní preberte vaše predstavy o vlastníctve objektu s vaším programátorom alebo poskytovateľom aplikácií. Ak aplikácie kupujete, asi nebudete môcť určiť, ktorý profil bude vlastniť knižnice a objekty. Aplikácia môže byť navrhnutá tak, aby sa vlastníctvo nedalo meniť.

- Ako vlastníka aplikácií nepoužívajte profil, dodaný spoločnosťou IBM, napríklad QSECOFR alebo QPGMR. Tieto profily vlastnia mnoho objektov v knižniciach, dodaných spoločnosťou IBM a sú už veľmi veľké.
- Za normálnych okolností by skupinový profil nemal vlastniť aplikáciu. Každý člen v skupine má rovnaké oprávnenie ako skupinový profil, pokiaľ konkrétne nepridelíte nižšie oprávnenie. Každému členovi skupiny by ste de facto udelili kompletné oprávnenie na aplikáciu.
- Ak plánujete preniesť zodpovednosť za riadenie aplikácií na manažérov v rôznych oddeleniach, títo manažéri by mohli byť vlastníkmi všetkých objektov aplikácie. Manažér aplikácie by však mohol meniť zodpovednosti. V tom prípade by ste mali vlastníctvo všetkých objektov aplikácie preniesť na nového manažéra.
- Mnohí užívatelia používajú techniku vytvárania špeciálneho profilu vlastníka pre každú aplikáciu s heslom, nastaveným na *NONE. Systém používa profil vlastníka na manažovanie oprávnení na túto aplikáciu. Správca bezpečnosti (alebo niekto s týmto oprávnením) vykonáva aktuálne manažovanie aplikácie alebo ho zveruje manažérom s oprávnením *ALL na určité aplikácie.

Rozhodnite, ktoré profily majú vlastniť vaše aplikácie. Informácie o profile vlastníka zadajte do každého formulára Opis knižnice.

Než začnete rozhodovať o vlastníctve a prístupe pre užívateľské knižnice, pravdepodobne si budete chcieť pozrieť príklad, ako spoločnosť JKL Toy Company stanovila vlastníctvo aplikácie.

Príklad: Vlastníctvo aplikácie spoločnosti JKL Toy

Sharon Jones sa rozhodla vytvoriť špeciálny profil vlastníka pre každú aplikáciu. Ona spolu s Kenom Harrisonom, záložným správcom bezpečnosti, prevezmú zodpovednosť za riadenie aplikačného zabezpečenia. Neskôr, ak budú bezpečnostné požiadavky spoločnosti zložitejšie, môže Sharon poveriť určitou zodpovednosťou za riadenie oprávnení vedúcich oddelení.

Sharon pridala novú položku do formulára názvových konvencií:

Tabuľka 49. Formulár názvových konvencií spoločnosti JKL Toy: Príklad profilu vlastníka

Typ objektu	Pomenúvacia konvencia
Profil vlastníka	Profil vlastníka bude vytvorený pre každú aplikáciu. Bude vlastniť všetky knižnice aplikácií a objekty v nich. Názov profilu vlastníka bude OWN plus skratka aplikácie. Profil vlastníka riadenia zásob bude OWNIC.

Sharon sa rozhodla dať na začiatok názvu profilu vlastníka OWN, aby sa všetky profily vlastníka na obrazovkách a zoznamoch objavovali spolu.

Sharon priradila vlastníkov ku všetkým knižniciam aplikácií a tie informácie zadala do formulárov názvových konvencií. Jedinou knižnicou, ktorá mala viac než jedného možného vlastníka aplikácie, bola knižnica zákazníckych záznamov. Keďže aplikácia pohľadávok sa používa na vytváranie nových zákazníkov a nastavovanie úverových limitov, Sharon rozhodla, že by mala vlastniť zákaznícke súbory. Toto sú vlastníci, ktorých priradila:

Názov knižnice	Meno vlastníka
ICPGMLIB	OWNIC
ITEMLIB	OWNIC
CONTRACTS	OWNCP
CPPGMLIB	OWNCP
COPGMLIB	OWNCO
CUSTLIB	OWNAR
ARPGMLIB	OWNAR

Teraz môžete rozhodnúť o vlastníctve a prístupe pre vaše užívateľské knižnice.

Rozhodnutie o vlastníctve a prístupe v prípade užívateľských knižníc

Ak má váš systém licenčný program IBM Query for iSeries alebo iný program na podporu rozhodovania, vaši užívatelia potrebujú knižnicu na ukladanie dotazovacích programov, ktoré vytvoria. Bežne je touto knižnicou **aktuálna knižnica** v užívateľskom profile. Viac informácií o vytvorení aktuálnej knižnice pre jednotlivých užívateľov nájdete v téme Výber hodnôt, ovplyvňujúcich prihlásenie.″ Sharon Jones plánuje pre Obchodné a marketingové oddelenie používať aktuálne knižnice a pre ostatné oddelenia skupinové knižnice:

- Pracovníci Obchodného a marketingového oddelenia budú často využívať program Query. Každý užívateľ by mal mať súkromnú knižnicu. V opačnom prípade by sa museli starať o to, ako nazvať svoje dotazy a mohli by si navzájom náhodne vymazať svoje programy.
- Ostatné oddelenia budú mať na začiatku skupinové knižnice. Ak vytvárajú veľa dotazovacích programov, môžeme zvážiť individuálne knižnice.

Ak užívateľ patrí do skupiny, použite pole v užívateľskom profile, aby ste určili, či tento užívateľ alebo skupina vlastnia nejaké objekty, vytvorené týmto užívateľom. Ak tento užívateľ vlastní objekty, môžete stanoviť oprávnenie, ktoré majú členovia skupiny na používanie týchto objektov. Môžete tiež stanoviť, či oprávnenie tejto skupiny je oprávnením

primárnej skupiny alebo súkromným oprávnením. Oprávnenie primárnej skupiny môže poskytnúť lepší výkon systému. Sharon si urobila ďalšie poznámky o užívateľských knižniciach:

- Pracovníci Obchodného a marketingového oddelenia by mali vlastniť objekty, ktoré vytvárajú a nie nechať tieto objekty vlastniť skupinou. Nemusia navzájom meniť svoje dotazovacie programy.
- Všetci členovia skupiny by mali mať možnosť navzájom spúšťať svoje dotazovacie programy, čo znamená, že táto skupina dostane oprávnenie *USE na všetky objekty, vytvorené členom skupiny.
- Oprávnenie skupiny by malo byť oprávnením primárnej skupiny.
- Verejnosť nemôže mať prístup k týmto knižniciam. Pracovníci Obchodného a marketingového oddelenia môžu mať výstupné súbory zo svojich dotazov. Tieto súbory by mohli obsahovať dôverné údaje.
- V prípade iných oddelení bude skupina vlastniť skupinovú knižnicu a všetko, čo sa v tejto knižnici vytvára. Znamená to, že ktorýkoľvek člen skupiny môže v tejto knižnici čokoľvek meniť alebo vymazávať. V prípade, že nastanú problémy, môžeme vyskúšať inú metódu.

Nižšie uvedená tabuľka znázorňuje Formulár Individuálny užívateľský profil pre Obchodné a marketingové oddelenie, používajúce objekty, ktoré vlastní užívateľ:

Tabuľka 50. Formulár Individuálny užívateľský profil, ktorý používa spoločnosť JKL Toy Company: Príklad objektov, vlastnených užívateľom

Názvy skupinových profilov: DPTSM	
Vlastník vytvorených objektov: *USRPRF	Skupinové oprávnenie na vytvorené objekty: *USE
Typ skupinového oprávnenia: *PGP	

Nižšie uvedená tabuľka znázorňuje Formulár Individuálny užívateľský profil pre oddelenie, používajúce objekty, ktoré vlastní skupina:

Tabuľka 51. Formulár Individuálny užívateľský profil, ktorý používa spoločnosť JKL Toy Company: Príklad objektov, vlastnených skupinou

Názvy skupinových profilov: DPTxx	
Vlastník vytvorených objektov: *GRPPRF	Skupinové oprávnenie na vytvorené objekty:

Ak je vlastníkom vytvorených objektov skupina, pole **Skupinové oprávnenie na vytvorené objekty** sa nepoužíva. Členovia skupiny majú automaticky oprávnenie *ALL na všetky vytvorené objekty.

Rozhodnite, kto má vlastniť užívateľské knižnice a mať k nim prístup. Vaše voľby zadajte do polí **Vlastník vytvorených objektov** a **Skupinové oprávnenie na objekty** vo formulári Individuálny užívateľský profil. Teraz môžete začať zoskupovať objekty.

Zoskupovanie objektov

Po určení vlastníctva knižníc a objektov môžete v systéme začať zoskupovať objekty. Ak chcete zjednodušiť manažovanie oprávnení, na zoskupenie objektov s rovnakými požiadavkami použite autorizačný zoznam. Potom môžete udeliť verejné oprávnenie, oprávnenie skupinových profilov a užívateľských profilov na tento autorizačný zoznam a nie na jednotlivé objekty v tomto zozname. Systém sa správa rovnako ku každému objektu, ktorý zabezpečíte autorizačným zoznamom, ale vy môžete dať rôznym užívateľom rôzne oprávnenia na celý zoznam.

Autorizačný zoznam uľahčuje obnovenie oprávnení, keď obnovujete objekty. Ak objekty zabezpečujete autorizačným zoznamom, proces obnovy automaticky pripojí tieto objekty do zoznamu.

Skupine alebo užívateľovi môžete dať oprávnenie na manažovanie autorizačného zoznamu (*AUTLMGT). Manažovanie autorizačného zoznamu umožňuje užívateľovi pridávať a odstraňovať z tohto zoznamu iných užívateľov a meniť oprávnenia pre týchto užívateľov.

Odporúčania

- Autorizačné zoznamy použite pre objekty, ktoré vyžadujú ochranu bezpečnosti a ktoré majú podobné požiadavky na bezpečnosť. Používanie autorizačných zoznamov je pre vás podnetom na zváženie kategórií oprávnení a nie individuálnych oprávnení. Autorizačné zoznamy uľahčujú aj obnovu objektov a auditovanie oprávnení vo vašom systéme.
- Vyhnite sa komplikovaným schémam, ktoré kombinujú autorizačné zoznamy, skupinové oprávnenie a individuálne oprávnenie. Namiesto použitia všetkých metód naraz zvoľte radšej metódu, ktorá najlepšie vyhovuje tejto požiadavke.

Do vášho formulára Názvové konvencie budete musieť pridať aj názvové konvencie pre autorizačné zoznamy.

Po vypracovaní formulára Autorizačný zoznam sa vráťte a pridajte tieto informácie do vášho formulára Opis knižnice. Váš programátor alebo poskytovateľ aplikácií možno už vytvoril autorizačné zoznamy. Určite si to u nich overte.

Než začnete plánovať bezpečnosť pre tlačiarne a tlačový výstup, pravdepodobne si budete chcieť pozrieť príklad, ako Sharon Jones zo spoločnosti JKL Toy Company plánovala autorizačné zoznamy.

Príklad: Formulár autorizačného zoznamu spoločnosti JKL Toy

Sharon si pozrela opis knižnice pre knižnicu zákazníckych záznamov a rozhodla sa vytvoriť autorizačný zoznam pre súbory, ktoré sa vymazávajú na konci každého mesiaca. I keď sa vymazávajú len tri súbory, Sharon sa rozhodla použiť autorizačný zoznam pre zjednodušenie riadenia oprávnení. Ak sa neskôr pridajú ďalšie súbory do procesu spracovávaného na konci mesiaca, bude môcť tie súbory jednoducho zabezpečiť autorizačným zoznamom. Sharon sa rozhodla nepripustiť verejnosť k súborom, aby zabránila neúmyselným problémom počas spracovania na konci mesiaca. Oprávnenie *ALL poskytla len užívateľom, ktorí spúšťajú spracovanie. Rose Willisová, ktorá býva večer operátorkou systému, môže potrebovať prezerať si informácie o súboroch pre kontrolu spracovania na konci mesiaca. Potrebuje oprávnenie *USE.

Nasledujúca tabuľka ukazuje názvovú konvenciu, ktorú Sharon použila pre autorizačné zoznamy:

Tabuľka 52. Formulár názvových konvencií spoločnosti JKL Toy: Príklad autorizačného zoznamu

Formulár názvových konvencií	
Pripravil: Sharon Jones	Dátum: 9/5/99
Typ objektu	**Pomenúvacia konvencia**
Autorizačné zoznamy	Pre zoznamy, ktoré zabezpečujú objekty z jednej knižnice, použite časť názvu knižnice plus LST a číslo. Zoznam pre objekty v CUSTLIB by bol CUSTLST1. Pre zoznam zabezpečujúci objekty z viac než jednej knižnice použite skratku aplikácie, ak je to možné: ARLST1. Ak sa zoznam vzťahuje na viaceré aplikácie, vyberte akýkoľvek zmysluplný názov. Opis zoznamu by mal uvádzať jeho hlavný účel.

Nasledujúca tabuľka ukazuje formulár autorizačného zoznamu pre knižnicu CUSTLIB. Sharon pripravila tento formulár s použitím informácií z formulára opisu knižnice:

Tabuľka 53. Plán autorizačného zoznamu spoločnosti JKL Toy: príklad

Formulár autorizačného zoznamu					
Názov autorizačného zoznamu: CUSTLST1					
Opis: Súbory vymazávané počas spracovania na konci mesiaca.					
Vypíšte objekty, ktoré zoznam zabezpečuje					
Názov objektu	Typ objektu	Knižnica objektov	Názov objektu	Typ objektu	Knižnica objektov
ARFILE01	*FILE	CUSTLIB	ARFFILE02	*FILE	CUSTLIB
ARFILE03	*FILE	CUSTLIB			
Vypíšte skupiny a užívateľov, ktorí majú prístup do zoznamu					

Tabuľka 53. Plán autorizačného zoznamu spoločnosti JKL Toy: príklad (pokračovanie)

Skupina alebo užívateľ	Typ povoleného prístupu	Vypísať riadenie?	Skupina alebo užívateľ	Typ povoleného prístupu	Vypísať riadenie?
PUBLIC	*EXCLUDE	nie	ROSSG	*ALL	nie
SMITHJ	*ALL	nie	JONESS	*ALL	áno
WILLISR	*USE	nie			

Sharon tiež pridala informácie autorizačného zoznamu do formulára opisu knižnice pre knižnicu CUSTLIB:

Formulár opisu knižnice				2. časť z 2
Pripravil: Sharon Jones			Dátum: 9/9/99	
Názov knižnice: CUSTLIB				
Vypíšte špecifické oprávnenia pre knižničné objekty				
Skupinový profil alebo užívateľský profil	Názov objektu	Typ objektu	Potrebné oprávnenie	Autorizačný zoznam
PUBLIC	ARFILE01	*FILE	*AUTL	CUSTLST1
PUBLIC	ARFILE02	*FILE	*AUTL	CUSTLST1
PUBLIC	ARFILE03	*FILE	*AUTL	CUSTLST1

Všimnite si, že verejné oprávnenie pre každý súbor musí byť zmenené na *AUTL, aby systém použil autorizačný zoznam na určenie verejného oprávnenia.

Pozrite si skupinové a individuálne oprávnenia vo vašich formulároch opisu knižnice. Rozhodnite, či bude použitie autorizačných zoznamov vhodné. Ak áno, pripravte formuláre autorizačného zoznamu a aktualizujte formuláre opisu knižnice informáciami autorizačného zoznamu. Potom môžete plánovať zabezpečenie pre tlačiarne a tlačový výstup.

Plánovanie bezpečnosti pre tlačiarne a tlačový výstup

Po zoskupení vašich objektov musíte naplánovať, ako budete chrániť tlačový výstup. Vypracovali ste plány na ochranu informácií, uložených vo vašom systéme. Musíte tiež naplánovať ochranu dôverných informácií počas ich tlače alebo čakania na tlač. Vo vašom Pláne fyzického zabezpečenia skontrolujte tlačiarne, ktoré vaša spoločnosť používa na tlač dôverného výstupu.

Keď spúšťate program, ktorý tlačí správu, táto správa zvyčajne nejde priamo na tlačiareň. Tento program vytvorí kópiu správy, nazývanú **spoolový súbor** alebo **tlačový výstup**. Kým bude k dispozícii tlačiareň, systém uloží spoolový súbor do objektu, nazývaného **výstupný front**. Keď je tlačový výstup vo výstupnom fronte, správu si môžete prezrieť na vašej pracovnej stanici. Môžete si ju aj ponechať alebo ju nasmerovať na konkrétnu tlačiareň.

Spoolovanie uľahčuje rozvrhnutie tlačových úloh a zdieľanie tlačiarní. Spoolovanie vám tiež pomáha chrániť dôverný výstup. Ak si chcete dôverný výstup ponechať a vymedziť osoby, ktoré môžu prezerať alebo manažovať tieto výstupné fronty, môžete vytvoriť jeden alebo viac špeciálnych výstupných frontov. Taktiež môžete určovať, kedy sa má dôverný výstup odoslať z frontu na tlačiareň.

Pri práci s touto témou vyplňte formulár Bezpečnosť tlačového výstupu a pracovných staníc.

Keď vytvárate špeciálny výstupný front, môžete špecifikovať niekoľko parametrov, týkajúcich sa bezpečnosti:

- **Parameter DSPDTA (Display Data)**: Parameter DSPDTA výstupného frontu určuje, či užívateľ môže prezerať, posielať alebo kopírovať spoolový súbor, ktorý je vlastníctvom iného užívateľa.
- **Parameter AUTCHK (Authority to Check)**: Parameter AUTCHK výstupného frontu určuje, či užívateľ môže zmeniť alebo vymazať spoolový súbor, ktorý je vlastníctvom iného užívateľa.

- **Parameter OPRCTL (Operator Control)**: Parameter OPRCTL výstupného frontu určuje, či užívatelia so zvláštnym oprávnením *JOBCTL (alebo s triedou užívateľa *SYSOPR) majú povolené riadiť výstupný front.

Parametre výstupného frontu, oprávnenie užívateľa na výstupný front a zvláštne oprávnenie užívateľa pracujú spolu, aby určili funkcie, ktoré môže užívateľ vykonávať na spoolových súboroch vo výstupnom fronte. Nižšie uvedená tabuľka znázorňuje, ktoré kombinácie umožňujú užívateľom vykonávať rozličné funkcie:

Tlačové funkcie	Parametre výstupného frontu			Oprávnenie na výstupný front	Zvláštne oprávnenie
	DSPDTA	AUTCHK	OPRCTL		
Pridať spoolový súbor do frontu [1]	Každý	Každý	Každý	*READ	Žiadny
	Každý	Každý	*Yes	Každý	*JOBCTL
Prezerať zoznamy spoolových súborov (príkaz WRKOUTQ)[2]	Každý	Každý	Každý	*READ	Žiadny
	Každý	Každý	*Yes	Každý	*JOBCTL
Zobrazovať, kopírovať alebo posielať spoolové súbory (DSPSPLF, CPYSPFL, SNDNETSPLF, SNTCPSPLF)[2]	*YES	Každý	Každý	*READ	Žiadny
	*NO	*DTAAUT	Každý	*CHANGE	Žiadny
	*NO	*OWNER	Každý	Vlastník[3]	Žiadny
	*YES	Každý	*Yes	Každý	*JOBCTL
	*NO	Každý	*Yes	Každý	*JOBCTL
	*OWNER[5]	Každý	Každý	Každý	Každý
Meniť, vymazávať, ponechať si, uvoľniť spoolový súbor (CHGSPLFA, DLTSPLF, HLDSPLF, RLSSPLF)[2]	Každý	*DTAAUT	Každý	*CHANGE	Žiadny
	Každý	*OWNER	Každý	Vlastník[3]	Žiadny
Meniť, čistiť, ponechať si a uvoľniť výstupný front (CHGOUTQ, CLROUTO, HLDOUTQ, RLSOUT)[2]	Každý	*DTAAUT	Každý	*CHANGE	Žiadny
	Každý	*OWNER	Každý	Vlastník[3]	Žiadny
	Každý	Každý	*YES	Každý	*JOBCTL
Spustiť zapisovač pre front (STRPRTWTR, STRRMTWTR)[2]	Každý	*DTAAUT	*Any	*CHANGE[4]	Žiadny
	Každý	Každý	*YES	Každý[4]	*JOBCTL

1 Toto je oprávnenie, vyžadované na nasmerovanie vášho výstupu do výstupného frontu.

2 Používanie týchto príkazov alebo rovnocenných volieb z obrazovky.

3 Musíte byť vlastníkom výstupného frontu.

4 Vyžaduje aj oprávnenie *USE na opis tlačového zariadenia.

5 Musíte byť vlastníkom spoolového súboru alebo musíte mať na prácu s týmto príkazom zvláštne oprávnenie *SPLCTL.

Vo vašom Pláne fyzického zabezpečenia si pozrite časť, týkajúcu sa tlačiarní. Pri práci s touto témou vyplňte vo formulári Bezpečnosť tlačového výstupu a pracovných staníc časť, týkajúcu sa výstupného frontu.

Než naplánujete zabezpečenie prostriedkov pre pracovné stanice, pravdepodobne si budete chcieť pozrieť príklad, ako Sharon Jones zo spoločnosti JKL Toy Company určila hodnoty v týchto parametroch výstupného frontu.

Príklad: Formulár zabezpečenia výstupného frontu a pracovnej stanice spoločnosti JKL Toy—výstupný front

Oddelenie odbytu a marketingu v spoločnosti JKL Toy má dve požiadavky pre dôvernú tlač:

- Predbežné cenníky sa tlačia pri plánovaní zmien cien. Tieto informácie nesmie vidieť nikto mimo oddelenia odbytu a marketingu, s výnimkou vedúcich pracovníkov spoločnosti.
- Kontrakty sú dôverné v čase, keď sú dojednávané. Hrubý návrh kontraktu môže vidieť iba osoba, ktorá kontrakt dojednáva, a nie ostatní členovia oddelenia odbytu a marketingu.

Sharon sa rozhodla vytvoriť dva špeciálne výstupné fronty:

PRICEQ
Má byť používaný pre predbežné cenníky. Každý v oddelení odbytu a marketingu môže vykonávať všetky funkcie v tomto výstupnom fronte. Nikto mimo oddelenia nemôže používať tento výstupný front, vrátane operátorov systému. PRICEQ je v knižnici CONTRACTS.

NEWCP
Má byť používaný pre tlač kontraktov, ktoré sú dojednávané. Výstupný front je zdieľaný členmi oddelenia odbytu a marketingu, ale iba človek, ktorý vytvára spoolový súbor vo výstupnom fronte, môže ten súbor riadiť. NEWCP je v knižnici CONTRACTS.

Nasledujúca tabuľka ukazuje formulár zabezpečenia výstupného frontu a pracovnej stanice, ktorý Sharon pripravila pre tieto výstupné fronty:

Tabuľka 54. Formulár zabezpečenia výstupného frontu a pracovnej stanice spoločnosti JKL Toy: Príklad výstupného frontu tlačiarne

Vypíšte parametre pre obmedzené výstupné fronty:				
Názov výstupného frontu	Knižnica výstupného frontu	Zobraziť každý súbor (DSPDTA)	Oprávnenie na označenie (AUTCHK)	Riadenie operátorom (OPRCTL)
PRICEQ	CONTRACTS	*YES	*DTAAUT	*NO
NEWCP	CONTRACTS	*NO	*OWNER	*NO

Téma Rozhodnutie o verejnom oprávnení pre knižnice programov obsahuje príklad, ktorý ukazuje oprávnenie pre knižnicu CONTRACTS v spoločnosti JKL Toy. Do tejto knižnice majú prístup iba vedúci pracovníci a oddelenie odbytu a marketingu. Verejné oprávnenie pre objekty v knižnici (vrátane týchto výstupných frontov) je *CHANGE.

Keďže parameter AUTCHK vo výstupnom fronte NEWCP je *OWNER, s tým súborom môže pracovať len vlastník spoolového súboru (pozrite si vyššie ukázanú tabuľku Vyžadované oprávnenie pre vykonávanie tlačových funkcií). Tým sa členom oddelenia odbytu a marketingu zabráni tlačiť nové kontrakty jeden druhého, alebo si ich prezerať vo výstupnom fronte.

Po naplánovaní zabezpečenia výstupného frontu tlačiarne môžete plánovať zabezpečenie pre pracovné stanice.

Plánovanie bezpečnosti pre pracovné stanice

Po naplánovaní zabezpečenia prostriedkov pre tlačiarne a tlačový výstup môžete začať plánovať bezpečnosť pracovných staníc. Vo vašom Pláne fyzického zabezpečenia ste uviedli pracovné stanice, ktoré predstavujú bezpečnostné riziko z dôvodu ich umiestnenia. Pomocou týchto informácií určite, ktoré pracovné stanice musíte obmedziť.

Ľuďom, ktorí používajú tieto pracovné stanice, môžete odporučiť, aby si dobre uvedomili dôležitosť bezpečnosti. Pri každom odchode od pracovnej stanice sa musia odhlásiť. V prípade citlivých pracovných staníc si vo vašej bezpečnostnej politike pravdepodobne budete chcieť zaznamenať vaše rozhodnutie o procedúrach odhlasovania. Ak chcete riziká znížiť na minimum, môžete tiež obmedziť funkcie, ktoré sa na týchto pracovných staniciach môžu vykonávať.

Najjednoduchšou metódou na obmedzenie funkcie na pracovnej stanici je obmedziť ju na užívateľské profily s obmedzenou funkciou. Sharon Jones použila túto techniku pre Skladové oddelenie v spoločnosti JKL Toy Company. Sharon povolila Rayovi Wagnerovi Janice Amesovej, ktorí pracujú v nákladnom prístave, spúšťať len program na prijímanie inventára. Sharon ich urobila aj jedinými užívateľmi, ktorí majú povolené prihlasovať sa na pracovnú stanicu v nákladnom prístave.

Môžete sa rozhodnúť, že užívateľom s oprávnením správcu bezpečnosti alebo servisným oprávnením zabránite v prihlasovaní na každú pracovnú stanicu. Ak na to použijete systémovú hodnotu QLMTSECOFR, užívatelia s oprávnením správcu bezpečnosti sa môžu prihlasovať len na konkrétne autorizované pracovné stanice.

Vo formulári Bezpečnosť výstupného frontu a pracovných staníc vypracujte časť, týkajúcu sa pracovných staníc.

Pri vypracovávaní časti, týkajúcej sa pracovných staníc vo formulári Bezpečnosť výstupného frontu a pracovných staníc, si pravdepodobne budete chcieť pozrieť príklad, ako Sharon plánovala bezpečnosť pre pracovné stanice. Aby ste mali istotu, že váš plán zabezpečenia prostriedkov bude jednoduchý a kompletný, mali by ste si pozrieť aj zoznam odporúčaní pre zabezpečenie prostriedkov. Po prečítaní príkladu a odporúčaní môžete začať plánovať inštaláciu vašich aplikácií.

Príklad: Formulár zabezpečenia výstupného frontu a pracovnej stanice spoločnosti JKL Toy—pracovná stanica

Sharon Jones si prezrela plán fyzického zabezpečenia, aby určila, ktoré pracovné stanice predstavujú bezpečnostné riziko. Napríklad v spoločnosti JKL Toy majú užívatelia mimo spoločnosti ľahký prístup k pracovným staniciam v priestore nakladania a vo vzdialenej predajnej kancelárii. Sharon v pláne fyzického zabezpečenia vyznačila, že tieto pracovné stanice predstavujú potenciálne bezpečnostné riziko.

Najjednoduchšou metódou obmedzenia funkcie na pracovnej stanici je obmedziť ju v užívateľských profiloch s obmedzenou funkciou. Sharon Jones použila túto techniku pre sklad spoločnosti JKL Toy. Sharon povolila Rayovi Wagnerovi a Janice Amesovej, ktorí pracujú na nakladacej rampe, spúšťať iba program zásob. Okrem toho ich Sharon urobila jedinými užívateľmi, ktorí majú povolené prihlásiť sa na pracovnej stanici v mieste nakladania.

Sharon prehodnotila svoju voľbu pre systémovú hodnotu QLMTSECOFR. Rozhodla sa, že ju nastaví na 1(Yes) kvôli dodatočnej ochrane zraniteľných pracovných staníc v mieste nakladania a vo vzdialenej predajnej kancelárii.

Nasledujúca tabuľka ukazuje časť formulára zabezpečenia výstupného frontu a pracovnej stanice prislúchajúcu pracovnej stanici, ktorý pripravila Sharon.

Tabuľka 55. Formulár zabezpečenia výstupného frontu a pracovnej stanice spoločnosti JKL Toy: Príklad pracovnej stanice

Pracovné stanice správcu bezpečnosti: Ak obmedzíte správcu bezpečnosti na určité pracovné stanice (systémová hodnota QLMTSECOFR je yes), vypíšte nižšie pracovné stanice s oprávnením pre správcu bezpečnosti a každého s oprávnením *ALLOBJ: Všetky pracovné stanice okrem tých, ktoré sú vypísané nižšie.	
Vypíšte nižšie oprávnenia pre obmedzené pracovné stanice:	
Názov pracovnej stanice	Skupiny alebo užívatelia, ktorí majú oprávnenie (oprávnenie *CHANGE)
DSP10	AMESJ, WAGNERR
DSP11	AMESJ, WAGNERR
RMT01	UNGERJ, BELLB
RMT02	UNGERJ, BELLB

Možno si budete chcieť pozrieť prehľad odporúčaní zabezpečenia prostriedkov skôr, než budete plánovať inštaláciu vašej aplikácie.

Súhrn odporúčaní pre zabezpečenie prostriedkov

Po dokončení plánovania bezpečnosti pracovných staníc si môžete prečítať nasledujúce odporúčania pre zabezpečenie prostriedkov. Systém iSeries ponúka viacero možností na ochranu informácií o vašom systéme. Poskytuje vám to pružnosť pri navrhovaní čo najlepšieho zabezpečenia prostriedkov pre vašu spoločnosť. Toto množstvo volieb však môže byť zavádzajúce.

Použitím spoločnosti JKL Toy Company ako príkladu sa táto téma pokúsila demonštrovať základný prístup k plánovaniu zabezpečenia prostriedkov, ktorý používa tieto inštrukcie:

- Prechod od všeobecného ku konkrétnemu:
  - Naplánovať bezpečnosť pre knižnice. Jednotlivými objektmi sa zaoberať len v prípade potreby.
  - Najprv naplánovať verejné oprávnenie, za ktorým nasleduje skupinové oprávnenie a individuálne oprávnenie.

- Ak chcete zlepšiť výkon a zjednodušiť zálohovanie a obnovu, zadefinujte konkrétne zabezpečenie len pre objekty, ktorých požiadavky na bezpečnosť nemožno uspokojiť pomocou verejného oprávnenia.
- Verejné oprávnenie na nové objekty v knižnici (CRTAUT) vytvorte rovnako ako verejné oprávnenie, ktoré ste zadefinovali pre väčšinu existujúcich objektov v tejto knižnici.
- Nepokúšajte sa dávať skupinám alebo jednotlivcom menšie oprávnenie ako má verejnosť. Znižuje to výkon, neskôr môže viesť k nedorozumeniam a sťažuje auditovanie. Ak viete, že každý má prinajmenšom rovnaké oprávnenie na objekt ako má verejnosť, uľahčí vám to plánovanie a auditovanie bezpečnosti.
- Na zoskupovanie objektov s rovnakými požiadavkami na bezpečnosť použite autorizačné zoznamy. Autorizačné zoznamy sa manažujú jednoduchšie ako jednotlivé oprávnenia a pomáhajú pri obnove bezpečnostných informácií.
- Vytvorte zvláštne užívateľské profily ako vlastníkov aplikácie. Heslo vlastníka nastavte na hodnotu *NONE.
- Vyhnite sa vlastneniu aplikácií profilmi dodanými spoločnosťou IBM, napríklad profilom QSECOFR alebo QPGMR.
- Pre dôverné správy použite zvláštne výstupné fronty. Výstupný front umiestnite do rovnakej knižnice ako dôverné informácie.
- Obmedzte počet užívateľov s oprávnením správcu bezpečnosti.
- Pri udeľovaní oprávnenia *ALL na objekty alebo knižnice buďte opatrní. Ľudia s oprávnením *ALL môžu náhodne všeličo vymazať.

Ak chcete mať istotu, že naplánovanie nastavenia zabezpečenia prostriedkov sa vám podarilo, mali by ste zozbierať nasledujúce informácie:

- Pre všetky vaše knižnice aplikácií vyplňte Časť 1 a Časť 2 formulárov Opis knižnice.
- Vo vašich formulároch Individuálny užívateľský profil vyplňte polia **Vlastník vytvorených objektov** a **Skupinové oprávnenie na vytvorené objekty**.
- Vo vašom formulári Názvové konvencie opíšte, ako plánujete pomenovať autorizačné zoznamy.
- Vypracujte formuláre Autorizačný zoznam.
- Informácie o autorizačnom zozname pridajte do vašich formulárov Opis knižnice.
- Vypracujte formulár Bezpečnosť výstupného frontu a pracovných staníc.

Teraz môžete začať plánovať inštaláciu vašich aplikácií.

Plánovanie inštalácie vašich aplikácií

Aby ste mohli skončiť plánovanie zabezpečenia prostriedkov musíte sa pripraviť na inštaláciu vašich aplikácií. Nasledujúce témy vám pomôžu naplánovať vlastníctvo a oprávnenie na vaše aplikácie po ich nainštalovaní. Metódy, ktoré sú v nich opísané, nemusia však fungovať pre všetky aplikácie. Poraďte sa s vaším programátorom alebo poskytovateľom aplikácií, ktorí vám pomôžu vypracovať kvalitný plán inštalácie.

Ak plánujete získať aplikáciu od poskytovateľa aplikácií, použite tieto informácie na naplánovanie bezpečnostných krokov, ktoré musíte vykonať pred a po načítaní knižníc aplikácií.

Ak plánujete nainštalovať aplikáciu, ktorú vyvinuli programátori vo vašom vlastnom systéme, použite tieto informácie na naplánovanie bezpečnostných krokov, potrebných na preradenie aplikácie z testovacieho do produkčného stavu.

Týmito krokmi prejdite s jednou aplikáciou. Potom sa vráťte a vypracujte formuláre Inštalácia aplikácií pre všetky ďalšie aplikácie.

Aké formuláre sa vyžadujú ?

Urobte si kópiu nasledujúcich formulárov a vyplňte ju, keď budete prechádzať touto témou:

Tabuľka 56. Plánovacie formuláre, potrebné k plánovaniu inštalácie aplikácií

Názov formulára	Potrebný počet kópií

Tabuľka 56. Plánovacie formuláre, potrebné k plánovaniu inštalácie aplikácií (pokračovanie)

Formulár Inštalácia aplikácií	Jedna na každú aplikáciu

Ak chcete zhromaždiť informácie k plánovaniu inštalácie aplikácií, použite tieto formuláre, na ktorých ste už predtým pracovali:

Názov formulára	**Vypracovaný v:**
Formulár Opis knižnice	Opísanie informácií o knižnici
Formulár Autorizačný zoznam	Zoskupovanie objektov

V téme Načítavanie vašich aplikácií sa dozviete, ako sa vykonávajú kroky, potrebné pre nainštalovanie vašich aplikácií.

Ak chcete plánovať inštalácie vašich aplikácií, pozrite si tieto témy:

- Určenie užívateľských profilov a inštalačných hodnôt pre aplikácie.
- Zmena inštalačných hodnôt.

Určenie užívateľských profilov a inštalačných hodnôt pre aplikácie

Keď plánujete inštaláciu vašich aplikácií, musíte najprv určiť užívateľské profily a inštalačné hodnoty pre každú aplikáciu. Pred nainštalovaním aplikácie, vytvorenej v inom systéme, budete pravdepodobne musieť vytvoriť jeden alebo viac užívateľských profilov. Užívateľský profil, ktorý vlastní knižnice aplikácií a objekty, musí existovať vo vašom systéme už pred načítaním týchto knižníc do tohto systému. Do formulára Inštalácia aplikácií si zaznamenajte profily, ktoré potrebujete vytvoriť pre každú knižnicu a parametre, ktoré tieto profily potrebujú.

Ak chcete zistiť potrebné inštalačné hodnoty, položte vášmu programátorovi alebo poskytovateľovi aplikácií nasledujúce otázky a ich odpovede si zaznačte do formulára Inštalácia aplikácií:

- Ktorý profil vlastní knižnicu aplikácií ?
- Ktorý profil vlastní objekty v tejto knižnici ?
- Aké je verejné oprávnenie na túto knižnicu (AUT)?
- Aké je verejné oprávnenie na nové objekty (CRTAUT)?
- Aké je verejné oprávnenie na objekty v tejto knižnici ?
- Ktoré programy (pokiaľ existujú) si osvojujú oprávnenie vlastníka ?

Zistite, či vaši programátori alebo poskytovateľ aplikácií vytvorili pre túto aplikáciu nejaké autorizačné zoznamy. Pre každý vytvorený autorizačný zoznam vypracujte formulár Autorizačný zoznam, alebo požiadajte vášho programátora o informácie k tomuto zoznamu.

Môžete sa rozhodnúť, či budete meniť inštalačné hodnoty.

Zmena inštalačných hodnôt pre aplikácie

Informácie z vášho formulára Inštalácia aplikácií porovnajte s vaším plánom zabezpečenia prostriedkov pre knižnicu vo formulári Opis knižnice. Ak sa odlišujú, musíte sa rozhodnúť, aké zmeny treba urobiť po nainštalovaní aplikácie.

Zmena vlastníctva aplikácie

Ak váš programátor alebo poskytovateľ aplikácie vytvoril zvláštny profil na vlastnenie knižníc aplikácií a objektov, pouvažujte o používaní tohto profilu, aj keď nie je v zhode s vašimi názvovými konvenciami. Prenos vlastníctva objektov môže dlho trvať a treba sa mu vyhnúť.

Ak jeden zo skupinových profilov dodaných spoločnosťou IBM, napríklad QSECOFR alebo QPGMR, vlastní aplikáciu, po nainštalovaní tejto aplikácie by ste mali vlastníctvo preniesť na iný profil.

Programátori niekedy navrhujú aplikácie tak, aby sa predišlo zmenám vo vlastníctve objektu. Pokúste sa pracovať v rámci týchto obmedzení a napriek tomu spĺňajte vaše vlastné požiadavky na manažovanie bezpečnosti. Ak však profil dodaný spoločnosťou IBM, napríklad QSECOFR, vlastní aplikáciu, musíte s vaším programátorom alebo poskytovateľom aplikácií vypracovať plán na zmenu vlastníctva. V ideálnom prípade by ste mali vlastníctvo zmeniť pred nainštalovaním aplikácie.

Zmena verejného oprávnenia

Keď ukladáte objekty, ukladáte s nimi aj ich verejné oprávnenie. Keď obnovujete knižnicu aplikácií na váš systém, táto knižnica a všetky jej objekty budú mať rovnaké verejné oprávnenia, aké mali v čase svojho uloženia. Platí to aj v prípade, ak ste knižnicu uložili do iného systému.

Hodnota CRTAUT pre knižnicu (verejné oprávnenie na nové objekty) nemá vplyv na objekty, ktoré sa obnovujú. Obnovujú sa so svojím uloženým verejným oprávnením bez ohľadu na hodnotu CRTAUT pre túto knižnicu.

Verejné oprávnenie na knižnice a objekty by ste mali zmeniť tak, aby bolo v zhode s vaším plánom vo formulári Opis knižnice.

Keď plánujete inštaláciu vašich aplikácií, pravdepodobne si budete chcieť pozrieť príklad, v ktorom sa dozviete, ako Sharon Jones zo spoločnosti JKL Toy Company plánovala inštaláciu aplikácií.

Ak chcete mať istotu, že ste inštaláciu vašich aplikácií naplánovali kompletne, urobte nasledovné:

- Dokončite vyplňovanie vášho úvodného formulára Inštalácia aplikácií. Potom sa vráťte a vypracujte formuláre pre každú ďalšiu aplikáciu.
- Skontrolujte všetky vaše formuláre a presvedčte sa, že sú kompletné. Z vašich formulárov si urobte kópie a kým nenainštalujete váš systém a licenčné programy, uschovajte si ich na bezpečnom mieste.

Po dokončení týchto úloh plánovania môžete začať nastavovať bezpečnosť vašich užívateľov.

Príklad: Formulár inštalácie aplikácie spoločnosti JKL Toy: Spoločnosť JKL Toy si kúpila aplikácie Zákaznícke objednávky a Pohľadávky od poskytovateľa aplikácií. Najala si externého programátora na vývoj aplikácie Kontrakty a tvorba cien a na jej prepojenie s aplikáciou Zákaznícke objednávky.

Sharon Jones použila informácie zo svojich formulárov opisu knižnice na prípravu formulára inštalácie aplikácie. Nasledujúca tabuľka ukazuje exemplár Sharoninho formulára opisu knižnice pre CUSTLIB: (Pozrite si tému ″Opis knižničných informácií.″)

Tabuľka 57. Formulár opisu knižnice spoločnosti JKL Toy: príklad

Formulár opisu knižnice	**1. časť z 2**
Pripravil: Sharon Jones	Dátum: 9/9/99
Názov knižnice: CUSTLIB	Opisný názov (text): Knižnica zákazníckych záznamov
Stručne opíšte funkciu tejto knižnice: Obsahuje všetky zákaznícke súbory, vrátane objednávok a účtov.	
Definujte ciele zabezpečenia pre knižnicu, napríklad či sú určité informácie dôverné: `V súčasnosti dovoľujeme každému v spoločnosti prezerať si zákaznícke objednávky. Pre ochranu presnosti informácií by sme mali obmedziť, komu bude povolené meniť ich.`	
Verejné oprávnenie pre knižnicu: *USE Verejné oprávnenie pre objekty v knižnici: *CHANGE Verejné oprávnenie pre nové objekty (CRTAUT): *CHANGE Vlastník knižnice: OWNAR	

Nasledujúca tabuľka ukazuje formulár inštalácie aplikácie, ktorý Sharon pripravila pre aplikáciu Zákaznícke objednávky. Všimnite si, že Sharon sa rozhodla použiť profil vlastníka vytvorený poskytovateľom aplikácie. Profil COWNER bude vlastniť aj súbor, aj knižnice programov.

Po nainštalovaní aplikácie by Sharon mala urobiť nasledovné:

- Zmeniť verejné oprávnenia pre knižnice, aby zodpovedali plánu zabezpečenia prostriedkov v jej formulároch opisu knižnice.
- Zmeniť užívateľskú triedu profilu COWNER na *USER a odstrániť všetky mimoriadne oprávnenia.
- Zmeniť heslo profilu COWNER na *NONE.

Tabuľka 58. Formulár inštalácie aplikácie spoločnosti JKL Toy: príklad

Názov aplikácie: Zákaznícke objednávky (CO)		Opis: Vkladá, sleduje a posiela objednávky.
Vypíšte a vysvetlite všetky profily, ktoré musia byť vytvorené pre inštaláciu aplikácie: Knižnica obsahujúca súbory je vlastnená profilom s názvom COWNER. Knižnicu programov vlastní QPGMR.		
Názov knižnice: CUSTLIB		
	Pred inštaláciou	**Po inštalácii**
Vlastník knižnice	COWNER	COWNER
Vlastník objektu	COWNER	COWNER
Verejné oprávnenie pre knižnicu	*EXCLUDE	*USE
Verejné oprávnenie pre objekt	*ALL	*CHANGE
Verejné oprávnenie pre nové objekty	*CHANGE	*CHANGE
Názov knižnice: COPGMLIB		
	Pred inštaláciou	**Po inštalácii**
Vlastník knižnice	QPGMR	COWNER
Vlastník objektu	QPGMR	COWNER
Verejné oprávnenie pre knižnicu	*EXCLUDE	*USE
Verejné oprávnenie pre objekt	*ALL	*CHANGE
Verejné oprávnenie pre nové objekty	*CHANGE	*CHANGE

Teraz keď ste dokončili úlohy plánovania, ste pripravený nastaviť užívateľské zabezpečenie.

Nastavenie užívateľského zabezpečenia

Táto téma vás prevedie úlohami, ktoré sú potrebné na nastavenie užívateľského zabezpečenia vo vašom systéme, pomocou rozhrania príkazového riadka. Ak nastavujete nový systém, tieto kroky by ste mali vykonať postupne jeden po druhom. Systém používa informácie z každého vykonaného kroku pre nasledujúci krok. Ak chcete nastaviť základné zabezpečenie systému, musíte dokončiť dve sady úloh. Po prvé musíte definovať svoje užívateľské zabezpečenie a po druhé musíte chrániť svoje prostriedky v systéme. Dve tabuľky nižšie zvýrazňujú každý krok, ktorý musíte nakonfigurovať, aby ste nastavili užívateľské zabezpečenie a zabezpečenie prostriedkov.

Poznámka: **MUSÍTE** najprv dokončiť všetky kroky na nastavenie užívateľského zabezpečenia a až potom môžete začať nastavovať zabezpečenie prostriedkov.

Tabuľka 59. Kroky na nastavenie užívateľského zabezpečenia

Krok	Čo sa robí v tomto kroku	Aké formuláre použijete
Nastavenie vášho celkového prostredia	Nastavte úvodné systémové hodnoty a sieťové atribúty. Vytvorte užívateľský profil správcu bezpečnosti.	formulár Výber systémových hodnôt
Nastavenie systémových hodnôt pre zabezpečenie	Nastavte ďalšie systémové hodnoty.	formulár Výber systémových hodnôt
Príprava krokov základného zabezpečenia na zavedenie vašich aplikácií	Vytvorte profily vlastníkov. Zaveďte svoje aplikácie. Knižnice a objekty aplikácií by mali byť v systéme ešte predtým, ako dokončíte zostávajúce kroky.	formulár Inštalácia aplikácií
Nastavenie skupín užívateľov	Vytvorte opisy úloh, knižnice skupín a skupinové profily.	formulár Opis skupín užívateľov
Nastavenie konkrétnych užívateľov	Vytvorte konkrétne knižnice a užívateľské profily.	formulár Konkrétny užívateľský profil

Tabuľka 60. Kroky na nastavenie zabezpečenia prostriedkov

Krok	Čo sa robí v tomto kroku	Aké formuláre použijete
Nastavenie vlastníckeho a verejného oprávnenia	Vytvorte vlastnícke a verejné oprávnenie pre knižnice a objekty.	formulár Inštalácia aplikácií
Vytvorenie autorizačného zoznamu	Vytvorte autorizačné zoznamy.	formulár Autorizačný zoznam
Nastavenie špecifických oprávnení	Nastavte prístup do knižníc a na konkrétne objekty.	formulár Opis knižníc
Zabezpečenie tlačového výstupu	Ochrana tlačového výstupu pomocou vytvorenia výstupných frontov a pridelenia výstupu.	formulár Výstupný front a zabezpečenie pracovnej stanice
Zabezpečenie pracovných staníc	Ochrana pracovných staníc.	formulár Výstupný front a zabezpečenie pracovnej stanice

Okrem tém, ktoré sú uvedené v tabuľke vyššie si pozrite nasledujúce témy pre správu zabezpečenia vášho systému:

- Testovanie zabezpečenia.
- Zmena bezpečnostných informácií.
- Ukladanie bezpečnostných informácií.
- Monitorovanie zabezpečenia.

Predtým, ako začnete

Ak inštalujete nový systém, predtým ako začnete nastavovať zabezpečenie, vykonajte nasledovné:

- Presvedčte sa, či je vaša systémová jednotka a vaše zariadenia nainštalované a či správne fungujú. Ak neplánujete použiť pomenúvanie iSeries pre vaše zariadenia, počkajte na pripojenie vašich pracovných staníc a tlačiarní, kým nezmeníte systémovú hodnotu, ktorá určuje ako budú zariadenia pomenúvané (QDEVNAMING). Používanie nových systémových hodnôt vám povie, kedy máte zariadenia pripojiť.
- Zaveďte všetky licenčné programy, ktoré plánujete použiť.

Nastavenie vášho celkového prostredia

Ak chcete začať nastavovať užívateľské zabezpečenie, musíte nastaviť celkové prostredie pre svojich užívateľov. Na nastavenie systémových hodnôt a vytvorenie svojho vlastného užívateľského profilu v tejto téme použite Ponuka NASTAVENIE. Zmeňte aj užívateľské ID a heslá pre profily DST (Dedicated Service Tools).

V nasledujúcich pokynoch nájdete príklady obrazoviek príkazového riadka, ktoré tieto kroky vysvetľujú. Neukazujú však celú obrazovku. Ukazujú iba informácie, ktoré sú potrebné na splnenie úlohy.

Aké formuláre sú potrebné?

Informácie zadajte z formulára Výber systémových hodnôt, ktoré ste si pripravili v ″Stratégii plánovania svojej celkovej bezpečnosti.″

Ak chcete nastaviť svoje celkové prostredie, musíte dokončiť tieto úlohy:

1. Prihlásenie do systému.
2. Vybratie správnej úrovne pomoci.
3. Zamedzenie prihlásenia ostatných užívateľov.
4. Zadanie systémových hodnôt pre zabezpečenie.
5. Použitie nových systémových hodnôt.
6. Vytvorenie profilu správcu bezpečnosti

Keď dokončíte vyššie uvedené kroky, musíte zmeniť heslá pre servisné nástroje, aby ich niekto iný nemohol nevhodne používať. Pozrite si detaily v časti Servisné nástroje.

Prihlásenie do systému

Ak chcete začať nastavovať svoje systémové prostredie, musíte sa prihlásiť do systému.

1. V konzole sa prihláste ako správca bezpečnosti (QSECOFR). Ak sa prihlasujete po prvýkrát, použite heslo QSECOFR. Pretože systém odosiela toto heslo ako po uplynutí platnosti, systém vás vyzve, aby ste toto heslo zmenili. Ak sa chcete úspešne prihlásiť musíte toto heslo zmeniť.
2. Na prihlasovacej obrazovke zadajte do poľa *Ponuka* hodnotu SETUP.

Poznámka: Ponuka NASTAVENIE sa nazýva Prispôsobte ponuku vášho systému, užívateľov a zariadenia. Tento text na to všade odkazuje ako na Ponuka NASTAVENIE.

```
                Prihlásenie
                            Systém  . . . . .
                            Podsystém . . . .
                            Obrazovka . . . .

Užívateľ  . . . . . . . . . . .   QSECOFR
Heslo     . . . . . . . . . . .   _________
Program/procedúra . . . . . . .   _________
Ponuka  . . . . . . . . . . . .   SETUP
Aktuálna knižnica . . . . . . .   _________
```

Po prihlásení sa do systému si musíte vybrať príslušnú úroveň pomoci.

Vybratie správnej úrovne pomoci

Po prihlásení sa do systému si môžete zvoliť príslušnú úroveň pomoci pre užívateľov. **Úroveň pomoci** určuje verziu obrazovky, ktorú uvidíte. Mnohé systémové obrazovky majú dve rôzne verzie:

- Verziu základná úroveň asistencie, ktorá obsahuje menej informácií a nepoužíva technickú terminológiu.
- Verziu stredná úroveň asistencie, ktorá ukazuje viac informácií a používa technické výrazy.

Niektoré polia alebo funkcie sú dostupné iba v určitých verziách obrazovky. Pokyny vám povedia, ktorú verziu máte použiť. Ak chcete zmeniť jednu úroveň pomoci na inú, použite tlačidlo **F21** (Výber úrovne pomoci). **F21** nie je dostupné zo všetkých obrazoviek.

Keď si vyberiete svoju úroveň pomoci, musíte zamedziť ostatným, aby sa neprihlásili do systému, pokiaľ budete nastavovať zabezpečenie.

Zamedzenie prihlásenia ostatných užívateľov

Po vybratí správnej úrovne pomoci musíte zamedziť, aby sa nikto iný neprihlásil do systému. Ak sa obávate, že by užívatelia mohli nedovolene manipulovať s vašim systémom predtým, ako ho budete môcť zabezpečiť, môžete na inej pracovnej stanici zamedziť tomu, aby sa nikto iný neprihlásil. Je to voliteľné. Urobte iba v prípade, keď máte pocit, že je potrebné dočasné zabezpečenie:

1. V ponuke NASTAVENIE stlačte **F9**, aby sa zobrazil príkazový riadok
2. Do príkazového riadka napíšte GO DEVICESTS.
3. Potom sa na obrazovke objaví ponuka Úlohy stavu zariadenia. Ak uvidíte ponuku Pracovať so stavom konfigurácie, použite **F21** (Výber úrovne pomoci) na prechod do základnej úrovne asistencie.
4. Vyberte voľbu **1** (Pracovať so zobrazovacími zariadeniami).
5. Na obrazovke Pracovať so zobrazovacími zariadeniami, zneprístupnite všetky pracovné stanice, s výnimkou tej, ktorú práve používate. Urobíte to, keď pred názov každej pracovnej stanice napíšete **2** a stlačíte kláves **Enter**.
6. Vráťte sa do ponuky NASTAVENIE tak, že dvakrát stlačíte **F3** (Ukončiť).
7. Stlačte **F12** (Zrušiť), ak chcete odstrániť príkazový riadok.

```
                          Pracovať so zobr. zariadeniami

Zadajte voľby, stlačte kláves Enter.
  1=Sprístupniť       2=Zneprístupniť     5=Zobraziť
  7=Zobraziť správu   8=Pracovať s radičom a riadkom
  13=Zmeniť opis

Voľ  Zariadenie  Typ     Stav
__   DSP01       3196    QSECOFR
2_   DSP02       3196    Dostupné pre použitie
2_   DSP03       3196    Dostupné pre použitie
2_   DSP04       3196    Dostupné pre použitie
```

Keď zariadenie zneprístupníte, nebude mať prihlasovaciu obrazovku, a to ani vtedy, keď bude zapnuté. Pracovné stanice zostanú neprístupné iba dovtedy, kým svoj systém nezastavíte a znova nespustíte. Možno budete musieť tento krok zopakovať.

Keď zamedzíte, aby sa do systému nemohol prihlásiť nikto iný, môžete zadať systémové hodnoty pre zabezpečenie.

Zadanie systémových hodnôt pre zabezpečenie

Keď ste iným užívateľom zamedzili prihlásiť sa, potrebujete do systému zadať systémové hodnoty.

Informácie z vášho formulára Výber systémových hodnôt Časť 1 zadajte podľa tohto postupu:

1. Z ponuky NASTAVENIE vyberte voľbu **1** (Zmeniť systémové voľby).
2. Informácie z vášho formulára Výber systémových hodnôt zadajte na obrazovke Zmeniť systémové voľby. Ak na obrazovke nechcete zmeniť niektorú z volieb, na jej preskočenie použite kláves Tab.
3. Na obrazovke zadajte správny dátum a čas, ak neboli nastavené pri spustení systému.
4. Keď zadáte informácie na tejto stránke, prejdite o stránku nižšie na nasledujúcu stránku. Nápis *Viac...* v spodnom ľavom rohu obrazovky znamená, že obrazovka obsahuje ešte aspoň jednu stránku.

```
                          Zmeniť systémové voľby
Systém:
Zadajte voľby, stlačte kláves Enter.

Názov systému . . . . . .   JKLTOY     Názov

Voľby dátumu a času:
  Systémový dátum . . . . . .   09/21/99     MM/DD/RR
  Systémový čas . . . . . . .   10:52:57     HH:MM:SS
  Oddeľovač dátumu  . . . . .   1            1=/
                                             2=-
                                             3=.
                                             4=,
                                             5=prázdny znak
  Formát dátumu   . . . . . .   MDR          RMD, MDR, DMR, JUL
  Oddeľovací znak času  . . .   1            1=:
                                             2=.
                                             3=,
                                             4=prázdny znak


                                                                  Viac...
F1=Pomoc   F3=Ukončiť   F5=Obnoviť   F12=Zrušiť
```

5. Napíšte svoje voľby na druhú stránku obrazovky a prejdite o stránku nižšie.

```
                          Zmeniť systémové voľby

Zadajte voľby, stlačte kláves Enter.

Voľby zabezpečenia:
  Úroveň zabezpečenia . . . . .   40
   :
  Povoliť správcom bezpečnosti
    prihlásenie na ľubovoľnú pracovnú
    stanicu . . . . . .   N
```

6. Napíšte svoje voľby na tretiu stránku obrazovky a stlačte kláves **Enter**.

```
                          Zmeniť systémové voľby

Zadajte voľby, stlačte kláves Enter.

Voľby zariadenia:
  Formát názvov zariadení pre nové
  zariadenia . . . . . .   1


  štandardná systémová tlačiareň . . . . . PRT01

Ďalšie voľby:
  Dať užívateľov do prostredia S/36
    pri prihlásení . . . . . .   N
  Uložiť informácie o evidencií
    úloh pre hotový tlačový
    výstup . . . . . .   Y
```

7. Znova by ste mali vidieť Ponuka NASTAVENIE. Všimnite si správu v spodnej časti obrazovky: **Systémové voľby boli úspešne zmenené. Vyžaduje sa IPL**.

   Poznámka: Systém vyžaduje IPL iba vtedy, ak ste zmenili úroveň zabezpečenia.

Na konci väčšiny tém o systémových úlohách nájdete tabuľku, ktorá opisuje možné chyby a kroky nápravy. Tieto tabuľky si vezmite na pomoc, ak sa vaše výsledky líšia od tých popísaných. V týchto tabuľkách nemusíte nájsť riešenie každého problému. zámerom týchto tabuliek je poskytnúť návod na riešenie problémov a spríjemniť vám používanie vášho systému.

Možná chyba	Obnova
Je zobrazená ponuka MAIN.	Stlačili ste **F3** (Ukončiť) alebo **F12** (Zrušiť). Napíšte GO SETUP a skúste znova.
Vidíte ďalšiu obrazovku, ako napríklad obrazovka Zmeniť voľby vymazania.	Z ponuky NASTAVENIE ste vybrali nesprávnu položku. Stlačte **F3** (Ukončiť), aby ste sa vrátili do ponuky a skúste to znova.
Po stlačení klávesu **Enter** sa znova objaví obrazovka Zmeniť systémové voľby.	Na konci obrazovky vyhľadajte chybové hlásenie. Pravdepodobne ste zadali hodnotu, ktorá nie je povolená. Ak potrebujete viac informácií nezabudnite použiť **F1** (Pomoc). Ak chcete, aby systém obnovil všetky hodnoty na také, ako boli pôvodne, predtým ako ste začali písať, použite **F5** (Obnoviť). Skúste to ešte raz.
Predtým, ako ste na obrazovke napísali všetky svoje voľby ste stlačili kláves **Enter**.	Túto obrazovku môžete použiť toľkokrát, koľkokrát je na zmenenie systémových hodnôt potrebné. Z Ponuka NASTAVENIE vyberte voľbu **1** a zadajte hodnoty, ktoré ste nestihli zadať prvýkrát. **Upozornenie: Akonáhle je váš systém v prevádzke, nemeňte úroveň zabezpečenia bez porady s programátorom. Rovnako, nemeňte názov systému, ak požívate iSeries Access alebo komunikujete s iným počítačom.**
Namiesto posunu o stránku nižšie ste stlačili kláves **Enter**.	Z Ponuka NASTAVENIE vyberte voľbu **1** a posuňte sa o stránku nižšie, aby sa zobrazila druhá stránka. Napíšte svoje voľby a stlačte kláves **Enter**.

Po zadaní vašich systémových hodnôt musíte následne nové systémové hodnoty použiť.

Použitie nových systémových hodnôt

Po zadaní vašich systémových hodnôt musíte použiť niektoré z týchto hodnôt. Väčšina zmien v systémových hodnotách sa prejaví okamžite. Keď ste však zmeníte úroveň zabezpečenia svojho systému, zmena sa neprejaví, pokiaľ svoj systém nezastavíte a znova ho nespustíte. Keď si overíte, či ste na obrazovke Zmeniť systémové voľby napísali všetky zmeny správne, ste pripravený použiť nové hodnoty.

Poznámka: Pripojte k systému svoje pracovné stanice, ak ste to ešte neurobili. Keď systém spustíte, automaticky nakonfiguruje tie zariadenia, ktoré používajú formát názvov, ktorý ste vybrali na obrazovke Zmeniť systémové voľby.

Nasledujúci postup použite na zastavenie svojho systému a na jeho opätovné spustenie. Keď sa váš systém spustí, začnú platiť hodnoty, ktoré ste zadali na obrazovke Zmeniť systémové voľby.

1. Presvedčte sa, či ste sa prihlásili na konzole a či nie sú prihlásené nejaké iné pracovné stanice.
2. Presvedčte sa, či uzamykateľný vypínač na procesorovej jednotke vo svojej Normálnej polohe.
3. Z Ponuka NASTAVENIE vyberte voľbu pre Úlohy zapínania a vypínania.
4. Vyberte voľbu pre okamžité vypnutie systému a jeho následné zapnutie. Stlačte kláves **Enter**.
5. Systém ukáže obrazovku, ktorá požaduje, aby ste potvrdili svoju požiadavku na vypnutie. Stlačte **F16** (Potvrdiť).

To spôsobí, že systém sa zastaví, a potom sa opäť automaticky spustí. Vaša obrazovka bude pár minút prázdna. potom by ste mali znova uvidieť prihlasovaciu obrazovku.

Po použití vašich nových systémových hodnôt musíte pre seba vytvoriť profil správcu bezpečnosti v systéme.

Vytvorenie profilu správcu bezpečnosti

Správca bezpečnosti je v systéme ľubovoľný užívateľ s triedou užívateľov *SECOFR alebo so špeciálnymi oprávneniami *ALLOBJ a *SECADM.

Keď použijete systémové hodnoty z obrazovky Zmeniť systémové voľby, vytvorte užívateľský profil pre seba a pre náhradného správcu bezpečnosti. Keď budete v budúcnosti vykonávať funkcie správcu bezpečnosti uprednostnite používanie svojho profilu pred používaním profilu QSECOFR.

1. Do systému sa prihláste ako QSECOFR a požadujte Ponuka NASTAVENIE.

   Všimnite si, že názov systému, ktorý ste si zvolili sa objaví vyššie vpravo na prihlasovacej obrazovke.

```
                  Prihlásenie
                              Systém  . . . . .
                              Podsystém . . . .
                              Obrazovka . . . .

Užívateľ  . . . . . . . . . . .   QSECOFR
Heslo     . . . . . . . . . . .   _________
Program/procedúra . . . . . . .   _________
Ponuka  . . . . . . . . . . . .   SETUP
Aktuálna knižnica . . . . . . .   _________
```

2. Z ponuky NASTAVENIE vyberte voľbu *Pracovať so zaradením užívateľa*. Obrazovka Pracovať so zaradením užívateľa uvádza profily, ktoré sú aktuálne vo vašom systéme.

   Poznámka: Ak vidíte obrazovku Pracovať s užívateľským profilom, stlačte **F21** (Vybrať úroveň pomoci) a prejdite na základná úroveň asistencie.

3. Ak chcete vytvoriť nový profil, napíšte **1** (Pridať) do stĺpca *Vol* (voľba) a názov vášho profilu napíšte do stĺpca *Užívateľ*. Stlačte kláves **Enter**.

```
                          Pracovať so zaradením užívateľa

Zadajte voľby, stlačte kláves Enter.
  1=Pridať   2=Zmeniť   3=Kopírovať   4=Odstrániť   5=Zobraziť

Vol     Užívateľ          Opis
1       JONESS
QDOC                           Užívateľský profil dokumentov
QSECOFR                        Užívateľský profil správcu bezpečnosti
```

4. Na obrazovke Pridať užívateľa si priraďte heslo.
5. Do polí, ktoré sú zobrazené na vzorovej obrazovke, doplňte svoje vlastné príslušné informácie.
6. Posuňte sa o stránku nižšie na nasledujúcu stránku obrazovky.

```
                          Pridať užívateľa

Zadajte voľby, stlačte kláves Enter.

Užívateľ  . . . . . .   JONESS
Opis užívateľa . . . . .  Jones, Sharon
Heslo . . . . . .   secret
Typ užívateľa . . . . .   *SECOFR
Skupina užívateľov  . . .   *NONE

Obmedziť použitie príkazového riadka   _____
Štandardná knižnica . . .
Štandardná tlačiareň  . .   *WRKSTN
Prihlasovací program  . .   *NONE
Knižnica  . . . . . .

Prvá ponuka . . . . . .
Knižnica  . . . . . .
```

7. Vyplňte druhú stránku obrazovky a stlačte kláves **Enter**.
8. Skontrolujte potvrdzovacie správy na konci obrazovky Pracovať so zaradením užívateľa.
9. Stlačte **F3** (Ukončiť) pre návrat do Ponuka NASTAVENIE.

```
                          Pridať užívateľa

Zadajte voľby, stlačte kláves Enter.

Program klávesu Attention. .   *SYSVAL
  Knižnica  . . . . . .
```

Možná chyba	Obnova
Kláves **Enter** ste stlačili skôr ako ste napísali informácie do všetkých polí.	Voľbu *Zmeniť* na obrazovke Pracovať so zaradením užívateľa použite na zmenu profilu, ktorý ste práve vytvorili. Ak sa profil neobjaví na zozname, stlačte **F5** (Obnoviť) a posuňte sa o stránku nižšie, aby ste ho našli.

Keď pre seba vytvoríte profil správcu bezpečnosti, musíte zmeniť užívateľské ID a heslá pre užívateľov servisných nástrojov. V informačnom centre si pozrite tému Servisné nástroje.

Nastavenie systémových hodnôt pre zabezpečenie

V tejto téme použite príkaz WRKSYSVAL (Work with System Values) na zmenu a zobrazenie systémových hodnôt.

Aké formuláre sú potrebné?

Informácie zadajte z formulára Výber systémových hodnôt, ktoré ste si pripravili v ″Stratégii plánovania svojej celkovej bezpečnosti.″

Ak chcete nastaviť svoje systémové hodnoty, dokončite tieto úlohy:

1. Zmena systémových hodnôt zabezpečenia.
2. Zmena konkrétnych systémových hodnôt.

Prihláste sa do rozhrania príkazového riadka

Na prihlásenie do systému použite tieto informácie:

Profil Váš vlastný (vyžaduje sa oprávnenie *SECADM a *ALLOBJ)

Ponuka
MAIN

Po prihlásení môžete začať meniť systémové hodnoty zabezpečenia.

Zmena systémových hodnôt zabezpečenia

Po prihlásení sa do systému použite tento postup na zadanie systémových hodnôt zabezpečenia, ktoré sa objavia v Časti 2 vášho formulára Výber systémových hodnôt.

1. Do príkazového riadka napíšte WRKSYSVAL *SEC a stlačte kláves **Enter**. *SEC za názvom príkazu znamená, že chcete vidieť iba tie systémové hodnoty, ktoré sa týkajú zabezpečenia.
2. Na obrazovke Pracovať so systémovými hodnotami napíšte voľbu **2** (Zmeniť) do stĺpca *Voľba* pred systémovú hodnotu, ktorú chcete zmeniť. Ak sa systémová hodnota, ktorú chcete zmeniť neobjaví na obrazovke, posúvajte sa o stránku nižšie, kým ju nenájdete.

```
                          Pracovať so systém. hodnotami

Premiestniť na . . . . .              Začiatočný znak
Podmnožina podľa typu  .   *SEC       F4 výber zo zoznamu

Napíšte voľby, stlačte kláves Enter.
  2=Zmeniť   5=Zobraziť

        Systém
Voľba   Hodnota      Typ         Opis
        QINACTMSGQ   *SEC        Front správ neaktívnej úlohy
2       QLMTDEVSSN   *SEC        Limit relácií zariadenia
        QLMTSECOFR   *SEC        Limit zariadenia správcu bezpečnosti
        QMAXSGNACN   *SEC        Akcia, ktorá sa má vykonať pri zlyhaní
  ⋮
```

3. Napíšte vašu voľbu pre systémovú hodnotu a stlačte kláves **Enter**. Na displeji sa znova zobrazí obrazovka Pracovať so systémovými hodnotami.

```
                            Zmeniť systémovú hodnotu
Systémová hodnota  . . :    QLMTDEVSSN
Opis  . . . . . . . . :     Limit relácií zariadenia


Napíšte voľbu, stlačte kláves Enter.

  Limit relácií zariadenia . .   0          0=Nie
                                            1=Áno
```

4. Skontrolujte potvrdzovaciu správu na konci obrazovky.

Možná chyba	Obnova
Vidíte iné systémové hodnoty, ako tie, ktoré sa zobrazili v príklade obrazovky Pracovať so systémovými hodnotami.	Zabudli ste napísať *SEC. Porovnajte pole *Podmnožina podľa typu* na začiatku vašej obrazovky so vzorovou obrazovkou. Presuňte kurzor do poľa *Podmnožina podľa typu*. Napíšte *SEC a stlačte kláves **Enter**.
Systém nespracoval váš príkaz. Naďalej vidíte ponuku.	Skontrolujte chybové hlásenia na konci svojej obrazovky. Pravdepodobne ste nesprávne napísali názov príkazu. Skúste to ešte raz. Ak sa v správa uvádza, že nie ste autorizovaný, odhláste sa a znova sa prihláste s použitím profilu, ktorý má oprávnenie správcu bezpečnosti.

Možná chyba	Obnova
Obrazovka Zmeniť systémovú hodnotu sa znovu objaví, keď stlačíte kláves **Enter**.	Skontrolujte, či na konci obrazovky nie sú chybové hlásenia. Pravdepodobne ste nesprávne napísali svoje voľby, alebo ste vybrali hodnotu, ktorá bola mimo povoleného rozsahu. Ďalšie informácie získate po stlačení **F1** (Pomoc).
Namiesto obrazovky Práca so systémovými hodnotami vidíte ponuku.	Pravdepodobne ste dvakrát stlačili kláves **Enter**. Napíšte WRKSYSVAL *SEC.
Vybrali ste systémovú hodnotu, ktorú nechcete zmeniť.	Stlačte **F12** (Zrušiť) pre návrat na obrazovku Pracovať so systémovými hodnotami.

Čo znamená * (hviezdička)?

Pravdepodobne ste si všimli, že niektoré hodnoty majú pred sebou hviezdičku (*). Systém používa hviezdičku, aby vyjadril rozdiel medzi špeciálnymi hodnotami a normálnymi slovami. Napríklad, keď zadáte, že heslo v užívateľskom profile má hodnotu *NONE, znamená to, že systém nikomu nedovolí prihlásiť sa s použitím tohto profilu. Ak zadáte, že heslo je NONE, užívateľ musí ako heslo napísať znaky NONE.

Zatiaľ čo vo svojom systéme nastavujete zabezpečenie, nezabudnite venovať pozornosť používaniu hviezdičky v inštrukciách a vo formulároch.

Keď ste zmenili systémové hodnoty zabezpečenia, môžete zmeniť konkrétne systémové hodnoty.

Zmena konkrétnych systémových hodnôt

Keď ste zmenili systémové hodnoty zabezpečenia, môžete zmeniť konkrétne systémové hodnoty.

Napríklad systémová hodnota QDSCJOBITV (interval ukončenia platnosti prerušenej úlohy) nie je zahrnutý ako systémová hodnota zabezpečenia. Neobjaví sa v podmnožine *SEC obrazovky Pracovať so systémovými hodnotami. Tento postup použite na zmenu systémovej hodnoty QDSCJOBITV alebo ľubovoľnej konkrétnej systémovej hodnoty:

1. Napíšte WRKSYSVAL QDSCJOBITV a stlačte kláves **Enter**.
2. Na obrazovke Pracovať so systémovými hodnotami napíšte **2** (Zmeniť) do stĺpca *voľba* pred QDSCJOBITV.
3. Napíšte vašu voľbu pre QDSCJOBITV.
4. Skontrolujte potvrdzovaciu správu.

```
                          Zmeniť systémovú hodnotu
Systémová hodnota  . . :   QDSCJOBITV
Opis  . . . . . . . . :   Interval ukončenia platnosti prerušenej úlohy


Napíšte voľbu, stlačte kláves Enter.

  Interval ukončenia prerušenej úlohy  ..... 300
```

Výpis vašich hodnôt zabezpečenia

Po zadaní všetkých informácií z vášho formulára Výber systémových hodnôt, môžete vytlačiť zoznam všetkých systémových hodnôt zabezpečenia. Napíšte WRKSYSVAL *SEC OUTPUT(*PRINT). Kópiu zoznamu založte do vášho formulára Výber systémových hodnôt. Zoznam znova vytlačte vždy, keď zmeníte systémovú hodnotu zabezpečenia.

Po zadaní všetkých volieb pre systémové hodnoty z formulára Výber systémových hodnôt sa môžete pripraviť na zavedenie svojich aplikácií.

Vykonanie krokov zabezpečenia na zavedenie vašich aplikácií

Po nastavení svojich systémových hodnôt sa môžete pripraviť na zavedenie svojich aplikácií. Táto téma pokrýva kroky zabezpečenia, ktoré sú potrebné na zavedenie vašich aplikačných knižníc do vášho systému. Keď vytvoríte profily a ostatné objekty zabezpečenia, ″Nastavenie vlastníctva a verejného oprávnenia″ a ″Nastavenie zabezpečenia prostriedkov″ ukazuje, ako sa má vytvoriť vlastníctvo a oprávnenie pre vaše aplikácie.

Ak je to možné svoje aplikačné knižnice by ste si mali do systému zaviesť ešte pred nastavením skupín užívateľov a konkrétnych profilov. Keď vytvárate opisy úloh a profily, potrebujete sa pozrieť do aplikačných objektov.

Ak svoje aplikácie nedokážete zaviesť ešte pred vytvorením skupinových a samostatných profilov, môžete dostať varovné správy, ako napríklad tieto:

- Systém nenájde východiskové knižnice, keď vytvoríte opisy úloh.
- Systém nenájde východiskový program alebo ponuku, keď vytvoríte profily.

Opisy úloh a profily nemôžete úspešne otestovať, kým nezavediete svoje aplikačné knižnice.

Použite formuláre Inštalácia aplikácií, ktoré ste si pripravili v ″Plánovaní inštalácie vašich aplikácií.″

Ak chcete zaviesť všetky svoje aplikácie, dokončite tieto úlohy:

1. Vytvorte profil vlastníka.
2. Zaveďte aplikácie.

Prihlásenie do systému

- Ak chcete vytvoriť profily vlastníkov:

  Profil Váš vlastný (vyžaduje sa oprávnenie *SECADM)

  Ponuka
  MAIN
- Ak chcete zaviesť aplikačné knižnice:

  U poskytovateľa vašich aplikácií si overte, či by ste sa mali prihlasovať ako správca bezpečnosti alebo ako vlastník aplikácie, keď zavádzate aplikačné knižnice.

Po prihlásení môžete vytvoriť profil vlastníka pre vaše aplikácie.

Vytvorenie profilu vlastníka

Po prihlásení sa do systému skontrolujte Plán inštalácie aplikácie, aby ste zistili, či potrebujete vytvoriť nejaké profily pred zavedením aplikácií. Ak chcete vytvoriť profil:

1. Napíšte CRTUSRPRF (Create User Profile) a stlačte **F4** (Výzva).
2. Polia na obrazovke Vytvoriť užívateľský profil vyplňte podľa pokynov vášho programátora alebo poskytovateľa aplikácií.
3. Na zobrazenie ďalších polí použite **F10** (Viac polí) a posuňte sa o stránku nižšie.

```
                      Vytvoriť užívateľský profil (CRTUSRPRF)

Napíšte voľby, stlačte kláves Enter.

Užívateľský profil . . . . . >
Užívateľské heslo  . . . . . .   *USRPRF
Nastaviť uplynutie platnosti hesla. .  *NO
Stav   . . . . . .   *ENABLED
Trieda užívateľov  . . . . . .   *USER
Úroveň pomoci    . . . . . .   *SYSVAL
Aktuálna knižnica  . . . . . .   *CRTDFT
Úvodný program, ktorý sa má volať. *NONE
  Knižnica . . . . . .
Úvodná ponuka  . . . . . .   MAIN
  Knižnica . . . . . .    *LIBL
Obmedziť schopnosti  . . . . . .   *NO
Textový 'opis'    . . . . . .   Vlastník xxxxxx
```

4. Skontrolujte, či na konci vašej obrazovky nie sú správy.

Poznámka: Vytváranie skupinového profilu podrobnejšie pojednáva o vytváraní profilov.

Po vytvorení vlastníka pre aplikáciu môžete začať zavádzať svoje aplikácie.

Zavádzanie aplikácií

Postupujte podľa pokynov poskytovateľa vašich aplikácií pre zavádzanie vašich aplikačných knižníc. V téme ″Nastavenie vlastníctva a verejného oprávnenia″ sa dozviete, ako sa nastavuje vlastníctvo a verejné oprávnenie pre aplikácie.

Po zavedení všetkých svojich aplikácií, môžete nastaviť skupiny užívateľov.

Nastavenie skupín užívateľov

Keď vykonáte kroky zabezpečenia na zavedenie vašich aplikácií, môžete nastaviť skupiny užívateľov. Budete vytvárať knižnice skupín, opisy úloh a skupinové profily. Prejdite si celú tému a pracujte iba s jednou z vašich skupín užívateľov, potom sa vráťte na začiatok a postup zopakujte pri iných skupinách. Vzorové obrazovky zobrazujú informácie z formulárov Opis skupiny užívateľov pre oddelenie predaja a marketingu a pre oddelenie skladového hospodárstva v Spoločnosť JKL Toy.

Použite formuláre Opis skupiny užívateľov, ktoré ste si pripravili v ″Plánovaní skupín užívateľov.″

Ak chcete nastaviť skupiny užívateľov, dokončite tieto úlohy:

1. Vytvorte knižnicu pre skupinu užívateľov.
2. Vytvorte opis úlohy.
3. Vytvorte skupinový profil.

Prihlásenie do systému

Profil Váš vlastný (vyžaduje sa oprávnenie *SECADM)

Ponuka
MAIN

Po prihlásení môžete vytvoriť knižnicu pre skupinu užívateľov.

Vytváranie knižnice pre skupinu

Po prihlásení sa do systému potrebujete vytvoriť knižnicu pre skupinu užívateľov. Ak plánujete, že skupiny bude v knižnici zdieľať objekty ktoré si vytvorí, ako napríklad programy Query, knižnicu vytvorte skôr ako vytvoríte skupinový profil:

1. Napíšte CRTLIB (Create Library) a stlačte **F4** (Výzva).
2. Vyplňte obrazovku. Názov knižnice by mal byť názvom skupinového profilu.
3. Stlačte **F10** (Ďalšie parametre).
4. Doplňte verejné oprávnenie pre knižnicu a nové objekty, ktoré sú v knižnici vytvorené.
5. Stlačte kláves **Enter**. Skontrolujte potvrdzovaciu správu.

```
                          Vytvoriť knižnicu

Napíšte voľby, stlačte kláves Enter.

Knižnica . . . . . .   DPTWH
Typ knižnice . . . . . .   *PROD
Textový 'opis'  . . . . . .   Skladová knižnica

                          Ďalšie parametre

Oprávnenie . . . . . .   *USE
ID pomocnej pamäťovej oblasti  . .   1
Vytvoriť oprávnenie  . . . . . .   *CHANGE
Vytvoriť audit objektu . . . . . .   *SYSVAL
```

Možná chyba	Obnova
Kláves **Enter** ste stlačili skôr, ako ste napísali opis pre knižnicu.	Napíšte **CHGLIB** a stlačte **F4** (Výzva). Názov knižnice napíšte do obrazovky výzvy a stlačte kláves **Enter**. Opis napíšte na obrazovke Zmeniť knižnicu.
Dali ste knižnici nesprávny názov.	Použite príkaz RNMOBJ (Rename Object).

Po vytvorení knižnice pre skupinu, môžete vytvoriť opis úlohy.

Vytváranie opisu úlohy

Po vytvorení knižnice pre skupinu môžete vytvoriť opis úlohy pre každú skupinu.

Ak sa knižnice, ktoré sú potrebné pre úvodný zoznam knižníc, ešte nenachádzajú v systéme, dostanete varovnú správu, keď vytvoríte opis úlohy.

1. Napíšte **CRTJOBD** (Create Job Description) a stlačte **F4** (Výzva).
2. Vyplňte tieto polia:

   Opis úlohy:
   Rovnaké ako názov skupinového profilu.

   Názov knižnice:
   QGPL

   Text: Opis skupiny
3. Stlačte **F10** (Ďalšie parametre).
4. Posúvajte sa o stránku nižšie až na pole *Úvodný zoznam knižníc*.

```
                  Vytvoriť opis úlohy

Napíšte voľby, stlačte kláves Enter.

Opis úlohy  . . . . . .  DPTSM
  Knižnica . . . . . .  QGPL
Front úloh . . . . . .  QBATCH
  Knižnica . . . . . .    *LIBL
Priorita úlohy (v JOBQ)  . . . . .  5
Výstupná priorita (v OUTQ) . . . .  5
Tlačové zariadenie . . . . . .  *USRPRF
Výstupný front . . . . . .  *USRPRF
  Knižnica . . . . . .
Textový 'opis'  . . . . . .  Predaj a marketing
```

5. V poli *Úvodný zoznam knižníc* prepíšte hodnotu *SYSVAL hodnotou **+** (plus), aby ste špecifikovali, že chcete zadať zoznam hodnôt. Stlačte kláves **Enter**.

```
Kód evidencie  . . . . . .  *USRPRF
   ⋮
Kontrola syntaxe CL . . . . . .  *NOCHK
Úvodný zoznam knižníc . . . . . .  +
              + pre viac hodnôt
```

6. Do poľa *Úvodný zoznam knižníc* napíšte názvy knižníc, ktoré sú označené (✓) z vášho formulára Opis skupiny užívateľov:
   - Do jedného riadka vložte jeden názov knižnice.
   - Zahrňte QGPL a QTEMP. Každá úloha používa knižnicu s názvom QTEMP pre ukladanie dočasných objektov. **Všetky úvodné zoznamy knižníc musia mať knižnicu QTEMP**. Pri väčšine aplikácií musí byť knižnica QGPL uvedená aj v úvodnom zozname knižníc.
   - Aktuálnu (štandardnú) knižnicu nemusíte zahrnúť do zoznamu knižníc. Systém pridá túto knižnicu automaticky pri prihlásení.
7. Stlačte kláves **Enter**. Skontrolujte správy. (Posúvajte sa o stránku nižšie, aby ste videli všetky správy.)

```
Špecifikovať viac hodnôt pre

Napíšte voľby, stlačte kláves Enter.

Úvodný zoznam knižníc  . . . . .   CUSTLIB
                                    ITEMLIB
                                    COPGMLIB
                                    ICPGMLIB
                                    QGPL
                                    QTEMP
```

Možná chyba	Obnova
Namiesto klávesu **F10** ste stlačili kláves **Enter**.	Ak chcete do úvodného zoznamu knižníc vložiť správne knižnice, napíšte **CHGJOBD** (Change Job Description) a stlačte **F4**.
Dostanete chybové hlásenia, keď sa pokúsite vytvoriť opis úlohy.	Najbežnejšie chybové hlásenie sa vyskytuje, keď sa pokúšate včleniť knižnicu, ktorá sa nenachádza v systéme. Toto je varovná správa. Opis úlohy sa aj tak vytvorí v knižnici, ktorá je v úvodnom zozname knižníc. Nemôžete sa prihlásiť s profilom, ktorý určuje opis úlohy, pokiaľ nebude knižnica v systéme. Ak sa knižnica nachádza v systéme, mohli ste nesprávne napísať jej názov. Overte názov knižnice a skúste to ešte raz.

Po vytvorení opisu úlohy môžete vytvoriť skupinový profil.

Vytvorenie skupinového profilu

Po vytvorení opisu úlohy môžete vytvoriť skupinový profil. Ak to chcete urobiť, použite informácie z formulára Opis skupín užívateľov Časť 2.

1. Použite príkaz Work with User Profiles. Napíšte WRKUSRPRF *ALL. Na začiatku obrazovka vypíše profily, ktoré dodala spoločnosť IBM.

   Poznámka: Ak uvidíte obrazovku Pracovať so zaradením užívateľa, stlačte **F21** pre prechod na stredná úroveň asistencie.

2. Ak chcete vytvoriť nový profil, napíšte **1** do stĺpca *Vol* (voľba) a názov profilu napíšte do stĺpca *Užívateľský profil*. Stlačte kláves **Enter**.

```
                        Pracovať s užívateľskými profilmi

Napíšte voľby, stlačte kláves Enter.
  1=Vytvoriť   2=Zmeniť   3=Kopírovať   4=Vymazať   5=Zobraziť
  12=Pracovať s objektmi podľa vlastníka

     Užívateľ
Vol  Profil      Text
1    DPTSM
     QDOC        Užívateľský profil dokumentov
     QSECOFR     Užívateľský profil správcu bezpečnosti
```

3. Informácie z vášho formulára Opis skupiny užívateľov vpíšte do príslušných polí.
4. Kláves **Tab** použite na preskočenie všetkých polí, v ktorých chcete používať štandardnú hodnotu.
5. Stlačte **F10** (Ďalšie parametre).
6. Posuňte sa o stránku nižšie.

```
                       Vytvoriť užívateľský profil (CRTUSRPRF)

Napíšte voľby, stlačte kláves Enter.

Užívateľský profil . . . . . > DPTSM
Užívateľské heslo  . . . . . .  *none
Nastaviť uplynutie platnosti hesla. .  *NO
Stav   . . . . . .  *ENABLED
Trieda užívateľov  . . . . . .  *USER
Úroveň pomoci    . . . . . .  *SYSVAL
Aktuálna knižnica  . . . . . .  *CRTDFT
Úvodný program, ktorý sa má volať. cpsetup
  Knižnica . . . . . .  cppgmlib
Úvodná ponuka  . . . . . .  cpmain
  Knižnica . . . . . .  cppgmlib
Obmedziť schopnosti  . . . . . .  *yes
Textový 'opis'  . . . . . .  Predaj a marketing
```

7. Na ďalšie stránky obrazovky zadajte zostávajúce polia z vášho formulára Opis skupín užívateľov a stlačte kláves **Enter**.

```
                        Vytvoriť užívateľský profil

                          Ďalšie parametre

Mimoriadne oprávnenie. . . . . *USRCLS

   :
Opis úlohy  . . . . . .  DPTSM
  Knižnica . . . . . .  QGPL
```

```
                        Vytvoriť užívateľský profil

Skupinové oprávnenia . . . . . *NONE

   :
Tlačové zariadenie . . . . . .  PRT03
```

8. Skontrolujte správy.

Nezabudnite

Skupinový profil je len špeciálnym typom užívateľského profilu. Mnohé správy a obrazovky odkazujú na skupinové profily ako na užívateľov alebo na užívateľské profily. Systém bude vedieť, že ste vytvorili skupinový profil iba vtedy, ak doň pridáte členov alebo mu priradíte identifikačné číslo skupiny (gid).

Možná chyba	Obnova
Kláves **Enter** ste stlačili skôr ako ste do skupinového profilu napísali všetky hodnoty.	Stlačte **F5** (Obnoviť), aby profil, ktorý ste vytvorili, pribudol na obrazovke Pracovať s užívateľskými profilmi. Voľbu **2** (Zmeniť) použite na opravu profilu.
Vytvorili ste profil s nesprávnym názvom.	Nedokážete zmeniť názov profilu. Voľbu kopírovania (**3**) použite na vytvorenie nového profilu so správnym názvom. Potom profil s chybným názvom vymažte (voľba **4**).
Niektoré polia z formulára Opis skupín užívateľov sa neobjavia na obrazovke.	Presvedčte sa, či používate stredná úroveň asistencie. Verzia základná úroveň asistencie obrazovky Vytvoriť užívateľský profil sa nazýva Pridať užívateľa. Ak chcete zmeniť úrovne pomoci, stlačte **F12** (Zrušiť) pre návrat na obrazovku Pracovať so zaradením užívateľa. **F21** použite na zmenenie úrovní pomoci. Pozrite si tému ″Vybratie správnej úrovne pomoci.″
Nedopatrením ste z obrazovky Vytvoriť užívateľský profil vymazali niektoré štandardné informácie.	Ak necháte pole prázdne, systém pri vytvorení užívateľského profilu použije štandardnú hodnotu. Ak chcete vidieť štandardné hodnoty, stlačte **F5** (Obnoviť) alebo obnovte celú obrazovku. Znovu napíšte svoje informácie.

Vypísanie vašich výsledkov

Vypíšte názvy a opisy všetkých profilov v systéme použitím príkazu DSPAUTUSR (Display Authorized Users). Napíšte DSPAUTUSR OUTPUT(*PRINT). Pre istotu skontrolujte, či majú všetky skupinové profily heslo *NONE.

Predtým, ako začnete nastavovať konkrétnych užívateľov, dokončite nasledovné:

- Vytvorte opis úlohy pre každú skupinu užívateľov.
- Voliteľne vytvorte knižnicu pre každú skupinu.
- Vytvorte skupinový profil pre každú skupinu užívateľov.

Nastavenie konkrétnych užívateľov

Keď ste nastavili skupiny užívateľov, dokončili ste kroky pre vytvorenie skupinových profilov. Teraz vytvoríte konkrétne profily pre členov týchto skupín.

Prejdite si celú tému a pritom pracujte iba s členmi jednej skupiny užívateľov, potom sa vráťte na začiatok a postup zopakujte pre ďalšie skupiny. Vzorové obrazovky ukazujú užívateľov z Formulár jednotlivého užívateľského profilu, ktoré Sharon Jonesov pripravil pre oddelenie predaja a marketingu a oddelenie skladového hospodárstva v Spoločnosť JKL Toy. Kópie týchto formulárov nájdete v ″Plánovanie konkrétnych užívateľských profilov.″

Použite formuláre Konkrétny užívateľský profil, ktoré ste si pripravili v ″Plánovaní konkrétnych užívateľských profilov.″

Ak chcete vytvoriť konkrétne profily pre členov týchto skupín, dokončite tieto úlohy:

1. Vytvorte osobnú knižnicu. (voliteľné)
2. Skopírujte skupinový profil.
3. Nastavte uplynutie platnosti hesla.
4. Vytvorte ďalších užívateľov. (voliteľné)

   Poznámka: Úlohu Vytvoriť osobnú knižnicu a Vytvoriť ďalších užívateľov opakujte dovtedy, pokiaľ nebude mať každý člen skupiny užívateľský profil.
5. Zmeňte informácie o užívateľovi, ak je to potrebné.
6. Zobrazte svoje výsledky.

Prihlásenie do systému

Profil Váš vlastný (vyžaduje sa oprávnenie *SECADM)

Ponuka

SETUP

Vytvorenie osobnej knižnice

Ak chcete začať nastavovať konkrétnych užívateľov, možno budete musieť pre každého člena vytvoriť osobnú knižnicu na objekty, ako napríklad programy Query. Osobné knižnice vytvorte skôr, ako vytvoríte konkrétne užívateľské profily.

1. Napíšte **CRTLIB** a stlačte **F4** (Výzva).
2. Knižnicu pomenujte rovnako ako užívateľský profil.
3. Stlačte **F10** (Ďalšie parametre).
4. Doplňte verejné oprávnenie pre knižnicu a nové objekty, ktoré sú v knižnici vytvorené.
5. Stlačte kláves **Enter**. Skontrolujte potvrdzovaciu správu.

```
                          Vytvoriť knižnicu

Napíšte voľby, stlačte kláves Enter.

Knižnica . . . . . .   DPTSM
Typ knižnice . . . . . .   *PROD
Textový 'opis'  . . . . . .   Skladová knižnica

                         Ďalšie parametre

Oprávnenie . . . . . .   *EXCLUDE
ID pomocnej pamäťovej oblasti. .   1
Vytvoriť oprávnenie  . . . . . .   *CHANGE
Vytvoriť audit objektu . . . . .   *SYSVAL
```

Po vytvorení osobnej knižnice, môžete konkrétny profil vytvoriť pomocou kopírovania skupinového profilu.

Kopírovanie skupinového profilu

Skupinový profil má dve roly:

1. Systém ho používa, aby určil či je člen skupiny autorizovaný na používanie objektu.
2. Môžete ho použiť ako vzor pre vytváranie užívateľských profilov pre konkrétnych členov skupiny.

Keď ste nastavili skupiny užívateľov, vytvorili ste skupinové profily. Teraz môžete skupinový profil kopírovať, aby ste vytvorili konkrétny profil a kopírovať konkrétny profil, aby ste vytvorili iné profily v skupine.

1. Z Ponuka NASTAVENIE vyberte voľbu Pracovať so zaradením užívateľa.

   Poznámka: Ak uvidíte obrazovku Pracovať s užívateľskými profilmi, **F21** (Vybrať úroveň pomoci) použite na prechod na základná úroveň asistencie.

2. Napíšte **3** (Kopírovať) do stĺpca *Vol* pred skupinu užívateľov. Na displeji sa zobrazí obrazovka Kopírovať užívateľa. (Ak sa skupina užívateľov, ktorú chcete kopírovať, nenachádza na vašej obrazovke, posúvajte sa o stránku nižšie, kým ju nenájdete.) Systém necháva pole pre meno užívateľa prázdne a zostávajúce polia doplní zo skupinového profilu, ktorý ste skopírovali.

```
                        Pracovať so zaradením užívateľa

Zadajte voľby, stlačte kláves Enter.
  1=Pridať   2=Zmeniť   3=Kopírovať   4=Odstrániť   5=Zobraziť

Vol     Užívateľ          Opis

        DPTSM          Oddelenie predaja a marketingu
3       DPTWH          Oddelenie skladového hospodárstva
```

3. Napíšte názov a opis užívateľského profilu, ktorý vytvárate.
4. Pole pre heslo nechajte prázdne. Systém automaticky vytvorí heslo, ktoré je rovnaké ako názov nového užívateľského profilu.
5. Názov skupinového profilu dajte do poľa *Skupina užívateľov*.
6. Skontrolujte si svoj formulár Konkrétny užívateľský profil, či má tento užívateľ aj iné hodnoty, ktoré sa líšia od skupinových. Zadajte tieto hodnoty.
7. Posuňte sa o stránku nižšie.

```
                              Kopírovať užívateľa

Kopírovať z užívateľa . :   DPTWH

Zadajte voľby, stlačte kláves Enter.

Užívateľ  . . . . . .   WILLISR
Opis užívateľa . . . . .  Willis, Rose
Heslo . . . . . .
Typ užívateľa . . . . . .   *SYSOPR
Skupina užívateľov  . . .   DPTWH

Obmedziť použitie príkazového riadka   N

Štandardná knižnica . . .   DPTWH
Štandardná tlačiareň  . .   PRT04
Prihlasovací program  . .   *NONE
  Knižnica  . . . . . .

Prvá ponuka . . . . . .   ICMAIN
  Knižnica  . . . . . .     ICPGMLIB
```

8. Na nasledujúcej stránke obrazovky vykonajte všetky potrebné zmeny a stlačte kláves **Enter**.
9. Skontrolujte potvrdzovacie správy na konci obrazovky Pracovať so zaradením užívateľa.

```
                                Kopírovať užívateľa

Kopírovať z užívateľa . :   DPTWH

Zadajte voľby, stlačte kláves Enter.

Program klávesu Attention.   *SYSVAL
  Knižnica  . . . . . .
```

Možná chyba	Obnova
Namiesto obrazovky Kopírovať užívateľa vidíte obrazovku Vytvoriť užívateľský profil.	Kláves **F12** (Zrušiť) použite pre návrat na obrazovku Pracovať s užívateľskými profilmi. Kláves **F21** použite na prechod do základnej úrovne asistencie. Operáciu kopírovania spustite ešte raz.
Názov užívateľského profilu, ktorý ste vybrali, sa nezmestí do užívateľskej výzvy.	Hoci názvy užívateľských profilov môžu obsahovať až 10 znakov, obrazovky Kopírovať užívateľa a Pridať užívateľa podporujú názvy, ktoré majú maximálne 8 znakov. Buď si zvoľte kratšie užívateľské meno alebo použite stredná úroveň asistencie, aby ste vytvorili konkrétne užívateľské profily.

Testovanie užívateľského profilu

Keď v skupine vytvoríte prvý konkrétny profil, mali by ste ho vyskúšať tak, že sa prihlásite s týmto profilom. Overte si, či vidíte správnu prvú ponuku a či je spustený prihlasovací program.

Ak sa s týmto profilom nedokážete úspešne prihlásiť, systém pravdepodobne nemohol v profile nájsť niečo špecifikované. Mohol by to byť prihlasovací program, opis úlohy alebo niektorá knižnica z úvodného zoznamu knižníc. Použite obrazovku Pracovať s tlačovým výstupom, aby ste našli protokol úlohy, ktorý bol napísaný pri vašom pokuse o prihlásenie sa. Protokol úlohy vám povie, aké chyby sa vyskytli.

Informácie o problémoch s testovaním a diagnostikou, keď vykonávate zmeny v zabezpečení, si pozrite v téme ″Testovanie zabezpečenia.″

Po preverení užívateľského profilu, môžete nastaviť uplynutie platnosti hesla.

Nastavenie uplynutia platnosti hesla

Nastavte konkrétne profily tak, aby od užívateľov vyžadovali zmenu ich hesiel pri ich prvom prihlásení sa. Pole *Nastaviť uplynutie platnosti hesla* sa neobjaví vo verzii základná úroveň asistencie obrazovky Kopírovať užívateľa. Musíte to zmeniť oddelene, po vytvorení užívateľského profilu cez funkciu kopírovania. Ak chcete zmeniť pole *Nastaviť uplynutie platnosti hesla*, napíšte CHGUSRPRF *názov-profilu* PWDEXP(*YES).

Poznámka: Ak chcete užívateľský profil vyskúšať tak, že sa s ním prihlásite, test vykonajte *skôr* ako nastavíte uplynutie platnosti hesla.

Možná chyba	Obnova
Otestovali ste profil a boli ste nútený zmeniť heslo.	Napíšte **CHGUSRPRF** *názov-profilu* a stlačte **F4** (Výzva). Heslo pre názov užívateľského profilu vráťte naspäť. (Do poľa pre heslo napíšte názov užívateľského profilu.) Do poľa *Nastaviť uplynutie platnosti hesla* napíšte ***YES**. Aby ste to mohli urobiť, potrebujete strednú úroveň asistencie.

Po vytvorení prvého konkrétneho užívateľského profilu, môžete vytvoriť ďalších užívateľov.

Vytvorenie ďalších užívateľov

Po skopírovaní skupinového profilu pre vytvorenie prvého konkrétneho profilu, môžete vytvoriť ďalších užívateľov. Prvý konkrétny užívateľský profil skopírujte, aby ste vytvorili ďalších členov v skupine. Keď vytvárate konkrétne užívateľské profily pomocou kopírovania, na každý konkrétny profil sa pozrite veľmi pozorne. Skontrolujte svoj formulár Konkrétny užívateľský profil a určite zmeňte všetky polia, ktoré sú pre nový užívateľský profil jedinečné.

1. Na obrazovke Pracovať so zaradením užívateľa napíšte **3** (Kopírovať) pred užívateľský profil, ktorý chcete kopírovať.
2. Na obrazovke Kopírovať užívateľa napíšte názov profilu a opis.
3. Informácie zadajte do všetkých poli, ktoré sú pre nového užívateľa jedinečné.

```
                        Pracovať so zaradením užívateľa

Zadajte voľby, stlačte kláves Enter.
  1=Pridať   2=Zmeniť   3=Kopírovať   4=Odstrániť   5=Zobraziť

Vol     Užívateľ          Opis

        DPTSM          Oddelenie predaja a marketingu
        DPTWH          Oddelenie skladového hospodárstva
3       WILLISR        Willis, Rose
```

Možná chyba	Obnova
Profil, ktorý chcete kopírovať sa neobjaví na obrazovke Pracovať so zaradením užívateľa.	Stlačte **F5** (Obnoviť). Posúvajte sa o stránku vyššie a nižšie. Zoznam je zoradený abecedne podľa názvu profilu.

Ak by ste chceli zmeniť informácie o užívateľovi, pozrite si tému Zmena informácií o užívateľovi.

Zmena informácií o užívateľovi

Pri niektorých užívateľoch môžete potrebovať nastaviť hodnoty, ktoré sa neobjavia na obrazovke Kopírovať užívateľa. Napríklad niektorí užívatelia môžu patriť do viac ako jedného skupinového profilu. Po vytvorení užívateľského profilu pomocou kopírovania, môžete tento profil zmeniť.

1. Na obrazovke Pracovať so zaradením užívateľa stlačte **F21** pre prechod na strednú úroveň asistencie.
2. Na obrazovke Pracovať s užívateľskými profilmi napíšte do stĺpca *Vol* (voľba) vedľa profilu, ktorý chcete zmeniť voľbu **2** (Zmeniť). Stlačte kláves **Enter**.

```
                        Pracovať s užívateľskými profilmi

Napíšte voľby, stlačte kláves Enter.
  1=Vytvoriť   2=Zmeniť   3=Kopírovať   4=Vymazať   5=Zobraziť
  12=Pracovať s objektmi podľa vlastníka

     Užívateľ
Vol  Profil      Text
2    AMESJ       Ames, Janice
     DPTSM       Oddelenie predaja a marketingu
     QDOC        Užívateľský profil dokumentov
     QSECOFR     Užívateľský profil správcu bezpečnosti
     WAGNERR     Wagner, Ray
     WILLISR     Willis, Rose
```

3. Na obrazovke Zmeniť užívateľský profil stlačte **F10** (Ďalšie parametre).
4. Posúvajte sa o stránku nižšie, kým nenájdete polia, ktoré chcete zmeniť. Napríklad, ak chcete, aby sa užívateľ stal členom ďalších skupinových profilov, posúvajte sa o stránku nižšie, kým nenájdete pole *Doplnkové skupiny*.

5. Napíšte potrebné hodnoty a stlačte kláves **Enter**. Dostanete potvrdzovacie správy a znovu uvidíte obrazovku Pracovať s užívateľskými profilmi.

```
                        Zmeniť užívateľský profil (CHGUSRPRF)

Napíšte voľby, stlačte kláves Enter.

Maximálna povolená pamäť . . . .   *NOMAX
Najvyššia priorita plánovania. .   3
Opis úlohy  . . . . . . . . . .   DPTWH
  Knižnica . . . . . . . . . . .     QGPL
Skupinový profil . . . . . . . .   DPTWH
Vlastník . . . . . . . . . . . .   *GRPPRF
Skupinové oprávnenia . . . . . .   *USEE
Typ skupinových oprávnení  . . .   *PGP
Doplnkové skupiny  . . . . . . .   DPTIC
              + pre viac hodnôt
```

Akonáhle ste zmenili užívateľské informácie, môžete zobraziť svoje výsledky pre kontrolu svojich profilov.

Zobrazenie užívateľských profilov

Na zobrazenie profilov, ktoré ste vytvorili máte k dispozícii niekoľko metód.

Zobrazenie jedného profilu
Voľbu **5** (Zobraziť) použite buď z obrazovky Pracovať so zaradením užívateľa alebo z obrazovky Pracovať s užívateľskými profilmi.

Vypísanie jedného profilu
Použite príkaz Display User Profile: DSPUSRPRF *názov-profilu* DETAIL(*BASIC) OUTPUT(*PRINT).

Zobrazenie členov skupiny
Napíšte DSPUSRPRF *názov-skupinového-profilu* *GRPMBR. Na vytlačenie zoznamu môžete použiť OUTPUT(*PRINT).

Vypísanie všetkých profilov
Ak chcete vypísať názvy a opisy všetkých profilov zotriedených podľa skupiny, použite príkaz Display Authorized Users: DSPAUTUSR SEQ(*GRPPRF) OUTPUT(*PRINT).

Skôr než nastavíte vlastníctvo a verejné oprávnenie, uistite sa, že ste dokončili tieto úlohy:

- Ukončite vytváranie všetkých svojich konkrétnych užívateľských profilov.
- Nastavte uplynutie platnosti hesla pre každý profil.
- Vytlačte zoznam všetkých profilov, utriedený podľa skupiny a založte si ho k svojim formulárom Opis skupín užívateľov. Keď pridáte nových užívateľov, zoznam znova vytlačte.

Nastavenie zabezpečenia prostriedkov

V tejto téme vytvoríte vlastníctvo a verejné oprávnenie pre objekty, a rovnako aj špecifické oprávnenie pre vaše aplikácie. Takisto nastavíte zabezpečenie prostriedku pre pracovné stanice a tlačiarne. Prejdite si celú tému a pracujte iba s jednou knižnicou, potom sa vráťte na začiatok a postup zopakujte pri všetkých ďalších knižniciach, ktoré aplikácia používa. Keď dokončíte nastavenie zabezpečenia prostriedku pri jednej aplikácii, zopakujte tieto kroky aj pri ostatných aplikáciách.

Tieto postupy používajte vždy, keď inštalujete novú aplikáciu do vášho systému, alebo keď nastavujete zabezpečenie prostriedku pre existujúcu aplikáciu.

Vzorové obrazovky v tejto téme ukazujú formuláre Autorizačný zoznam, formuláre Opis knižnice a formulár Výstupný front a Zabezpečenie pracovnej stanice pre Spoločnosť JKL Toy. Vzory týchto formulárov nájdete v téme ″Nastavenie vlastníctva a verejného oprávnenia.″

Aké formuláre sú potrebné?

- Formuláre Inštalácia aplikácií, ktoré ste si pripravili v ″Plánovaní inštalácie svojich aplikácií.″
- Formuláre Autorizačný zoznam, ktoré ste si pripravili v ″Zoskupovaní objektov.″
- Formuláre Opis knižnice, ktoré ste si pripravili v ″Určovaní vlastníctva knižníc a objektov.″
- Formulár Výstupný front a zabezpečenie pracovnej stanice, ktorý ste si pripravili v ″Ochrane tlačového výstupu″ a v ″Ochrane pracovných staníc.″
- Formulár Zodpovednosti systému, ktorý ste si pripravili v ″Stratégii plánovania svojej celkovej bezpečnosti.″

Zabezpečenie prostriedku môžete nastaviť niekoľkými spôsobmi. Poradie krokov v tejto téme je zhodné s poradím informácií na formulároch Inštalácia aplikácií, formulároch Autorizačný zoznam a na formulári Opis knižnice:

1. Nastavenie vlastníctva a verejného oprávnenia.
2. Vytvorenie autorizačných zoznamov.
3. Zabezpečovanie objektov cez autorizačný zoznam.
4. Pridanie užívateľov do autorizačných zoznamov.
5. Nastavenie všetkých špecifických oprávnení.
6. Zabezpečovanie tlačového výstupu.
7. Zabezpečovanie pracovných staníc.
8. Obmedzovanie prístupu do frontu správ operátora systému.

Nastavenie vlastníctva a verejného oprávnenia

V tejto téme vytvoríte vlastníctvo a verejné oprávnenie pre aplikačné knižnice, knižnice skupín a osobné knižnice. Prejdite si celú tému a pracujte iba s jednou aplikáciou, potom sa vráťte na začiatok a postup zopakujte pri ostatných aplikáciách. Vzorové obrazovky ukazujú formuláre Inštalácia aplikácií, ktoré pripravila Sharon Jones pre aplikáciu Objednávky zákazníkov v ″Plánovaní inštalácie svojich aplikácií.″

Postupy z tejto témy používajte vždy, keď do svojho systému nainštalujete novú aplikáciu, alebo keď nastavujete zabezpečenie pre existujúcu aplikáciu.

Použite formuláre Inštalácia aplikácií, ktoré ste si pripravili v ″Plánovaní inštalácie svojich aplikácií.″

Aby ste mohli nastaviť vlastníctvo a verejné oprávnenie, dokončite tieto úlohy:

1. Vytvorte profil vlastníka.
2. Zmeňte vlastníctvo knižnice.
3. Nastavte vlastníctvo aplikačných objektov.
4. Nastavte verejný prístup do knižnice.
5. Nastavte verejné oprávnenie pre všetky objekty v knižnici.
6. Nastavte verejné oprávnenie pre nové objekty.
7. Pracujte s knižnicami skupín a s osobnými knižnicami.

Prihlásenie do systému

Profil Váš vlastný (vyžaduje sa oprávnenie *ALLOBJ)

Ponuka
MAIN

Vytvorenie profilu vlastníka

Ak profil vlastníka ešte neexistuje, urobte nasledovné:

- Na jeho vytvorenie použite príkaz CRTUSRPRF (Create User Profile). Heslo nastavte na *NONE.

Ak už profil vlastníka existuje, urobte nasledovné:

- Príkaz CHGUSRPRF (Change User Profile) použite na nastavenie hesla na *NONE.

Po vytvorení profilu vlastníka môžete zmeniť vlastníctvo knižníc.

Zmena vlastníctva knižníc

Tieto kroky zmenia vlastníctvo knižnice, nie však vlastníctvo objektov v tejto knižnici.

Upozornenie: Skôr než zmeníte vlastníctvo nejakých aplikačných objektov, určite si to dajte odsúhlasiť u svojho poskytovateľa aplikácií. Niektoré aplikácie používajú funkcie, ktoré sa spoliehajú na špecifické vlastníctvo objektu.

1. Napíšte CHGOBJOWN (Change Object Owner) a stlačte kláves **F4** (Výzva).
2. Vyplňte názov knižnice, typ objektu (*LIB) a nového vlastníka.
3. Skontrolujte potvrdzovacie správy.

```
                      Zmeniť vlastníka objektu (CHGOBJOWN)

Napíšte voľby, stlačte kláves Enter.

Objekt . . . . . . . . . . . . . > COPGMLIB
  Knižnica . . . . . . . . . . . >   *LIBL       Názov,
Typ objektu  . . . . . . . . . .> *LIB
Nový vlastník  . . . . . . . . .   COWNER
Oprávnenie aktuálneho vlastníka.   *REVOKE
```

Možná chyba	Obnova
Dostali ste chybové hlásenia.	Najbežnejšia správa je, že buď nebola nájdená knižnica alebo nebol nájdený profil nového vlastníka. Skontrolujte, či ste pri písaní neurobili chybu a skúste to znovu.

Potom, ako ste zmenili vlastníctvo knižníc, môžete nastaviť vlastníctvo pre aplikačné objekty.

Nastavenie vlastníctva aplikačných objektov

Zmena vlastníctva aplikačných objektov je namáhavá úloha, pretože musíte zmeniť každý objekt zvlášť. Ak je to možné, požiadajte svojho programátora poskytovateľa aplikácií, aby vám vlastníctvo vytvoril.

Vypísanie objektov v knižnici

Predtým ako zmeníte vlastníctvo, použitím príkazu Display Library vytlačte zoznam všetkých objektov v knižnici. Môžete ho použiť ako kontrolný zoznam. Napíšte DSPLIB *názov-knižnice* *PRINT.

Výber najlepšej metódy

Vyberte si jednu z týchto dvoch metód pre zmenenie vlastníctva objektov vo vašich aplikačných knižniciach:

Tabuľka 61. Metódy pre zmenenie vlastníctva objektu

Metóda	Čo robí	Kedy sa má použiť
Príkaz Work with Objects by Owner	Ukazuje obrazovku, na ktorej sú vypísané všetky objekty, ktoré profil vlastní. Na zmenu vlastníka objektu použite voľbu z obrazovky.	Táto metóda sa ľahšie používa. Ak však QPGMR alebo QSECOFR vlastnia tieto objekty, IBM neodporúča túto metódu. Tieto profily vlastnia mnohé objekty a obrazovka so zoznamom by bola veľmi veľká.
Príkaz Change Object Ownership	Vyžaduje použitie samostatného príkazu pre každý objekt. Môžete však použiť *Opakovane získať* (**F9**), aby sa zopakoval predchádzajúci príkaz, čo šetrí čas, potrebný na písanie.	Táto metóda je rýchlejšia, ak sú objekty vo vlastníctve QPGMR alebo QSECOFR.

použitie príkazu WRKOBJOWN (Work with objects by Owner): Túto metódu použite na zmenu vlastníctva objektov v knižnici, ak profily dodané spoločnosťou IBM, ako napríklad QPGMR alebo QSECOFR, objekty *nevlastnia*:

1. Napíšte WRKOBJOWN *názov-profilu-vlastníka*. Na vašej obrazovke sa zobrazí zoznam všetkých objektov, ktoré takýto užívateľský profil vlastní.
2. Napíšte **9** (Zmeniť vlastníka) pred každý objekt v knižnici, na ktorých pracujete.
3. Do riadka *Parametre alebo príkaz* na konci obrazovky napíšte NEWOWN(*názov-profilu-vlastníka*) a stlačte kláves **Enter**.
4. Systém zmení vlastníka každého objektu, ktorý ste určili, na nového vlastníka, ktorého ste zadali na konci obrazovky. Potvrdzovacie správy dostanete na konci svojej obrazovky. Tieto objekty sa na vašej obrazovke už ďalej nezobrazujú, pretože profil ich už nevlastní.
5. Kroky 2 a 4 opakujte dovtedy, kým nezmeníte vlastníctvo všetkých objektov v knižnici.

```
                          Pracovať s objektmi podľa vlastníka

Užívateľský profil . . . . :   OLDOWNER

Napíšte voľby, stlačte kláves Enter.
  2=Upraviť oprávnenie    4=Vymazať  5=Zobraziť autora
  8=Zobraziť opis        9=Zmeniť vlastníka

Vol  Objekt        Knižnica       Typ      Atribút
     COPGMMSG      COPGMLIB      *MSGQ
9    CUSTMAS       CUSTLIB       *FILE
9    CUSTMSGQ      CUSTLIB       *MSGQ
     ITEMMSGQ      ITEMLIB       *MSGQ


   ⋮

Parametre alebo príkaz
===> NEWOWN(COWNER)
F3=Ukončiť   F4=Výzva   F5=Obnoviť   F9=Opakovane získať
F18=Koniec obrazovky
```

Možná chyba	Obnova
Vidíte obrazovku Zmeniť vlastníka objektu.	Túto obrazovku uvidíte, ak zadáte voľbu **9** (Zmeniť vlastníka) a na konci obrazovky Pracovať s objektmi podľa vlastníka nenapíšete žiadne parametre. Túto obrazovku uvidíte aj vtedy, ak napíšete parametre nesprávne. Stlačte **F12** (Zrušiť) pre návrat na obrazovku Pracovať s objektmi podľa vlastníka. Skúste to znova. Uistite sa, že ste parameter napísali presne tak, ako je uvedený v príklade.

Príkaz Change Object Owner môžete použiť na zmenenie vlastníctva objektov, ktoré vlastní QPGMR alebo QSECOFR.

Použitie príkazu Change Object Owner: Túto metódu použite na zmenu vlastníka objektov v knižnici, ak QPGMR alebo QSECOFR *vlastnia* tieto objekty.

1. Napíšte CHGOBJOWN a stlačte **F4** (Výzva).
2. Na obrazovke vyplňte informácie pre prvý objekt na vašom zozname a stlačte **Enter**.

```
                      Zmeniť vlastníka objektu (CHGOBJOWN)

Napíšte voľby, stlačte kláves Enter.

Objekt . . . . . . . . . . . . . > CUSTMAS
  Knižnica . . . . . . . . . . . >   CUSTLIB
Typ objektu  . . . . . . . . . . > *FILE
Nový vlastník  . . . . . . . . .   COWNER
Oprávnenie aktuálneho vlastníka.   *REVOKE
```

3. Dostane potvrdzovaciu správu o tom, že sa zmenilo vlastníctvo objektu. Odškrtnite si položku vo svojom zozname.
4. Stlačte **F9** (Opakovane získať), aby ste opakovane získali príkaz, ktorý ste napísali.
5. Stlačte **F4** (Výzva). Na obrazovke Zmeniť vlastníka objektu zadajte informácie pre nasledujúci objekt v knižnici a stlačte kláves **Enter**.
6. Kroky štyri a päť zopakujte pre každý objekt v knižnici.

Kontrola vašej práce

Ak sa chcete uistiť, že ste zmenili vlastníctvo všetkých objektov v knižnici, použite príkaz WRKOBJOWN (Work with Objects by Owner). Napíšte WRKOBJOWN *nový-profil-vlastníka*. Porovnajte obrazovku so zoznamom objektov v knižnici.

Potom, keď zmeníte vlastníctvo objektov v knižnici, môžete do knižnice nastaviť verejný prístup.

Nastavenie verejného prístupu do knižnice

Potom ako ste zmenili nastavili vlastníctvo aplikačných objektov, môžete príkaz EDTOBJAUT (Edit Object Authority) použiť na zmenu verejného oprávnenia pre knižnicu:

1. Napíšte EDTOBJAUT *názov-knižnice* *LIB.
2. Kurzor presuňte nižšie na riadok s nápisom **PUBLIC*.
3. Napíšte oprávnenie, ktoré má mať verejnosť pre túto knižnicu a stlačte kláves **Enter**.

```
                          Upraviť oprávnenie na objekt

Objekt . . . . . . . :   CUSTLIB         Vlastník . . . . . . :   COWNER
  Knižnica . . . . . :     QSYS          Primárna skupina . . :   *NONE
Typ objektu  . . . . :   *LIB

Napíšte zmeny pre aktuálne oprávnenia, stlačte kláves Enter.

  Objekt je zabezpečený autorizačným zoznamom  . . . . . . . . .   *NONE

                         Objekt
Užívateľ    Skupina      Oprávnenie
COWNER                   *ALL
*PUBLIC                  *CHANGE
```

4. Obrazovka ukazuje nové oprávnenie.

Teraz môžete nastaviť verejné oprávnenie pre všetky objekty v knižnici.

Nastavenie verejného oprávnenia pre všetky objekty v knižnici

Príkaz RVKOBJAUT (Revoke Object Authority) použite na odstránenie aktuálneho verejného oprávnenia pre objekty v knižnici. Príkaz Grant Object Authority (GRTOBJAUT) použite na nastavenie verejného oprávnenia pre všetky objekty v knižnici:

1. Napíšte RVKOBJAUT a stlačte **F4** (Výzva).

2. Na obrazovke tak, ako je zobrazená nahraďte názov vašej aplikačnej knižnice a stlačte kláves **Enter**.

```
                    Zrušiť oprávnenie na objekt (RVKOBJAUT)

Napíšte voľby, stlačte kláves Enter.

Objekt . . . . . .   *ALL
  Knižnica . . . . . .    CUSTLIB
Typ objektu  . . . . . .   *ALL
Užívatelia . . . . . .   *PUBLIC
              + pre viac hodnôt
Oprávnenie . . . . . .   *ALL
```

Poznámka: Ak má knižnica veľké množstvo objektov, systému môže spracovanie vašej požiadavky trvať niekoľko minút.

3. Napíšte GRTOBJAUT a stlačte **F4** (Výzva).
4. Vyplňte obrazovku, tak ako je zobrazená a nahraďte názov vašej aplikačnej knižnice a oprávnenie ktoré potrebujete a stlačte kláves **Enter**.

```
                    Prideliť oprávnenie na objekt (GRTOBJAUT)

Napíšte voľby, stlačte kláves Enter.

Objekt . . . . . .   *ALL
  Knižnica . . . . . .    CUSTLIB
Typ objektu  . . . . . .   *ALL
Užívatelia . . . . . .   *PUBLIC
              + pre viac hodnôt
Oprávnenie . . . . . .   *USE
```

Poznámka: Ak má knižnica veľké množstvo objektov, systému môže spracovanie vašej požiadavky trvať niekoľko minút.

Po dokončení nastavenia verejného oprávnenia pre všetky objekty v knižnici, ako ďalšie môžete použiť protokol úloh na kontrolu vašej práce.

Použitie protokolu úloh na kontrolu vašej práce: Keď príkaz GRTOBJAUT používate na vykonanie viacerých zmien v oprávnení, pozrite si svoj protokol úlohy, aby ste si overili, či sa zmeny vykonali.

1. Napíšte DSPJOBLOG (Display Job Log).
2. Stlačte **F10** (Zobraziť podrobné správy).
3. Mali by ste mať správu o zmene oprávnenia pre každý objekt v knižnici. Pri prezeraní správ si postupne odškrtávajte objekty na zozname.

```
                          Zobraziť všetky správy
                        Systém:   RCHASxxx
Úloha . :   QPADEV0010    Užívateľ :   JCHEIDEL      Číslo  . . . :   025457

7 > GRTOBJAUT OBJ(CUSTLIB/*ALL) OBJTYPE(*ALL) USER(*PUBLIC) AUT(*USE)
  Oprávnenie uvedené pre užívateľa *PUBLIC pri objekte CUSTMAS v type objektu CUSTLIB
    je *FILE.
  Oprávnenie uvedené pre užívateľa *PUBLIC pri objekte CUSTMSGQ v type objektu CUSTLIB
    je *MSGQ.
  Oprávnenie je dané pre 2 objekty. Nie je dané pre 0 objektov. Čiastočne je dané 0
    objektom.
  Oprávnenie na objekt je pridelené.
7>> dspjoblog
```

Možná chyba	Obnova
Váš protokol úlohy indikuje, že takéto oprávnenie nebolo zmenené pri niektorých objektoch v knižnici.	Ak sa chcete dozvedieť bližšie informácie o správe, použite Pomoc (**F1**). EDTOBJAUT použite na samostatné nastavenie oprávnenia pre tieto objekty.

Teraz môžete nastaviť verejné oprávnenie pre nové objekty.

Nastavenie verejného oprávnenia pre nové objekty

Opis knižnice má parameter s názvom vytvoriť oprávnenie (CRTAUT), ktorý určuje verejné oprávnenie pre nové objekty, ktoré sú vytvorené v knižnici. Príkazy na vytváranie objektov štandardne používajú oprávnenie CRTAUT objektovej knižnice. CRTAUT by malo byť pri knižnici rovnaké ako je verejné oprávnenie pri väčšine existujúcich objektov v knižnici.

1. Napíšte CHGLIB *názov-knižnice* a stlačte **F4** (Výzva).
2. Stlačte **F10** (Ďalšie parametre).
3. Vašu voľbu zadajte do poľa *Vytvoriť oprávnenie*.

```
                    Zmeniť knižnicu (CHGLIB)

Napíšte voľby, stlačte kláves Enter.

Knižnica . . . . . . . . . . . . > CUSTLIB
Typ knižnice . . . . . . . . . .   *PROD
Textový 'opis'  . . . . . . . .   'Záznamy o zákazníkoch'


                    Ďalšie parametre

Vytvoriť oprávnenie  . . . . . .   *CHANGE
Vytvoriť audit objektu . . . . .   *SYSVAL
```

Ak CRTAUT nastavíte na *SYSVAL, systém použije aktuálne nastavenie pre systémovú hodnotu QCRTAUT, keď v knižnici vytvoríte nový objekt. Nastavenie špecifického oprávnenia CRTAUT pre každú knižnicu chráni proti budúcim zmenám v systémovej hodnote QCRTAUT.

Teraz môžete pracovať s knižnicami skupín a s osobnými knižnicami.

Práca s knižnicami skupín a s osobnými knižnicami

Váš profil vlastní knižnice skupín a osobné knižnice, ktoré ste vytvorili pri nastavovaní skupín užívateľov a konkrétnych užívateľov.

Uvádzané postupy použite na zmenu vlastníctva knižníc skupín pre skupinový profil a na zmenu vlastníctva osobných knižníc pre konkrétne užívateľské profily. Použite príkaz EDTOBJAUT.

Parameter Vytvoriť oprávnenie nastavte pre každú knižnicu skupiny a každú osobnú knižnicu pre určenie verejného oprávnenia pre ľubovoľné nové objekty v týchto knižniciach. Použite príklad CHGLIB.

Skôr než začnete vytvárať autorizačné zoznamy, dokončite tieto úlohy:

- Svoje formuláre Inštalácia aplikácií a formuláre Opis knižníc použite, aby ste sa uistili, že ste vytvorili vlastníctvo a verejné oprávnenie pre všetky svoje aplikačné knižnice.
- Nastavte vlastníctvo a vytvorte oprávnenie pre všetky knižnice skupín a všetky osobné knižnice, ktoré ste vytvorili.

  Poznámka: Zoznam všetkých knižníc vo vašom systéme získate, keď napíšete DSPOBJD *ALL *LIB *PRINT.

Vytvorenie autorizačného zoznamu

Keď ste nastavili vlastníctvo a verejné oprávnenie, ste pripravený nastaviť autorizačné zoznamy. Použitím informácií z vašich formulárov Autorizačný zoznam vytvorte všetky autorizačné zoznamy, ktoré sú potrebné na zabezpečenie knižnice. Použite príkaz CRTAUTL (Create Authorization List):

1. Napíšte CRTAUTL a stlačte **F4** (Výzva).
2. Doplňte informácie zo svojho formulára Autorizačný zoznam.
3. Stlačte **F10** (Ďalšie parametre).
4. Parameter zabezpečenie použite na zadanie verejného oprávnenia pre objekty, ktoré zoznam zabezpečuje.
5. Skontrolujte, či prišli potvrdzovacie správy.

```
                    Vytvoriť autorizačný zoznam (CRTAUTL)

Napíšte voľby, stlačte kláves Enter.

Autorizačný zoznam . . . . . .   CUSTLST1
Textový 'opis'  . . . . . .   Súbory vymazané pri

                        Ďalšie parametre

Oprávnenie . . . . . .   *ALL
```

Možná chyba	Obnova
Názov zoznamu ste napísali nesprávne.	Názov zoznamu nemôžete zmeniť, ak ho už systém vytvoril. Vymažte zoznam (DLTAUTL) a skúste to odznova.
Pri zozname ste zabudli zadať verejné oprávnenie.	Použite príkaz EDTAUTL (Edit Authorization List).

Teraz môžete zabezpečiť objekty cez autorizačný zoznam.

Zabezpečovanie objektov cez autorizačný zoznam

Akonáhle vytvoríte autorizačný zoznam, na zabezpečenie položiek, ktoré sú uvedené vo vašom formulári Autorizačný zoznam, použite príkaz EDTOBJAUT (Edit Object Authority):

1. Napíšte EDTOBJAUT a stlačte **F4** (výzva).
2. Vyplňte obrazovku výzvy a stlačte kláves **Enter**.
3. Na obrazovke Edit Object Authority zadajte názov autorizačného zoznamu.
4. Ak verejné oprávnenie pre objekt pochádza z autorizačného zoznamu, verejné oprávnenie zmeňte na *AUTL.
5. Tieto kroky zopakujte pri každom objekte vo vašom formulári Autorizačný zoznam.

```
                          Upraviť oprávnenie na objekt

Objekt . . . . . :   ARFILE01        Vlastník . . . . . :   OWNAR
  Knižnica . . . . . :    CUSTLIB       Primárna skupina . . :   *NONE
Typ objektu  . . . . :   *FILE

Napíšte zmeny pre aktuálne oprávnenia, stlačte kláves Enter.

  Objekt je zabezpečený pomocou autorizačného zoznamu . . . . .   CUSTLST1

                          Objekt
Užívateľ    Skupina      Oprávnenie
OWNER                    *ALL
*PUBLIC                  *AUTL
```

Teraz môžete pridať užívateľov do autorizačného zoznamu.

Pridanie užívateľov do autorizačného zoznamu

Akonáhle zabezpečíte objekty cez autorizačný zoznam, príkaz EDTAUTL (Edit Authorization List) použite na pridanie užívateľov, ktorý sú uvedení vo vašom formulári Autorizačný zoznam:

1. Napíšte EDTAUTL *názov-autorizačného-zoznamu*.
2. Na obrazovke Upraviť autorizačný zoznam, stlačte **F6** (Pridať nových užívateľov).
3. Zadajte mená užívateľov alebo názvy skupín a oprávnenie, ktoré by mali mať pre položky v zozname a stlačte kláves **Enter**.
4. Na zozname by sa mali objaviť noví užívatelia.

```
                            Pridať nových užívateľov

Objekt . . . . . :   WSLST1          Vlastník .
  Knižnica . . . . . :    QSYS

Napíšte nových užívateľov, stlačte kláves Enter.

             Objekt    Zoznam
Užívateľ     Oprávnenie Mgt
QSECOFR      *CHANGE
```

Možná chyba	Obnova
Užívateľovi alebo skupine ste udelili nesprávne oprávnenie pre zoznam.	Oprávnenie môžete zmeniť na obrazovke Upraviť autorizačný zoznam.
Na zoznam ste pridali nesprávneho užívateľa alebo skupinu.	Užívateľa alebo skupinu môžete odstrániť použitím príkazu RMVAUTLE (Remove Authorization List Entry), alebo na obrazovke Upraviť autorizačný zoznam môžete užívateľské oprávnenie nahradiť prázdnymi znakmi.

Kontrola vašej práce

Príkaz DSPAUTL (Display Authorization List) použite na výpis všetkých užívateľských oprávnení pre autorizačný zoznam. Ak chcete, aby sa vypísali všetky objekty, ktoré sú zabezpečené pomocou autorizačného zoznamu, použite **F15** na obrazovke.

Skôr než začnete vytvárať špecifické oprávnenia, dokončite tieto úlohy:

- Príkaz CRTAUTL použite na vytvorenie všetkých autorizačných zoznamov, ktoré potrebujete pre aplikáciu.

- Zabezpečte objekty cez autorizačné zoznamy pomocou príkazu EDTOBJAUT.
- Pridajte užívateľov do autorizačných zoznamov použitím príkazu EDTAUTL.

Nastavenie špecifických oprávnení

V téme ″Nastavenie vlastníctva a verejného oprávnenia″ ste sa na základe informácií v Časti 1 vášho formulára Opis Knižnice dozvedeli, ako sa má používať príkaz GRTOBJAUT na nastavenie verejného oprávnenia pre všetky objekty v knižnici. Teraz, na základe informácií v Časti 2 vášho formulára Opis knižnice, môžete príkaz EDTOBJAUT (Edit Object Authority) použiť na nastavenie špecifického oprávnenia pre knižnicu a pre objekty v knižnici.

Ak chcete nastaviť špecifické oprávnenia, pozrite si tieto témy:

- Nastavenie špecifického oprávnenia pre knižnicu.
- Nastavenie špecifického oprávnenia pre objekt.
- Nastavenie oprávnenia pri viacerých objektoch súčasne.

Nastavenie špecifického oprávnenia pre knižnicu

Knižnica je v skutočnosti špeciálny typ objektu. Oprávnenie pre knižnicu nastavíte rovnako ako oprávnenie pre každý iný objekt, použitím príkazu EDTOBJAUT. Všetky knižnice sú trvalo umiestnené v knižnici, ktorú dodala spoločnosť IBM, s názvom QSYS. Obrazovky v nasledujúcich príkladoch používajú formulár Opis knižnice, Časť 2 pre knižnicu CONTRACTS v Spoločnosť JKL Toy:

Výpis špecifických oprávnení pre objekty knižníc				
Skupinový profil alebo užívateľský profil	Názov objektu	Typ objektu	Potrebné oprávnenie	Autorizačný zoznam
DPTSM	CONTRACTS	*LIB	*USE	
DPTMG	CONTRACTS	*LIB	*USE	

1. Napíšte EDTOBJAUT a stlačte **F4** (Výzva).
2. Vyplňte obrazovku výzvy a stlačte kláves **Enter**.

```
                    Upraviť oprávnenie na objekt (EDTOBJAUT)

Napíšte voľby, stlačte kláves Enter.

Objekt . . . . . . . . . . . . .   CONTRACTS
  Knižnica . . . . . . . . . . .     QSYS
Typ objektu  . . . . . . . . . .   *LIB
```

3. Na obrazovke Upraviť oprávnenie na objekt stlačte **F6** (Pridať nových užívateľov), ak chcete udeliť oprávnenie užívateľom, ktorí nie sú na obrazovke vypísaní.
4. Stlačte kláves **Enter**.

```
                              Pridať nových užívateľov

Objekt . . . . . . . :   CONTRACTS       Vlastník . . . . . :   OWNCP
  Knižnica . . . . . :     QSYS          Primárna skupina . . :   *NONE
Typ objektu  . . . . :   *LIB


Napíšte nových užívateľov, stlačte kláves Enter.

                    Objekt
Užívateľ            Oprávnenie
DPTSM       *USE
DPTMG       *USE
```

5. Obrazovka Upraviť oprávnenie na objekt by sa mala zhodovať s informáciami aj z Časti 1 aj z Časti 2 formulára Opis knižnice.

```
                          Upraviť oprávnenie na objekt

Objekt . . . . . :   CONTRACTS       Vlastník . . . . . :   OWNCP
  Knižnica . . . . :     QSYS        Primárna skupina . . :   *NONE
Typ objektu  . . . . :   *LIB

Napíšte zmeny pre aktuálne oprávnenia, stlačte kláves Enter.

  Objekt je zabezpečený autorizačným zoznamom  . . . . . .   *NONE

                          Objekt
Užívateľ    Skupina      Oprávnenie
OWNCP                    *ALL
DPTSM                    *USE
DPTMG                    *USE
*PUBLIC                  *EXCLUDE
```

Verejné oprávnenie pre oprávnenie nových objektov (CRTAUT) sa neobjaví pri knižnici na obrazovke Upraviť oprávnenie na objekt. Na zobrazenie CRTAUT pri knižnici použite príkaz DSPLIB (Display Library).

Tento postup môžete použiť aj na nastavenie špecifického oprávnenia pre objekt v systéme.

Teraz môžete nastaviť špecifické oprávnenie pre objekt.

Nastavenie špecifického oprávnenia pre objekt

Postup na nastavenie špecifického oprávnenia pre objekt v aplikačnej knižnici je rovnaký ako postup na nastavenie špecifického oprávnenia pre knižnicu. V príklade sa pre knižnicu COPGMLIB v spoločnosti JKL Toy používa formulár Opis knižnice, Časť 2:

Tabuľka 62. formulár Opis knižnice spoločnosti JKL Toy

Skupinový profil alebo užívateľský profil	Názov objektu	Typ objektu	Potrebné oprávnenie	Autorizačný zoznam
PUBLIC	COMSGQ01	*MSGQ	*CHANGE	

1. Napíšte EDTOBJAUT a stlačte **F4** (Výzva).
2. Na obrazovke výzvy doplňte informácie a stlačte kláves **Enter**.
3. Na obrazovke Upraviť oprávnenie na objekt doplňte informácie o oprávneniach a stlačte kláves **Enter**.

```
                          Upraviť oprávnenie na objekt

Objekt . . . . . :   COMSGQ01        Vlastník . . . . . :   OWNCO
  Knižnica . . . . :     COPGMLIB    Primárna skupina . . :   *NONE
Typ objektu  . . . . :   *MSGQ

Napíšte zmeny pre aktuálne oprávnenia, stlačte kláves Enter.

  Objekt je zabezpečený autorizačným zoznamom  . . . . . .   *NONE

                          Objekt
Užívateľ    Skupina      Oprávnenie
OWNCO                   *ALL
*PUBLIC                  *CHANGE
```

Teraz môžete nastaviť oprávnenie pri viacerých objektoch súčasne.

Nastavenie oprávnenia pri viacerých objektoch súčasne

Príkaz EDTOBJAUT bol doteraz v príkladoch používaný na nastavenie špecifického oprávnenia pre jeden objekt. Použite príkaz GRTOBJAUT (Grant Authority) na nastavenie zabezpečenia pre viacero objektov. Napíšte GRTOBJAUT a stlačte **F4** (Výzva). Nasledujú príklady pre vykonanie viacerých zmien pre oprávnenie.

- Polia zadané na nasledujúcej obrazovke nastavujú verejné oprávnenie pre všetky fronty správ v knižnici CUSTLIB na *CHANGE.

```
                     Prideliť oprávnenie na objekt (GRTOBJAUT)

Napíšte voľby, stlačte kláves Enter.

Objekt . . . . . .   *ALL
  Knižnica . . . . . .    CUSTLIB
Typ objektu  . . . . . .   *MSGq
Užívatelia . . . . . .   *PUBLIC
             + pre viac hodnôt
Oprávnenie . . . . . .   *CHANGE
```

- Polia zadané na nasledujúcej obrazovke dávajú oprávnenie *ALL pre všetky súbory, názvy ktorých začínajú znakmi WRK, v knižnici CUSTLIB pre užívateľa AMES.

```
                    Prideliť oprávnenie na objekt

Napíšte voľby, stlačte kláves Enter.

Objekt . . . . . .   WRK*
  Knižnica . . . . . .    CUSTLIB
Typ objektu  . . . . . .   *FILE
Užívatelia . . . . . .   AMES
             + pre viac hodnôt
Oprávnenie . . . . . .   *ALL
```

Tento príklad používa techniku pre zadávanie parametrov, ktorá sa nazýva **generické** pomenovávanie. Mnohé príkazy vám pri parametri umožnia zadať prvé znaky, za ktorými nasleduje hviezdička (*). Systém vykoná operáciu na každom objekte, názov ktorého začína týmito znakmi. Online informácie pre príkaz udávajú, ktoré parametre povoľujú generické názvy.

- Pre zabezpečenie všetkých súborov, názvy ktorých začínajú znakmi AR a používajú autorizačný zoznam s názvom ARLST1 a na to, aby súbory získali svoje verejné oprávnenie zo zoznamu budete musieť vykonať dva kroky. Tieto obrazovky ukazujú požadované kroky.

```
                    Prideliť oprávnenie na objekt

Napíšte voľby, stlačte kláves Enter.

Objekt . . . . . .   AR*
  Knižnica . . . . . .    CUSTLIB
Typ objektu  . . . . . .   *FILE

   :
Autorizačný zoznam . . . . . .   ARLST1
```

```
                    Prideliť oprávnenie na objekt

Napíšte voľby, stlačte kláves Enter.

Objekt . . . . . .   AR*
  Knižnica . . . . . .    CUSTLIB
Typ objektu  . . . . . .   *FILE
Užívatelia . . . . . .   *PUBLIC
             + pre viac hodnôt
Oprávnenie . . . . . .   *AUTL
             + pre viac hodnôt
```

Príkaz DSPJOBLOG použite podľa opisu v téme ″Použitie protokolu úlohy na kontrolu vašej práce,″ aby ste si overili, či systém vykonal požadované zmeny oprávnení.

Skôr než prejdete na tému ″Zabezpečenie tlačového výstupu″ použite príkaz EDTOBJAUT alebo príkaz GRTOBJAUT na nastavenie špecifických oprávnení v Časti 2 vášho formulára Opis knižnice.

Zabezpečenie tlačového výstupu

Po nastavení špecifických oprávnení, môžete dôverný tlačový výstup ochrániť použitím informácií z týchto tém:

- Vytvorenie výstupného frontu a dohľad nad tým, kto ho môže riadiť.
- Priradenie špeciálneho tlačového výstupu pre front.

Vytvorenie výstupného frontu

1. Napíšte CRTOUTQ (Create Output Queue) a stlačte **F4** (Výzva).
2. Doplňte názov výstupného frontu a knižnice.
3. Stlačte **F10** (Ďalšie parametre).
4. Posúvajte sa o stránku nižšie, aby ste našli informácie o zabezpečení tohto výstupného frontu.

```
                  Vytvoriť výstupný front (CRTOUTQ)

Napíšte voľby, stlačte kláves Enter.

Výstupný front . . . . . >   NEWCP
  Knižnica . . . . . .       CONTRACTS
Maximálna veľkosť spoolového súboru
  Počet stránok    . . . . . .   *NONE         Číslo,  *NONE
  Čas spustenia  . . . . . .                  Čas
  Čas ukončenia  . . . . . .                  Čas
            + pre viac hodnôt
Poradie súborov vo fronte  . . .   *FIFO
Vzdialený systém   . . . . . .   *NONE

   ⋮
Textový 'opis'  . . . . . .   Front pre nové zmluvy
```

5. Doplňte informácie zo svojho formulára Výstupný front a zabezpečenie pracovnej stanice, aby ste mali dohľad nad tým, kto môže výstupný front riadiť.
6. Stlačte kláves **Enter** a skontrolujte potvrdzovacie správy.

```
                    Vytvoriť výstupný front (CRTOUTQ)

Napíšte voľby, stlačte kláves Enter.


Ďalšie parametre

Zobraziť ľubovoľný súbor . . . .   *NO
Oddeľovače úloh  . . . . . .   0
Riadený operátorom   . . . . . .   *NO
Front údajov . . . . . .   *NONE
  Knižnica . . . . . .
Oprávnenie na kontrolu . . . . .   *OWNER
Oprávnenie . . . . . .   *LIBCRTAUT
```

Možná chyba	Obnova
Namiesto klávesu **F10** ste stlačili kláves **Enter**.	Na zadanie ďalších informácií použite príkaz CHGOUTQ (Change Output Queue).
Výstupný front ste vytvorili v nesprávnej knižnici.	Na jeho presun do správnej knižnice použite príkaz MOVOBJ (Move Object).

Teraz môžete tlačový výstup priradiť pre výstupný front.

Priradenie tlačového výstupu pre výstupný front

Po vytvorení výstupného frontu, môžete tlačový výstup priradiť výstupnému frontu. Cieľ tlačového výstupu zvyčajne riadi súbor tlačiarne. Spolu s poskytovateľom vašich aplikácií vyhľadajte názvy a knižnice súborov tlačiarne pre dôverné správy.

Ak k týmto informáciám nemáte prístup, správu vytlačte a pozastavte ju vo výstupnom fronte. Na obrazovke Pracovať so spoolovými súbormi použite voľbu atribútov, aby ste našli názov súboru tlačiarne. Súbor tlačiarne sa objaví v poli *Súbor zariadenia* na obrazovke Pracovať s atribútmi spoolového súboru.

Ak chcete zmeniť cieľ (výstupný front) súboru tlačiarne, použite príkaz Change Printer File (CHGPRTF):

```
CHGPRTF FILE(názov-knižnice/názov-súboru-tlačiarne)
        OUTQ(názov-knižnice/názov-výstupného-frontu)
```

Správa prejde do nového miesta určenia vždy, keď si správu niekto opäť vyžiada. Ak chcete zmeniť cieľ pre spoolový súbor, ktorý sa už vo výstupnom fronte nachádza, použite voľbu Zmeniť na obrazovke Pracovať so spoolovými súbormi.

Napríklad Sharon Jones zo spoločnosti JKL Toy chce priradiť súbor tlačiarne cenník PRCLST1 výstupnému frontu PRICEQ. Napíše:

```
CHGPRTF FILE(CONTRACTS/PRCLST1) OUTQ(CONTRACTS/PRICEQ)
```

Ak chce Sharon priradiť všetky správy cenníkov do výstupného frontu PRICEQ, mohla by použiť generický názov súboru tlačiarne:

```
CHGPRTF FILE(CONTRACTS/PRCLST*) OUTQ(CONTRACTS/PRICEQ)
```

Ak chce smerovať všetky nové zmluvy do výstupného frontu NEWCP, Sharon by mohla zmeniť výstupný front pridružený k vzorovému dokumentu, ktorý sa používa na vytváranie zmlúv.

Kontrola vašej práce

Najlepší spôsob ako si skontrolovať svoju stratégiu ochrany dôverného tlačového výstupu je jeho vytlačenie. Skontrolujte, či sa radí do správneho výstupného frontu. Prihláste sa ako operátor systému a zistite, či sa môžete pozrieť alebo narábať so súbormi vo fronte.

Skôr než zabezpečíte pracovné stanice, uistite sa, či ste:

- Použitím príkazu CRTOUTQ vytvorili všetky výstupné fronty, uvedené vo vašom formulári Výstupný front a zabezpečenie pracovnej stanice.
- Pomocou príkazu CHGPRTF priradili tlačový výstup pre nové výstupné fronty.

Zabezpečenie pracovných staníc

Po zabezpečení tlačového výstupu by ste mali zabezpečiť svoje pracovné stanice. Pracovné stanice autorizujete presne tak, ako autorizujete ostatné objekty v systéme. Príkaz EDTOBJAUT použite na udelenie oprávnenia pre pracovné stanice.

Ak sa chcú užívatelia prihlásiť na pracovnú stanicu, musia mať oprávnenie *CHANGE. Ak má systémová hodnota QLMTSECOFR hodnotu nie (0), správca bezpečnosti alebo ktokoľvek s oprávnením *ALLOBJ sa môže prihlásiť na ľubovoľnú pracovnú stanicu.

Ak má systémová hodnota QLMTSECOFR hodnotu áno (1), na nastavenie oprávnenia pre pracovné stanice použite tento návod:

Užívatelia s povolením prihlásiť sa na pracovnú stanicu	Verejné oprávnenie	oprávnenie QSECOFR	Oprávnenie konkrétneho užívateľa
Všetci užívatelia	*CHANGE	*CHANGE	Nevyžaduje sa
Iba vybratí užívatelia	*EXCLUDE	Bez oprávnenia	*CHANGE
Vybraní užívatelia a užívatelia s oprávnením na všetky objekty	*EXCLUDE	*CHANGE	*CHANGE
Všetci užívatelia okrem užívateľov s oprávnením na všetky objekty	*CHANGE	Bez oprávnenia	Nevyžaduje sa

Predtým ako obmedzíte prístup do frontu správ operátora systému, použite na zabezpečenie pracovnej stanice príkaz EDTOBJAUT, na základe informácií vo vašom výstupnom fronte a formulári zabezpečenia pracovných staníc.

Obmedzenie prístupu do frontu správ operátora systému

Zabezpečenie môžete vylepšiť zabezpečením tlačového výstupu, zabezpečením pracovných staníc a obmedzením prístupu do frontu správ operátora systému.

Voľba pre zaobchádzanie so správami v ponuke ASSIST umožňuje užívateľom na zobrazenie frontu správ operátora systému (QSYSOPR) použiť funkčný kláves. Nesprávne odpovede na správy operátora systému môžu spôsobiť problémy vo vašom systéme. Pre odpoveď na správy a na vymazanie správ vo fronte správ sa od užívateľov vyžaduje oprávnenie *CHANGE. Toto oprávnenie by mali mať iba operátori systému. Pozrite sa do formulára Zodpovednosti systému, aby ste zistili kto by mal mať oprávnenie *CHANGE pre front správ operátora systému.

Použite príkaz EDTOBJAUT:

1. Napíšte EDTOBJAUT QSYSOPR *MSGQ a stlačte kláves **Enter**.
2. Ak chcete zobraziť podrobné informácie o oprávneniach na objekt, stlačte **F11**.
3. Udeľte verejné oprávnenie *OBJOPR, ako je ukázané na vzorovej obrazovke, stlačte kláves **Enter**.

```
                          Upraviť oprávnenie na objekt

Objekt . . . . . :   QSYSOPR         Vlastník . . . . . :   QSYS
  Knižnica . . . . . :     QSYS          Primárna skupina . . :   *NONE
Typ objektu  . . . . :  *MSGQ

Napíšte zmeny pre aktuálne oprávnenia, stlačte kláves Enter.

  Objekt je zabezpečený autorizačným zoznamom  . . . . . .   *NONE

                         Objekt    ----------Objekt-----------
Užívateľ    Skupina     Oprávnenie Opr  Mgt  Exist  Alter  Ref
*PUBLIC                 USER DEF    X
```

4. Systém zmení stĺpec *Oprávnenie na objekt* na USER DEF (Užívateľom definované).
5. Opäť stlačte **F11**, aby sa zobrazili podrobné informácie o oprávneniach na údaje.
6. Udeľte verejné oprávnenie *ADD, ako je ukázané na vzorovej obrazovke a stlačte kláves **Enter**.

```
                          Upraviť oprávnenie na objekt

Objekt . . . . . :   QSYSOPR         Vlastník . . . . . :   QSYS
  Knižnica . . . . . :     QSYS          Primárna skupina . . :   *NONE
Typ objektu  . . . . :  *MSGQ

Napíšte zmeny pre aktuálne oprávnenia, stlačte kláves Enter.

  Objekt je zabezpečený autorizačným zoznamom  . . . . . .   *NONE

                         Objekt    ----------------------Údaje----------------------
Užívateľ    Skupina    Oprávnenie  Čítať  Pridať  Aktualizovať  Vymazať  Vykonať
*PUBLIC                 USER DEF            X
```

7. **F6** (Pridať užívateľov) použite na pridanie užívateľov, ktorí potrebujú odpovedať na správy QSYSOPR. Udeľte im oprávnenie *CHANGE.

Upozornenie: Nevytvárajte verejné oprávnenie *EXCLUDE. Všetky úlohy (a užívatelia) musia mať možnosť pridať správy do frontu správ QSYSOPR.

Ak sa chcete presvedčiť, či ste ukončili nastavenie zabezpečenia prostriedku, mali by ste:

- Použiť vaše formuláre Autorizačný zoznam a vaše formuláre Opis knižnice, aby ste sa uistili, že ste vytvorili zabezpečenie pre všetky svoje aplikačné knižnice.
- Skontrolovať svoj formulár Výstupný front a zabezpečenie pracovnej stanice, aby ste sa uistili, že ste ochránili pracovné stanice a vytvorili všetky špeciálne výstupné fronty.
- Obmedziť prístup do frontu správ operátora systému (QSYSOPR).
- Svoje aplikačné knižnice uložiť podľa pokynov, ktoré boli dodané spolu s aplikáciami. Systém ukladá informácie o vlastníctve a verejnom oprávnení spolu s aplikáciou.
- Príkaz SAVSECDTA (Save Security Data) použiť na uloženie bezpečnostných informácií, ktoré ste vytvorili. Bližšie informácie o tom, ako ukladať bezpečnostné informácie nájdete v téme ″Ukladanie bezpečnostných informácií″.

Teraz môžete začať testovať svoje bezpečnostné nastavenie.

Testovanie zabezpečenia

Táto téma opisuje techniky na testovanie zabezpečenia, ktoré ste nastavili vo vašom systéme. Testovanie v tejto súvislosti znamená presvedčiť sa, či ste všetko, čo ste nastaviť mali, nastavili tak, ako ste chceli. Téma ″Monitorovanie zabezpečenia″ hovorí o vyhodnocovaní efektívnosti zabezpečenia vo vašom systéme.

Vždy, keď vo svojom systéme vykonáte rozsiahlejšie zmeny, otestujte zabezpečenie. Medzi takéto zmeny sa počíta pridanie novej aplikácie, nastavenie zabezpečenia prostriedku pre existujúcu aplikáciu, pridanie novej skupiny užívateľov alebo zmena úrovne zabezpečenia.

Prezrite si nasledujúce témy. Dozviete sa v nich o metódach pre testovanie a pre diagnostiku problémov, keď robíte zmeny v zabezpečení:

- Testovanie užívateľských profilov.
- Testovanie zabezpečenia prostriedku.

Testovanie užívateľských profilov

Ak chcete začať testovať svoje zabezpečenie, vždy budete chcieť testovať užívateľský profil, keď vo svojom systéme nastavíte novú skupinu. Otestujte niektorý z konkrétnych profilov, ktoré ste skopírovali zo skupinového profilu.

- Dokážete sa úspešne prihlásiť s týmto užívateľským profilom? Ak sa nedokážete prihlásiť, skontrolujte protokol úlohy, ktorý bol napísaný pri neúspešnom pokuse o prihlásenie sa. V ponuke ASSIST použite voľbu Pracovať s tlačovým výstupom, aby ste lokalizovali protokol úlohy, v ktorom je viac informácií.

  Najpravdepodobnejšie problémy sú tieto:

  – Niektorý z potrebných objektov, ako napríklad úvodná ponuka, aktuálna knižnica alebo úvodný program, neexistujú.
  – Zoznam knižníc, ktorý je uvedený v opise úlohy, spôsobuje chyby. Buď neexistuje knižnica alebo ste do zoznamu knižníc zabudli zahrnúť QGPL a QTEMP.
  – Užívateľ nemá autorizáciu na pracovnú stanicu.
- Keď sa prihlásite, nezobrazí sa na obrazovke správna úvodná ponuka alebo program?
- Čo sa stane, ak na prihlasovacej obrazovke zadáte úvodnú ponuku alebo aktuálnu knižnicu? Ak má užívateľský profil nastavené Obmedzené schopnosti (YES), mali by ste dostať chybové hlásenie.
- Dostanete správnu obrazovku, keď stlačíte kláves Attention?
- Prichádza výstup do správnej tlačiarne? Ak nie, v ponuke ASSIST použite voľbu Pracovať s tlačovým výstupom, aby ste zistili kam odišiel. Ak chcete určiť, prečo výstup odišiel do inej tlačiarne, skontrolujte užívateľský profil a opis úlohy.
- Dokážete získať príkazový riadok?
- Dokážete vykonať požadované aplikačné funkcie bez chýb v zabezpečení? Viac podrobností nájdete téme ″Testovanie zabezpečenia prostriedku″.
- Dokážete vykonať potrebné systémové úlohy, ako napríklad riadenie tlačiarní alebo ukladanie knižníc?

Ak systém od vás vyžadoval, aby ste po prihlásení s profilom priradili nové heslo, po dokončení testovania nastavte heslo naspäť na názov užívateľského profilu:

1. Prihláste sa pod svojim vlastným profilom (s oprávnením správcu bezpečnosti).
2. Napíšte CHGUSRPRF *názov-profilu* PASSWORD(*názov-profilu*) PWDEXP(*YES).

Teraz, keď ste už otestovali užívateľské profily, môžete otestovať zabezpečenie prostriedku.

Testovanie zabezpečenia prostriedku

Potom, ako ste otestovali užívateľské profily by ste mali otestovať aj zabezpečenie prostriedku. Keď testujete zabezpečenie prostriedku, hľadáte nasledujúce:

- Užívateľov, ktorí nemajú dostatočné oprávnenie pre vykonávanie svojich úloh.
- Užívateľov, ktorí majú väčšie oprávnenie, ako ste chceli.

Testovanie pre zistenie nedostatočných oprávnení

Testujte aj interaktívne aj dávkové funkcie, aby ste zistili, či majú užívateľské profily dostatočné oprávnenie.

Interaktívne testovanie

Ak chcete otestovať zabezpečenie vášho prostriedku pre aplikáciu, možno sa budete musieť prihlásiť s niekoľkými rozdielnymi užívateľskými profilmi. Vašim cieľom bude otestovať vzorových užívateľov, aby ste sa presvedčili, že oprávnenie, ktoré ste priradili je dostatočné.

- Otestujte funkcie, ktoré vyžadujú rôzne úrovne oprávnenia: prezeranie, zmenenie a vymazanie.
- Otestujte programy, nie iba ponuky. Vybratie voľby v ponuke nemusí byť dostatočné na otestovanie oprávnenia. Niekedy systém na súbor nepristúpi, pokiaľ sa skutočne nepokúsite vykonať operáciu, ako napríklad vymazanie záznamu. Kontrola oprávnenia nastáva, keď necháte systém otvoriť súbor. Návrh aplikácie určuje, kedy systém súbor otvorí.
- Zaznamenávajte si chyby v zabezpečení a odstráňte ich. Ak sa vyskytne chyba oprávnenia, na obrazovke by ste mali vidieť správu, ktorá vám povie, že máte nedostatočné oprávnenie pre operáciu a aký objekt ste sa pokúšali použiť.

Dávkové testovanie

- Vzorové dávkové úlohy spustite z aplikácie s použitím profilov užívateľov, ktorí úlohy odovzdajú.
- Otestujte dávkové úlohy, ktoré vyžadujú rozdielne úrovne oprávnení, ako napríklad: tlač informácií, zmena informácií alebo mazanie súborov na konci mesiaca.
- Skontrolujte, či front správ QSYSOPR a protokol QHST neobsahujú chyby zabezpečenia. Príkaz DSPLOG použite na prezeranie protokolu QHST. Správy o zabezpečení majú nasledujúce rozsahy: CPF2200, CPI2200, CPC2200, CPD2200, CPF4A00, CPI4A00, CPC4A00 a CPD4A00.

  Na protokolovanie zlyhaní oprávnenia a ostatných udalostí, ktoré sa týkajú zabezpečenia použite funkciu auditu zabezpečenia.

Testovanie pre zistenie priveľkých oprávnení

Ak ste zabezpečenie prostriedku nastavili na ochranu dôverných informácií, otestujte vzorové užívateľské profily, aby ste sa uistili, že vaše zabezpečenie funguje. Prihláste sa s profilom užívateľa, ktorý by nemal mať prístup k dôverným súborom.

- Môžete sa dostať do ponuky, ktorá vám umožňuje prístup do tohto súboru?
- Čo sa stane, ak vyberiete z ponuky voľbu, ktorá takýto súbor používa?
- Dokážete získať príkazový riadok?
- Dokážete spustiť príkaz na vypísanie súboru, ako napríklad CPYF FROMFILE(*názov-súboru*) TOFILE(QSYSPRT)?
- Dokážete použiť nástroj pre dotazovanie, aby ste sa na súbor pozreli?

Výsledky vášho testovania môžu indikovať, že potrebujete zmeniť bezpečnostné informácie.

Zmena bezpečnostných informácií

Keďže ste si už naplánovali zabezpečenie svojho systému potrebujete sa uistiť, že váš plán zostane účinný aj pri zmenách, ktoré bude vyžadovať vaše podnikanie.

Táto téma pri navrhovaní zabezpečenia zdôrazňuje ako najdôležitejší cieľ jednoduchosť. Skupiny užívateľov ste navrhli ako vzory pre konkrétnych užívateľov. Radšej ste sa pokúsili použiť verejné oprávnenie, autorizačné zoznamy a oprávnenie na knižnicu ako špecifické konkrétne oprávnenia. Využite výhodu tohto prístupu pri riadení zabezpečenia:

- Keď pridáte novú skupinu užívateľov alebo novú aplikáciu, použite techniky, ktoré ste použili na plánovanie zabezpečenia.
- Keď potrebujete vykonať zmeny v zabezpečení, radšej sa pokúste použiť všeobecný prístup ako vytváranie výnimiek pre riešenie špecifických problémov.

Téma Príkazy zabezpečenia opisuje príkazy, ktoré sa majú použiť na zobrazenie, zmenu a vymazanie bezpečnostných informácií.

Pozrite si nasledujúce témy. Nájdete v nich návrhy pre zaobchádzanie s rôznymi typmi zmien:

- Pridanie nového užívateľa do systému.
- Vytvorenie novej skupiny užívateľov.
- Zmena skupiny užívateľov.
- Pridanie novej applikácie.
- Pridanie novej pracovnej stanice.
- Zmena užívateľskej zodpovednosti.
- Odstránenie užívateľa zo systému.

Príkazy zabezpečenia

Tabuľka nižšie ukazuje príkazy, ktoré používate na prácu s objektmi zabezpečenia v systéme. Tieto príkazy môžete použiť na vykonanie týchto úloh:

- Prezeranie a výpis bezpečnostných informácií.
- Zmena bezpečnostných informácií.
- Vymazanie bezpečnostných informácií.

Tabuľka 63. Príkazy zabezpečenia

Objekt zabezpečenia	Ako prezerať	Ako zmeniť	Ako vymazať
Systémová hodnota	WRKSYSVAL DSPSYSVAL	WRKSYSVAL CHGSYSVAL	Nedá sa vymazať
Opis úlohy	WRKJOBD DSPJOBD	WRKJOBD CHGJOBD	DLTJOBD
Skupinový profil	WRKUSRPRF DSPUSRPRF DSPAUTUSR	WRKUSRPRF CHGUSRPRF	DLTUSRPRF[1],[2]
Užívateľský profil	WRKUSRPRF DSPUSRPRF DSPAUTUSR	WRKUSRPRF CHGUSRPRF CHGUSRAUD	DLTUSRPRF[1]
Oprávnenia na objekt	DSPAUT DSPOBJAUT DSPUSRPRF TYPE(*OBJAUT)	CHGAUT EDTOBJAUT GRTOBJAUT WRKAUT	EDTOBJAUT RVKOBJAUT WRKAUT
Vlastníctvo objektu	WRKOBJOWN DSPOBJAUT DSPUSRPRF TYPE(*OBJOWN)	CHGOBJOWN CHGOWN	CHGOBJOWN CHGOWN vám umožňuje zrušiť práva predchádzajúceho vlastníka.
Primárna skupina	DSPOBJAUT WRKOBJPGP DSPUSRPRF TYPE(*OBJPGP)	CHGOBJPGP CHGPGP	CHGOBJPGP CHGPGP nastaviť primárnu skupinu na *NONE
Audit objektu	DSPOBJD	CHGOBJAUD CHGAUD	CHGOBJAUD (nastaviť na *NONE) CHGAUD
Autorizačný zoznam	DSPAUTL DSPAUTLOBJ	EDTAUTL (užívateľské oprávnenie pre zoznam) EDTOBJAUT (objekt zabezpečený pomocou zoznamu) ADDAUTLE CHGAUTLE GRTOBJAUT	DLTAUTL (celý zoznam)[3] RMVAUTLE (odstrániť užívateľské oprávnenie pre zoznam) EDTOBJAUT (objekt zabezpečený pomocou zoznamu) RVKOBJAUT

Tabuľka 63. Príkazy zabezpečenia (pokračovanie)

Objekt zabezpečenia	Ako prezerať	Ako zmeniť	Ako vymazať

1. IBM odporúča pre vymazanie profilu voľbu odstránenia z obrazovky Work with User Enrollment. Použitie tejto voľby vám umožní vymazať všetky objekty, ktoré profil vlastní, alebo ich môžete nanovo priradiť novému vlastníkovi. Určité parametre príkazu DLTUSRPRF vám umožnia vymazať všetky objekty, ktoré užívateľ vlastní, alebo ich nanovo priradiť novému vlastníkovi. Profil nemôžete vymazať pokiaľ nevymažete alebo nanovo nepriradíte objekty, ktoré vlastní. Takisto nemôžete vymazať profil, ktorý je primárnou skupinou pre nejaké objekty.
2. Nemôžete vymazať skupinový profil, ktorý obsahuje nejakých členov. Na vypísanie členov skupiny použite voľbu *GRPMBR príkazu DSPUSRPRF. Skôr než skupinový profil vymažete, zmeňte pole *skupinový profil* vo všetkých konkrétnych skupinových profiloch.
3. Nemôžete vymazať autorizačný zoznam, ktorý sa používa na zabezpečenie objektov. Na vypísanie objektov, ktoré sú zabezpečené pomocou zoznamu, použite príkaz DSPAUTLOBJ. Oprávnenie na ľubovoľné objekty, ktoré sú zabezpečené pomocou zoznamu, zmeňte použitím príkazu EDTOBJAUT.

Prezeranie a výpis bezpečnostných informácií

Bezpečnostné informácie môžete vypísať použitím príkazu na zobrazenie (DSP) s voľbou tlače (*PRINT). Napríklad, ak chcete zobraziť autorizačný zoznam s názvom MYLIST, napíšte DSPAUTL MYLIST *PRINT.

Niektoré príkazy na zobrazenie poskytujú voľby pre rôzne typy zoznamov. Napríklad, keď ste vytvorili konkrétne užívateľské profily, na vypísanie všetkých členov skupinového profilu ste použili voľbu *GRPMBR príkazu DSPUSRPRF. Ak chcete zistiť, ktoré zoznamy sú dostupné pre objekty zabezpečenia, používajte vyvolanie výzvy (**F4**) a online informácie.

príkazy Display môžete použiť na prezeranie bezpečnostných informácií na vašej pracovnej stanici. Môžete použiť aj príkazy WRK (Work with...), ktoré poskytujú viac funkcií. Príkazy Work with... vám dajú obrazovku zoznamu. Túto obrazovku môžete použiť na zmenu, vymazanie a prezeranie informácií.

Na výpis alebo prezeranie informácií s použitím generických názvov môžete použiť aj príkazy zabezpečenia. Ak napíšete WRKUSRPRF DPT*, vaša obrazovka Pracovať so zaradením užívateľa alebo Pracovať s užívateľským profilom ukáže iba profily, ktoré sa začínajú znakmi *DPT*. Ak chcete zistiť, ktoré parametre povoľujú generické názvy, použite online informácie pre príkaz.

Zmena bezpečnostných informácií

Bezpečnostné informácie môžete zmeniť interaktívne použitím príkazu WRK (Work with...) alebo príkazu EDT (Edit...). Informácie si môžete prezerať, zmeniť ich a znova si ich prezrieť po vykonaní zmien.

Bezpečnostné informácie môžete zmeniť aj bez ich prezerania pred a po zmene, ak použijete príkaz CHG (Change...) alebo GRT (Grant...). Táto metóda je užitočná hlavne pri vykonávaní zmien vo viacerých objektoch súčasne. Napríklad, príkaz GRTOBJAUT sta použili na nastavenie verejného oprávnenia pre všetky objekty v knižnici (pozrite si “Nastavenie verejného oprávnenia pre všetky objekty v knižnici” na strane 93).

Vymazanie bezpečnostných informácií

Určité typy bezpečnostných informácií môžete vymazať alebo odstrániť interaktívne, použitím príkazov WRK (Work with...) alebo EDT (Edit...). Na vymazanie bezpečnostných informácií môžete použiť aj príkazy DLT (Delete...), RMV (Remove...) a RVK (Revoke...). Skôr než vám systém umožní vymazať bezpečnostné informácie, musíte častokrát spĺňať určité podmienky. Poznámky v téme Príkazy zabezpečenia opisujú niektoré z týchto podmienok.

Pridanie nového užívateľa do systému

Keď potrebujete do systému pridať nového užívateľa, použite nasledujúci postup:

1. Priraďte osobu k skupine užívateľov. Ako pomôcku použite formulár Opis skupiny užívateľov.
2. Rozhodnite, či nový užívateľ potrebuje vykonávať systémové funkcie. Ak áno, pridajte tieto informácie do formulára Zodpovednosti systému.
3. Pridajte osobu do formulára Konkrétny užívateľský profil.

4. Prezrite si formulár Zodpovednosti systému a formulár Opis skupiny užívateľov, aby ste určili, či nový užívateľ potrebuje hodnoty, ktoré sú iné ako hodnoty skupiny.
5. Skopírovaním skupinového profilu alebo profilu člena skupiny vytvorte užívateľský profil. Nezabudnite nastaviť uplynutie platnosti hesla. (Pozrite si tému ″Kopírovanie skupinového profilu.″)
6. Novému užívateľovi dajte kópiu vášho memoranda o zabezpečení.

Ak sa chcete dozvedieť, ako máte vytvoriť novú skupinu užívateľov, pozrite si tému″Vytvorenie novej skupiny užívateľov.″

Vytvorenie novej skupiny užívateľov

Potreba vytvorenia novej skupiny užívateľov môže mať niekoľko príčin:

- Systém potrebujú používať ďalšie oddelenia.
- Zistili ste, že potrebujete mať špecifickejšie skupiny užívateľov, aby spĺňali vaše potreby zabezpečenia prostriedkov.
- Vaša spoločnosť reorganizovala niektoré oddelenia.

Ak chcete vytvoriť novú skupinu užívateľov, urobte nasledovné:

1. Podľa pokynov v téme ″Plánovanie skupín užívateľov″ vyplňte Formulár opisu skupiny užívateľov.
2. Novú skupinu užívateľov pridajte do svojho diagramu aplikácií, knižníc a skupín dokumentov.
3. Vyhodnoťte, či niektorí členovia skupiny potrebujú vykonávať systémové funkcie. Aktualizujte svoj formulár Zodpovednosti systému. (Pozrite si tému ″Určenie toho, kto by mal zodpovedať za systémové funkcie.″)
4. Ak chcete vyplniť formulár Konkrétny užívateľský profil, použite na to informácie z formulára Opis skupiny užívateľov a z formulára Zodpovednosti systému.
5. Vytvorte knižnicu skupiny.
6. Vytvorte opis úlohy pre skupinu.
7. Vytvorte skupinový profil.

   Poznámka: Pozrite si tému ″Nastavenie skupín užívateľov,″ kde nájdete pokyny na vykonanie krokov päť, šesť a sedem.
8. Vytvorte konkrétne užívateľské profily pre členov skupiny. (Pozrite si tému ″Nastavenie konkrétnych užívateľov.″)
9. Vyhodnoťte formuláre Opis knižnice pre všetky aplikácie, ktoré skupiny potrebuje. Urobte všetky potrebné kroky na udelenie skupinového prístupu na aplikačné objekty s použitím techník, ktoré sú popísané v téme ″Nastavenie zabezpečenia prostriedku.″
10. Všetkým členom skupiny dajte kópiu vášho memoranda o zabezpečení.

Ak sa chcete dozvedieť, ako zmeniť skupinu užívateľov, pozrite si tému ″Zmena skupiny užívateľov.″

Zmena skupiny užívateľov

Budete musieť spracovávať rôzne typy zmien v charakteristikách skupiny, rôznymi spôsobmi. Nasleduje niekoľko príkladov na zmeny a spôsob, ako sa s nimi vysporiadať:

Zmena skupinového oprávnenia

môžete zistiť, že skupina potrebuje oprávnenie na objekty, s ktorými ste vo svojom úvodnom plánovaní nepočítali. Urobte nasledovné:

1. Príkaz EDTOBJAUT (Edit Object Authority) použite, aby skupina dostala správny prístup na objekty alebo na príslušný autorizačný zoznam. “Nastavenie špecifických oprávnení” na strane 98 ukazuje príklad, ako sa to dá urobiť. Keď udelíte skupinové oprávnenie, každý člen skupiny dostane oprávnenie pre objekt.
2. Ak pridelíte skupinové oprávnenie pre dôverný prostriedok, možno si budete chcieť overiť aktuálnych členov v skupine. Príkaz Display User Profile (DSPUSRPRF *názov-skupinového-profilu* *GRPMBR) použite na vypísanie členov skupiny.

Zmena prispôsobenia pre skupinu

Možno budete pre členov skupiny potrebovať zmeniť nastavenie užívateľského prostredia. Napríklad, ak oddelenie dostane svoju vlastnú tlačiareň, budete chcieť, aby sa nová tlačiareň stala štandardnou pre členov skupiny užívateľov takéhoto oddelenia. Alebo, keď bude do vášho systému nainštalovaná nová aplikácia, členovia skupiny užívateľov môžu chcieť rozdielne úvodné ponuky, keď sa prihlásia.

Skupinový profil poskytuje vzor, ktorý môžete skopírovať, aby ste vytvorili konkrétne profily pre členov skupiny. Hodnoty prispôsobenia v skupinovom profile však nemajú vplyv na konkrétne užívateľské profily, keď už sú vytvorené. Napríklad, zmena poľa, ako *Tlačové zariadenie*, v skupinovom profile nemá vplyv na členov skupiny. Pole *Tlačové zariadenie* musíte zmeniť v každom konkrétnom užívateľskom profile.

Obrazovku Pracovať s užívateľským profilom môžete použiť na zmenu parametra pre viacero užívateľov súčasne. V príklade je ukázaná zmena výstupného frontu pre všetkých členov skupiny:

1. Napíšte WRKUSRPRF *ALL a stlačte kláves **Enter**.
2. Ak vidíte obrazovku Pracovať so zaradením užívateľa, použite **F21** (Vybrať úroveň pomoci), aby ste prešli na obrazovku Pracovať s užívateľským profilom.

```
                          Pracovať s užívateľskými profilmi

Napíšte voľby, stlačte kláves Enter.
  1=Vytvoriť   2=Zmeniť   3=Kopírovať   4=Vymazať   5=Zobraziť
  12=Pracovať s objektmi podľa vlastníka

          Užívateľ
Vol       Profil        Text

                HARRISOK         Harrison, Keith
2               HOGANR           Hogan, Richard
                JONESS           Jones, Sharon
2               WILLISR          Willis, Rose

   ⋮                                                                  Viac...
Parametre pre voľby 1, 2, 3, 4 a 5 alebo príkaz
===> PRTDEV(PRT02)
F3=Ukončiť   F5=Obnoviť   F12=Zrušiť   F16=Zopakovať umiestnenie na   F17=Umiestniť na
F21=Vybrať úroveň pomoci         F24=Viac klávesov
```

3. Vedľa každého profilu, ktorý chcete zmeniť napíšte **2** (Zmeniť).
4. Do riadka parametrov na konci obrazovky napíšte názov parametra a novú hodnotu. Ak názov parametra nepoznáte, stlačte **F4** (Výzva).
5. Stlačte kláves **Enter**. Pre každý zmenený profil dostanete potvrdzovaciu správu.

   Hoci zmena poľa prispôsobenia v skupinovom profile nemá žiadny vplyv na členov skupiny, môže vám pomôcť v budúcnosti. Keď chcete pridať členov do skupiny neskôr, skupinový profil poskytne vzor. Okrem toho je aj záznamom hodnôt štandardných polí pre skupinu.

Udelenie skupinového prístupu do novej aplikácie

Keď skupina užívateľov potrebuje prístup do novej aplikácie, musíte analyzovať informácie o skupine a o aplikácii. Nasleduje navrhovaná metóda:

1. Pozrite sa do formulára Opis aplikácie pre novú aplikáciu a do svojho diagram aplikácií, knižníc a skupín užívateľov, aby ste videli knižnice, ktoré aplikácia používa. Tieto knižnice pridajte do formulára Opis skupiny užívateľov.
2. Aktualizujte svoj diagram aplikácií, knižníc a skupín užívateľov, aby sa ukázali nové vzťahy medzi skupinou užívateľov a aplikáciou.

3. Ak by mal úvodný zoznam knižníc skupiny obsahovať knižnice, opis skupinovej úlohy zmeňte použitím príkazu CHGJOBD (Change Job Description). Ak potrebujete pomoc pri práci s opismi úloh, pozrite si “Vytváranie opisu úlohy” na strane 81.

   Poznámka: Keď pridávate knižnice do úvodného zoznamu knižníc v opise úlohy, nemusíte meniť užívateľské profily, ktoré používajú opis úlohy. Pri nasledujúcom prihlásení sa užívateľov budú do ich úvodného zoznamu knižníc tieto knižnice automaticky pridané.
4. Vyhodnoťte, či potrebujete pre skupinu zmeniť buď úvodný program alebo úvodnú ponuku, aby sa zabezpečil prístup do novej aplikácie. Použitím príkazu CHGUSRPRF musíte vykonať konkrétnu zmenu v úvodnej ponuke alebo programe každého užívateľského profilu.
5. Prezrite formuláre Opis knižnice, pre všetky knižnice, ktoré aplikácia používa. Určite, či je verejný prístup, ktorý je k dispozícii pre knižnice, dostatočný pre potreby skupiny. Ak nie je, možno budete musieť dať skupinové oprávnenie knižnici, špecifickým objektom alebo autorizačným zoznamom. Ak to chcete urobiť, použite na to príkazy EDTOBJAUT (Use the Edit Object Authority) a EDTAUTL (Edit Authorization List). (Ak potrebujete viac informácií, pozrite si tému ″Nastavenie zabezpečenia prostriedku.″)

Ak chcete do vášho systému pridať aplikácie, pozrite si tému ″Pridanie novej aplikácie.″

Pridanie novej aplikácie

Zabezpečenie pre všetky nové aplikácie by ste mali plánovať rovnako starostlivo, ako ste plánovali zabezpečenie vašich pôvodných aplikácií. Dodržiavajte rovnaké postupy:

1. Pre aplikáciu pripravte formulár Opis aplikácie a formuláre Opis knižnice.
2. Aktualizujte svoj diagram aplikácií, knižníc a skupín užívateľov.
3. Postupujte podľa postupov v téme ″Plánovanie zabezpečenia prostriedku″, aby ste sa rozhodli, ako novú aplikáciu zabezpečíte.
4. Formulár Inštalácia aplikácií pripravte metódou, ktorú opisuje téma ″Plánovanie inštalácie vašich aplikácií.″
5. Vyhodnoťte, či je niektorý tlačový výstup z aplikácie dôverný a potrebuje ochranu. Ak je to potrebné, aktualizujte svoj formulár Výstupný front a zabezpečenie pracovnej stanice.
6. Postupujte podľa krokov, popísaných v téme ″Nastavenie vlastníctva a verejného oprávnenia″ a ″Nastavenie zabezpečenia prostriedku,″ aby ste aplikáciu mohli nainštalovať a zabezpečiť.

Ak chcete do svojho systému pridať pracovnú stanicu, pozrite si tému ″Pridanie novej pracovnej stanice.″

Pridanie novej pracovnej stanice

Keď do systému pridáte novú pracovnú stanicu, zvážte požiadavky na zabezpečenie:

1. Predstavuje fyzické umiestnenie novej pracovnej stanice nejaké bezpečnostné riziká? (Pozrite si tému ″Plánovanie fyzického zabezpečenia,″ aby ste si oživili pamäť.)
2. Ak pracovná stanica nepredstavuje riziko, aktualizujte svoj formulár Výstupný front a zabezpečenie pracovnej stanice.
3. Normálne by ste mali nové pracovné stanice vytvoriť s verejným oprávnením *CHANGE. Ak to nespĺňa požiadavky na vaše zabezpečenie pre pracovnú stanicu, na zadanie iného oprávnenia použite príkaz EDTOBJAUT.

Ak chcete v systéme zmeniť užívateľskú zodpovednosť, pozrite si tému ″Zmena užívateľských zodpovedností.″

Zmena užívateľských zodpovedností

Keď užívateľ systému vo vašej spoločnosti dostane novú úlohu alebo novú sadu zodpovedností, musíte vyhodnotiť, aký to bude mať vplyv na užívateľský profil.

1. Mal by užívateľ patriť k inej skupine užívateľov? Na zmenu skupiny užívateľov môžete použiť príkaz CHGUSRPRF.
2. Potrebujte v profile zmeniť niektoré hodnoty prispôsobenia, ako napríklad tlačiareň alebo úvodnú ponuku? Aj na zmenu týchto hodnôt môžete použiť príkaz CHGUSRPRF.

3. Sú aplikačné oprávnenia novej skupiny užívateľov dostatočné pre túto osobu?
   - Príkaz DSPUSRPRF (Display User Profile) použite na pozretie oprávnení pre starý a nový skupinový profil.
   - Pozrite sa aj na oprávnenia konkrétneho užívateľského profilu.
   - Použitím príkazu EDTOBJAUT vykonajte všetky potrebné zmeny.
4. Vlastní užívateľ nejaké objekty? Mali by ste zmeniť vlastníctvo týchto objektov? Použite príkaz WRKOBJOWN (Work with Objects by Owner).
5. Vykonáva užívateľ systémové funkcie? Potrebuje užívateľ vykonávať systémové funkcie pre novú úlohu? Aktualizujte formulár Zodpovednosti systému, a ak je to potrebné, zmeňte užívateľský profil.

Ak sa chcete dozvedieť, ako máte odstrániť užívateľa zo systému, pozrite si tému ″Odstránenie užívateľa zo systému.″

Odstránenie užívateľa zo systému

Ak niekto vašu spoločnosť opustí, mali by ste zo systému okamžite odstrániť užívateľský profil. Predtým, ako môžete užívateľský profil vymazať, musíte buď vymazať alebo presunúť vlastníctvo všetkých objektov, ktoré profil vlastní. Môžete na to použiť príkaz WRKOBJOWN alebo môžete použiť voľbu **4** (Odstrániť) na obrazovke Pracovať so zaradením užívateľa.

Keď pri profile vyberiete, na obrazovke Pracovať so zaradením užívateľa, voľbu **4** (Odstrániť), uvidíte ďalšie obrazovky, ktoré vám umožnia narábať so všetkými objektmi, ktoré užívateľ vlastní. Môžete si vybrať, že všetky objekty dáte novému vlastníkovi, alebo budete narábať s jednotlivými objektmi:

```
                              Odstrániť užívateľa

Užívateľ . . . . . :   HOGANR
Opis užívateľa . . . . . :   Oddelenie predaja a marketingu

Ak chcete tohto užívateľa odstrániť, nižšie napíšte svoju voľbu, potom stlačte kláves Enter.

    1. Dať všetky objekty, ktoré tento užívateľ vlastní, novému vlastníkovi.
    2. Vymazať alebo zmeniť vlastníka špecifických objektov, ktoré tento užívateľ vlastní.
```

Ak si zvolíte spracovanie jednotlivých objektov (voľba **2**), na obrazovke sa zobrazí zoznam všetkých objektov, ktoré užívateľ vlastní:

```
                              Odstrániť užívateľa

Užívateľ . . . . . :   HOGANR
Opis užívateľa . . . . . :   Oddelenie predaja a marketingu

Nový vlastník . . . . . .                  Meno, F4 pre zobrazenie zoznamu

Ak chcete odstrániť tohto užívateľa, vymažte alebo zmeňte vlastníka všetkých objektov.
Zadajte voľby, stlačte kláves Enter.
  2=Zmeniť na nového vlastníka   4=Vymazať   5=Zobraziť podrobnosti

Vol  Objekt        Knižnica      Opis
 4   HOGANR        QUSRSYS       Front správ pre Richarda Hogana
 4   QUERY1        DPTWH         Dotaz na inventár
```

Ak si vyberiete vymazanie objektov, uvidíte obrazovku Potvrdiť vymazanie. Akonáhle systém objekty vymaže, užívateľský profil môžete odstrániť. Potom znova uvidíte obrazovku Pracovať so zaradením užívateľa, na ktorej bude správa, ktorá vám oznámi, že systém užívateľa odstránil.

Ukladanie bezpečnostných informácií

Táto téma prináša prehľad toho, ako ukladáte a obnovujete bezpečnostné informácie. Keď plánujete zálohu a obnovu svojho systému, musíte pouvažovať o zabezpečení svojich informácií ako aj o samotných informáciách. Pozrite si tému informačného centra Záloha, obnova a dostupnosť, ktorá vám pomôže pri návrhu a vypracovaní plánu pre zálohu a obnovu.

Nasledujúce témy opisujú, ako máte zálohovať a obnoviť bezpečnostné informácie, ktoré ste vytvorili pri nastavení zabezpečenia:

- Ukladanie systémových hodnôt.
- Ukladanie skupinových a užívateľských profilov.
- Ukladanie opisov úloh.
- Ukladanie informácií o zabezpečení prostriedku.
- Použitie profilu štandardného vlastníka (QDFTOWN).
- Obnova z poškodeného autorizačného zoznamu.

Ukladanie systémových hodnôt

Systémové hodnoty sa ukladajú v systémovej knižnici QSYS. Knižnicu QSYS uložíte, keď urobíte nasledovné:

- Použijete príkaz SAVSYS (Save System).
- Z ponuky Uložiť použijete voľbu na uloženie celého systému.
- Z ponuky Uložiť použijete voľbu na uloženie systémových informácií.
- Z ponuky RUNBCKUP (Run Backup) použijete voľbu na zálohovanie celého systému.

Ak potrebujete obnoviť celý systém, vaše systémové hodnoty sa obnovia automaticky, keď obnovíte svoj operačný systém.

Ďalej si pozrite tému ″Ukladanie skupinových a užívateľských profilov.″

Ukladanie skupinových a užívateľských profilov

Skupinové a užívateľské profily sa ukladajú do knižnice QSYS. Uložíte ich, keď použijete príkaz SAVSYS (Save System), alebo ak z ponuky vyberiete voľbu na uloženie celého systému.

Skupinové a užívateľské profily môžete uložiť aj použitím príkazu SAVSECDTA (Save Security Data).

Užívateľské profily uložte použitím príkazu RSTUSRPRF (Restore User Profile). Bežná postupnosť je takáto:

1. Obnovte operačný systém, čím sa obnoví knižnica QSYS.
2. Obnovte užívateľské profily.
3. Obnovte zostávajúce knižnice.
4. Obnovte oprávnenie na objekty použitím príkazu RSTAUT (Restore Authority).

Ďalej si pozrite tému ″Ukladanie opisov úloh.″

Ukladanie opisov úloh

Keď vytvoríte opis úlohy, zadajte knižnicu, v ktorej by mal byť trvalo umiestnený. IBM odporúča vytvárať opisy úloh do knižnice QGPL.

Opisy úloh môžete uložiť tak, že uložíte knižnicu, v ktorej sú trvalo umiestnené. Použite na to príkaz SAVLIB (Save Library). Opis úlohy môžete uložiť aj použitím príkazu SAVOBJ (Save Object).

Obsahy knižnice môžete obnoviť použitím príkazu RSTLIB (Restore Library). Konkrétny opis úlohy môžete obnoviť použitím príkazu RSTOBJ (Restore Object).

Ďalej si pozrite tému ″Ukladanie informácií o zabezpečení prostriedku.″

Ukladanie informácií o zabezpečení prostriedku

Zabezpečenie prostriedku, ktoré definuje, ako môžu užívatelia pracovať s objektmi, sa skladá z rôznych typov informácií, ktoré sa ukladajú na niekoľkých rôznych miestach:

Tabuľka 64. Ukladanie a obnovenie informácií o zabezpečení prostriedku

Typ informácií	Kde sú uložené	Ako sa ukladajú	Ako sa obnovujú
Verejné oprávnenie	S objektom	príkaz SAVxxx [1]	príkaz RSTxxx [2]
Auditovacia hodnota objektu	S objektom	príkaz SAVxxx [1]	príkaz RSTxxx [2]
Vlastníctvo objektu	S objektom	príkaz SAVxxx [1]	príkaz RSTxxx [2]
Primárna skupina	S objektom	príkaz SAVxxx [1]	príkaz RSTxxx [2]
Autorizačný zoznam	knižnica QSYS	SAVSYS alebo SAVSECDTA	RSTUSRPRF USRPRF(*ALL)
Prepojenie medzi objektom a autorizačným zoznamom	S objektom	príkaz SAVxxx [1]	príkaz RSTxxx [2]
Súkromné oprávnenie	S užívateľským profilom	SAVSYS alebo SAVSECDTA	RSTAUT

1. Väčšinu typov objektov môžete uložiť použitím príkazov SAVOBJ alebo SAVLIB. Niektoré typy objektov, ako napríklad konfigurácie, majú osobitné príkazy na uloženie.
2. Väčšinu typov objektov môžete obnoviť použitím príkazov RSTOBJ alebo RSTLIB. Niektoré typy objektov, ako napríklad konfigurácie, majú osobitné príkazy na obnovenie.

Keď potrebujete obnoviť aplikáciu alebo celý svoj systém, kroky, vrátane obnovy oprávnení na objekty, musíte starostlivo naplánovať. Nasledujú základné kroky, ktoré sú potrebné na obnovu informácií o zabezpečení prostriedku pre aplikáciu:

1. Ak je to potrebné, obnovte užívateľské profily, vrátane profilov, ktoré vlastnia aplikáciu. Špecifické profily alebo všetky profily môžete obnoviť príkazom RSTUSRPRF.
2. Obnovte všetky autorizačné zoznamy, ktoré aplikácia používa. Autorizačné zoznamy obnovíte, keď použijete RSTUSRPRF USRPRF(*ALL).

   Poznámka: Z média zálohy sa tak obnovia všetky hodnoty užívateľského profilu, vrátane hesiel.
3. Aplikačné knižnice obnovte použitím príkazu RSTLIB alebo RSTOBJ. Obnoví sa tak vlastníctvo objektov, verejné oprávnenie a prepojenia medzi objektmi a autorizačnými zoznamami.
4. Súkromné oprávnenie na objekty obnovte použitím príkazu RSTAUT. Príkaz RSTAUT obnoví aj užívateľské oprávnenia na autorizačné zoznamy. Môžete obnoviť oprávnenie pre špecifických alebo pre všetkých užívateľov.

Informácie o obnove objektu a profilu vlastníka, ktorý sa nenachádza vo vašom systéme, si pozrite v téme ″Použitie profilu štandardného vlastníka (QDFTOWN).″

Použitie profilu štandardného vlastníka (QDFTOWN)

Ak obnovíte objekt a profil vlastníka sa v systéme nenachádza, systém prevedie vlastníctvo objektu na štandardný profil, ktorý sa nazýva QDFTOWN. Akonáhle obnovíte profil vlastníka alebo ho znova vytvoríte, vlastníctvo môžete previesť naspäť použitím príkazu WRKOBJOWN (Work with Object by Owner).

Informácie o obnove autorizačných záznamov si pozrite v téme ″Obnova z poškodeného autorizačného zoznamu.″

Obnova z poškodeného autorizačného zoznamu

Keď je objekt zabezpečený cez autorizačný zoznam a dôjde k poškodeniu autorizačného zoznamu, na tento objekt budú mať prístup iba užívatelia, ktorí majú mimoriadne oprávnenie na všetky objekty (*ALLOBJ).

Obnova z poškodeného autorizačného zoznamu vyžaduje dva kroky:

1. Obnoviť užívateľov a ich oprávnenia na autorizačnom zozname.

2. Obnoviť pridruženie autorizačného zoznamu k objektom.

Tieto kroky môže vykonať užívateľ s mimoriadnym oprávnením *ALLOBJ.

Kroky 1: Obnovenie autorizačného zoznamu

Ak poznáte užívateľské oprávnenie pre autorizačný zoznam, autorizačný zoznam vymažte, znova ho vytvorte a pridajte doň užívateľov.

Ak nepoznáte všetky užívateľské oprávnenia pre autorizačný zoznam, obnovte ich z vašich posledných pások SAVSYS alebo SAVSECDTA. Postupujte podľa týchto krokov:

1. Vymažte poškodený autorizačný zoznam:
   ```
   DLTAUTL AUTL(názov-autorizačného-zoznamu)
   ```
2. Obnovte autorizačný zoznam:
   ```
   RSTUSRPRF USRPRF(*ALL)
   ```
3. Užívateľov pridajte do zoznamu použitím príkazu RSTAUT (Restore Authority).

Krok 2: Obnovenie pridruženia objektov k autorizačnému zoznamu

Keď ste autorizačný zoznam obnovili alebo ste ho znova vytvorili, potrebujete vytvoriť prepojenie medzi zoznamom a objektmi, ktoré bude zabezpečené zoznamom:

1. Použite príkaz RCLSTG (Reclaim Storage). RCLSTG priradí objekty, ktoré sú zabezpečené poškodenými alebo chýbajúcimi autorizačnými zoznamami, k štandardnému zoznamu s názvom QRCLAUTL.
2. Vypíšte objekty, ktoré sú zabezpečené autorizačným zoznamom QRCLAUTL:
   ```
   DSPAUTLOBJ AUTL(QRCLAUTL)
   ```
3. Príkaz GRTOBJAUT použite na zabezpečenie objektov cez správny autorizačný zoznam. Napríklad, ak chcete zabezpečiť súbor ARWRK01 v knižnici CUSTLIB cez autorizačný zoznam ARLST01, napíšte
   ```
   GRTOBJAUT OBJ(CUSTLIB/ARWRK01) OBJTYPE(*FILE) +
             AUTL(ARLST01)
   ```

Monitorovanie zabezpečenia

Táto téma poskytuje základné návrhy pre monitorovanie efektivity bezpečnostného zabezpečenia vo vašom systéme.

Pravidelné monitorovanie zabezpečenia má dva základné ciele:

- Uistiť sa, že adekvátne chránite prostriedky svojej spoločnosti.
- Zistenie neautorizovaných pokusov o prístup do vášho systému a k firemným informáciám.

Prezrite si svoje vyhlásenie o bezpečnostnej politike a svoje memorandum užívateľom o bezpečnosti, aby ste rozhodli, ktoré úlohy monitorovania potrebujete vykonávať pravidelne.

Bližšie informácie o monitorovaní zabezpečenia nájdete v nasledujúcich témach:

- Kontrolné zoznamy pre monitorovanie zabezpečenia.
- Audit bezpečnosti.

Kontrolné zoznamy pre monitorovanie zabezpečenia

Nasledujú kontrolné zoznamy pre revíziu rôznych hľadísk zabezpečenia vo vašom systéme. Použite ich na vytvorenie svojho plánu.

Monitorovanie fyzického zabezpečenia

- Ochráňte médiá zálohy pred poškodením a krádežou.

- Obmedzte prístup na pracovné stanice vo verejných priestoroch. Príkaz DSPOBJAUT použite, aby ste zistili kto má oprávnenie *CHANGE na pracovné stanice.

Monitorovanie systémových hodnôt

- Overte, či sa nastavenia zhodujú s vašim formulárom Výber systémových hodnôt. Použite príkaz PRTSYSSECA (Print System Security Attributes).
- Revidujte svoje rozhodnutia ohľadne systémových hodnôt, hlavne keď nainštalujete nové aplikácie.

Monitorovanie skupinových profilov

- Overte, či skupinové profily nemajú heslá. Príkaz DSPAUTUSR použite na overenie toho, či všetky skupinové profily majú heslo *NONE.
- Overte, či sú členmi skupiny správni užívatelia. Príkaz DSPUSRPRF s voľbou *GRPMBR použite na vypísanie členov skupiny.
- Skontrolujte špeciálne oprávnenia pre každý skupinový profil. Použite príkaz DSPUSRPRF. Ak máte spustenú úroveň zabezpečenia 30, 40 alebo 50, skupinové profily by nemali mať oprávnenie *ALLOBJ.

Monitorovanie užívateľských profilov

- Overte, či užívateľské profily v systéme patria do niektorej z týchto kategórií:
  - Užívateľské profily pre súčasných zamestnancov
  - Skupinové profily
  - Profily vlastníka aplikácií
  - Profily dodané spoločnosťou IBM (začínajú sa na Q)
- Keď spoločnosť užívateľa presunie, alebo keď užívateľ spoločnosť opustí, odstráňte jeho užívateľský profil. Príkaz CHGEXPSCDE (Change Expiration Schedule Entry) použite na automatické vymazanie alebo zakázanie profilu ihneď po odchode užívateľa.
- Vyhľadajte neaktívne profily a odstráňte ich. Príkaz ANZPRFACT (Analyze Profile Activity) použite na automatické zakázanie profilov, keď už boli určitý čas neaktívne.
- Určite užívateľov, ktorí majú rovnaké heslo, ako je názov ich užívateľského profilu. Použite príkaz ANZDFTPWD (Analyze Default Passwords). Voľbu tohto príkazu použite, aby ste prinútili užívateľov zmeniť svoje heslá, keď sa nabudúce prihlásia do systému.

  Upozornenie: Zo systému neodstraňujte žiadne profily, ktoré dodal spoločnosť IBM. Profily dodané spoločnosťou IBM sa začínajú písmenom Q.
- Buďte informovaní o tom, kto má inú triedu užívateľov ako *USER a prečo. Príkaz PRTUSRPRF (Print User Profile) použite na získanie zoznamu všetkých užívateľov, ich tried užívateľov a ich špeciálnych oprávnení. Porovnajte tieto informácie s vašim formulárom Zodpovednosti systému.
- Riaďte užívateľov, užívateľské profily ktorých majú pole *Obmedziť schopnosti* nastavené na *NO.

Monitorovanie kritických objektov

- Urobte si prehľad toho, kto má prístup na kritické objekty. Príkaz PRTPVTAUT (Print Private Authorities) a príkaz PRTPUBAUT (Print Publicly Authorized Objects) použite na monitorovanie objektov. Ak má skupina prístup, členov skupiny overte pomocou voľby *GRPMBR príkazu DSPUSRPRF.
- Overte, kto môže používať aplikačné programy, ktoré poskytujú prístup na objekty prostredníctvom inej metódy zabezpečenia, ako je napríklad osvojené oprávnenie. Použite príkaz PRTADPOBJ (Print Adopting Objects).

Monitorovanie neautorizovaného prístupu

- Operátorom systému dajte pokyny, aby okamžite reagovali na bezpečnostné správy vo fronte správ QSYSOPR. Hlavne nech upovedomia správcu bezpečnosti na opakované neúspešné pokusy o prihlásenie. Bezpečnostné správy majú rozsah od 2200 do 22FF a od 4A00 do 4AFF. Majú predpony CPF, CPI, CPC a CPD.
- Bezpečnostný audit nastavte na protokolovanie neautorizovaných pokusov o prístup na objekty.

Ďalej si pozrite Bezpečnostný audit .

Bezpečnostný audit

Počas monitorovania vašej bezpečnosti dokáže operačný systém protokolovať bezpečnostné udalosti, ktoré sa vyskytnú vo vašom systéme. Tieto udalosti sa zaznamenávajú do špeciálnych systémových objektov, ktoré sa nazývajú **žurnálové prijímače**. Žurnálové prijímače môžete nastaviť, aby zaznamenávali rôzne typy bezpečnostných udalostí, ako napríklad zmena systémovej hodnoty alebo užívateľského profilu alebo neúspešný pokus o prístup na objekt. Nasledujúce hodnoty riadia to, ktoré udalosti budú zaprotokolované:

- Systémová hodnota riadenia auditu (QAUDCTL)
- Systémová hodnota úrovne auditu (QAUDLVL)
- Hodnota úrovne auditu (AUDLVL) v užívateľských profiloch
- Hodnota auditu objektu (OBJAUD) v užívateľských profiloch
- Hodnota auditu objektu (OBJAUD) v objektoch.

Informácie v auditovacích žurnáloch sa používajú:

- Na zistenie pokusov o narušenie zabezpečenia.
- Na plánovanie migrácie na vyššiu úroveň zabezpečenia.
- Na monitorovanie použitia citlivých objektov, ako napríklad tajné súbory.

Na rôzne zobrazenia informácií z auditovacích žurnálov sú k dispozícii príkazy.

Formuláre plánovania základného zabezpečenia systému

Tieto formuláre môžete kopírovať alebo tlačiť z prehliadača.

Ak chcete vytlačiť všetky informácie o základnom zabezpečení, vyberte prvú sekciu okna, a potom kliknite na ikonu PDF na pruhu informačného centra.

Ak chcete vytlačiť jeden plánovací formulár, kliknite na odkaz, ktorý sa zhoduje s plánovacím formulárom, ktorý by ste chceli vytlačiť. Kliknite na prvú sekciu okna, a potom vo vašom prehliadači kliknite na ikonu Tlač. Takto si vybratý formulár vytlačíte.

Uvádzame úplný výpis všetkých plánovacích formulárov, ktoré sú potrebné, aby ste mohli úspešne plánovať a používať základnú systémovú bezpečnosť:

- formulár Plánovanie fyzického zabezpečenia
- formulár Opis aplikácií
- formulár Pomenúvacie konvencie
- formulár Opis knižníc
- formulár Výber systémových hodnôt
- formulár Zodpovednosti systému
- formulár Identifikácia skupín užívateľov
- formulár Opis skupín užívateľov
- formulár Konkrétny užívateľský profil
- formulár Autorizačný zoznam
- formulár Výstupný front a zabezpečenie pracovnej stanice
- formulár Inštalácia aplikácií

Formulár plánovania fyzického zabezpečenia

Tabuľka 65. Formulár plánovania fyzického zabezpečenia

Formulár plánovania fyzického zabezpečenia	
Pripravil:	Dátum:

Tabuľka 65. Formulár plánovania fyzického zabezpečenia (pokračovanie)

Pokyny • Oboznámte sa s týmto formulárom v téme ″Plánovanie zabezpečenia prostriedkov.″ • Použite tento formulár na popísanie všetkých bezpečnostných problémov, ktoré súvisia s fyzickým umiestnením vašej systémovej jednotky a pripojených zariadení. • Informácie v tomto formulári nemusíte zadať do systému.	
Systémová jednotka:	
Opíšte vaše bezpečnostné opatrenia na ochranu systémovej jednotky (napríklad uzamknutá miestnosť):	
Aká poloha uzamykateľného vypínača sa normálne používa?	
Kde sa necháva kľúč?	
Ďalšie poznámky týkajúce sa systémovej jednotky:	
Zálohovacie médiá a dokumentácia:	
Kde sú na vašom pracovisku uložené zálohovacie pásky?	
Kde sú uložené zálohovacie pásky mimo vášho pracoviska?	
Kde sú uchovávané heslá správcu bezpečnosti, služieb a DST?	
Kde sa uchováva dôležitá systémová dokumentácia, ako napríklad sériové číslo a konfigurácia?	

Formulár plánovania fyzického zabezpečenia			2. časť z 2
Ďalšie pokyny pre 2. časť • Vypíšte všetky pracovné stanice alebo tlačiarne, ktorých umiestnenie by mohlo vyvolať narušenie zabezpečenia. Vyznačte, aké ochranné opatrenia budú urobené. Pre tlačiareň vypíšte príklady dôverných tlačených správ pod stĺpec *Bezpečnostná trhlina*. • Ak povolíte vášmu systému automaticky konfigurovať vaše lokálne zariadenia, možno nebudete poznať názvy pracovných staníc a tlačiarní dovtedy, kým nebude váš systém nainštalovaný. Ak pri pripravovaní tohto formulára tie názvy nepoznáte, vyplňte opisy (napríklad umiestnenie) a dodajte názvy neskôr.			
Fyzické zabezpečenie pracovných staníc a tlačiarní			
Názov pracovnej stanice alebo tlačiarne	Jej umiestnenie alebo opis	Bezpečnostná trhlina	Ochranné opatrenia, ktoré treba urobiť

Formulár opisu aplikácií

Tabuľka 66. Formulár opisu aplikácií

Formulár opisu aplikácií	
Pripravil:	Dátum:

Tabuľka 66. Formulár opisu aplikácií (pokračovanie)

Pokyny • Oboznámte sa s týmto formulárom v téme ″Opis vašej aplikácie″ a ″Plánovanie zabezpečenia prostriedkov.″ • Pripravte osobitný formulár pre každú skupinu. • Informácie v tomto formulári nemusíte zadať do systému.	
Názov aplikácie:	Skratka:
Stručný opis aplikácie:	
Názov primárnej ponuky:	Knižnica:
Názov úvodného programu:	Knižnica:
Vypíšte knižnice používané aplikáciou pre súbory aj pre programy:	
Definujte ciele zabezpečenia pre aplikáciu, napríklad či sú určité informácie dôverné:	

Formulár názvových konvencií

Tabuľka 67. Formulár názvových konvencií

Formulár názvových konvencií	
Pripravil:	Dátum:
Pokyny • Oboznámte sa s týmto formulárom v téme ″Opis vašich aplikácií.″ • Informácie z tohto formulára nemusíte zadať priamo do systému. • Použite tento formulár na popísanie, ako budete priraďovať názvy objektom vo vašom systéme. Pre každý uveďte príklad.	
Typ objektu	**Pomenúvacia konvencia**
Skupinové profily	
Užívateľské profily	
Autorizačné zoznamy	
Knižnice	
Súbory	
Kalendáre	
Zariadenia	
Pásky	

Formulár opisu knižnice

Tabuľka 68. Formulár opisu knižnice

Formulár opisu knižnice	1. časť z 2
Pripravil:	Dátum:
Pokyny: • Oboznámte sa s týmto formulárom v téme ″Plánovanie užívateľského zabezpečenia″ a ″Plánovanie zabezpečenia prostriedkov.″ • Použite tento formulár na opis vašich hlavných knižníc a definovanie ich bezpečnostných požiadaviek. • Vyplňte jeden formulár pre každú väčšiu knižnicu aplikácií v systéme. • Naučte sa, ako zadať informácie z tohto formulára, v téme Nastavenie zabezpečenia prostriedkov.″	
Názov knižnice:	Opisný názov (text):
Stručne opíšte funkciu tejto knižnice:	

Tabuľka 68. Formulár opisu knižnice (pokračovanie)

Definujte ciele zabezpečenia pre knižnicu, napríklad či sú určité informácie dôverné:	
Verejné oprávnenie pre knižnicu:	
Verejné oprávnenie pre objekty v knižnici:	
Verejné oprávnenie pre nové objekty (CRTAUT):	
Vlastník knižnice:	

Formulár opisu knižnice				2. časť z 2
Pripravil:			Dátum:	
Názov knižnice:				
Ďalšie pokyny pre 2. časť: • V nasledujúcom diagrame vypíšte všetkých jednotlivcov alebo objekty vyžadujúce špecifické oprávnenie. • Zadajte typ vyžadovaného oprávnenia: *ALL, *CHANGE, *USE alebo *EXCLUDE.				
Vypíšte špecifické oprávnenia pre objekty knižnice				
Skupinový profil alebo užívateľský profil	Názov objektu	Typ objektu	Potrebné oprávnenie	Autorizačný zoznam

Formulár výberu systémových hodnôt

Tabuľka 69. Formulár výberu systémových hodnôt

Formulár výberu systémových hodnôt		1. časť z 2
Pripravil:		Dátum:
Pokyny • Oboznámte sa s týmto formulárom v téme ″Plánovanie celkového prístupu.″ • Použite tento formulár na zaznamenanie vašich volieb pre systémové hodnoty, ktoré ovplyvňujú zabezpečenie a prispôsobenie. • Použite voľbu **1** z ponuky NASTAVENIE pre zadanie 1. časti tohto formulára.		
Hodnoty z obrazovky zmien systémových volieb		
Systémová hodnota/sieťový atribút	**Odporúčaná voľba**	**Vaša voľba**
Názov systému		
Oddeľovač dátumu (QDATSEP)		
Formát dátumu (QDATFMT)		
Oddeľovací znak času (QTIMSEP)		
Formát pomenovania zariadenia pre nové zariadenia (QDEVNAMING)	1 (Systém iSeries)	
Systémová tlačiareň (QPRTDEV)		
Úroveň bezpečnosti (QSECURITY)	40	

Tabuľka 69. Formulár výberu systémových hodnôt (pokračovanie)

Povoliť správcom bezpečnosti prihlásiť sa na ktorúkoľvek pracovnú stanicu (QLMTSECOFR)	N	
Uložiť účtovné informácie úlohy o dokončenom tlačovom výstupe (QACGLVL)	N (*NONE)	

Formulár výberu systémových hodnôt		2. časť z 2
Ďalšie pokyny pre 2. časť • Oboznámte sa bližšie s 2. časťou tohto formulára v téme ″Nastavenie systémových hodnôt.″ • Použite príkaz WRKSYSVAL (Work With System Value) na zadanie 2. časti.		
Systémové hodnoty zabezpečenia		
Systémová hodnota	**Odporúčaná voľba**	**Vaša voľba**
Interval uplynutia vyhradeného času neaktívnej úlohy (QINACTITV)	30 až 60	
Front správ neaktívnej úlohy (QINACTMSGQ)	*DSCJOB	
Obmedziť relácie zariadenia (QLMTDEVSSN)	1 (YES)	
Akcia pri neúspešných prihlasovacích pokusoch (QMAXSGNACN)	3 (Vypnúť oboje)	
Maximálny povolený počet prihlasovacích pokusov (QMAXSIGN)	3 až 5	
Interval ukončenia platnosti hesla (QPWDEXPITV)	30 až 60	
Maximálna dĺžka hesla (QPWDMAXLEN)	8	
Minimálna dĺžka hesla (QPWDMINLEN)	6	
Vyžadovať odlišné heslá (QPWDRQDDIF)	7 (6 jedinečných hesiel)	
Ďalšie systémové hodnoty		
Systémová hodnota	**Odporúčaná voľba**	**Vaša voľba**
Interval uplynutia vyhradeného času odpojenej úlohy (QDSCJOBITV)	300	
Poznámka: Možno budete chcieť nastaviť niektoré ďalšie systémové hodnoty týkajúce sa zabezpečenia. Pozrite si 3. kapitolu *Security-Reference* (SC41-5302-04), kde je uvedený úplný zoznam systémových hodnôt bezpečnosti a ich odporúčaní.		

Formulár systémových zodpovedností

Tabuľka 70. Formulár systémových zodpovedností

Formulár systémových zodpovedností	
Pripravil:	Dátum:
Pokyny: • Oboznámte sa s týmto formulárom v téme ″Plánovanie jednotlivých užívateľských profilov.″ • Použite tento formulár na výpis každého, kto má inú užívateľskú triedu než *USER. • Preneste informácie z tohto formulára do stĺpca *Užívateľská trieda* formulára jednotlivého užívateľského profilu.	

Tabuľka 70. Formulár systémových zodpovedností (pokračovanie)

Kto je váš primárny správca bezpečnosti? Kto je váš záložný správca bezpečnosti?			
Názov profilu	Meno užívateľa	Trieda	Poznámky

Formulár identifikácie skupiny užívateľov

Tabuľka 71. Formulár identifikácie skupiny užívateľov

Formulár identifikácie skupiny užívateľov								
Pripravil:		Dátum:						
Pokyny: • Oboznámte sa s týmto formulárom v téme ″Plánovanie skupín užívateľov.″ • Tento formulár vám pomôže identifikovať skupiny užívateľov, ktorí majú podobné aplikačné potreby. 1. Vypíšte vaše hlavné aplikácie navrchu formulára. 2. Vypíšte vašich užívateľov v ľavom stĺpci. 3. Označte potrebné aplikácie pre každého užívateľa. • Informácie v tomto formulári nemusíte zadať do systému.								
		Potrebný prístup pre aplikácie						
Meno užívateľa	Oddelenie	APP:	APP:	APP:	APP:	APP:	APP:	APP:
Poznámka: • Ak máte *voľnejšie* bezpečnostné prostredie, použite **X** na označenie, ktoré aplikácie užívatelia potrebujú. • Ak máte *prísne* bezpečnostné prostredie, možno bude potrebné použiť **C** (zmeniť) a **V** (zobraziť) pre zadanie, *ako* budú aplikácie používané.								

Formulár opisu skupiny užívateľov

Tabuľka 72. Formulár opisu skupiny užívateľov

Formulár opisu skupiny užívateľov	1. časť z 2
Pripravil:	Dátum:

Tabuľka 72. Formulár opisu skupiny užívateľov (pokračovanie)

Pokyny pre 1. časť • Naučte sa pripraviť tento formulár v téme Plánovanie skupín užívateľov.″ • Naučte sa, ako zadať tento formulár, v téme ″Nastavenie užívateľského zabezpečenia.″ • Pripravte osobitný formulár pre každú skupinu, ktorá bude používať systém. • Použite príkaz CRTJOBD (Create Job Description) na vytvorenie opisu úlohy pre skupinu. Opis úlohy má úvodný zoznam knižníc skupiny.
Názov skupinového profilu: Opis skupiny:
Primárna aplikácia pre skupinu: Výpis ostatných aplikácií potrebných pre skupinu:
Urobte výpis každej knižnice, ktorú skupina potrebuje. Označte (✓) každú knižnicu, ktorá by mala byť v úvodnom zozname knižníc pre skupinu:
Poznámka: Pozrite si vo formulári opisu aplikácií každú aplikáciu, ktorá je uvedená v predošlej časti, aby ste zistili, ktoré knižnice aplikácia používa.

Formulár opisu skupiny užívateľov		2. časť z 2
Ďalšie pokyny pre 2. časť • Nasledujúce tabuľky uvádzajú všetky polia, ktoré sa objavia na obrazovke vytvorenia užívateľského profilu. Tieto polia sú rozdelené do skupín: tie, kde musíte robiť výber a tie, kde IBM odporúča predvolenú hodnotu. • Použite obrazovku práce s užívateľskými profilmi alebo príkaz CRTUSRPRF (Create User Profile) na zadanie informácií z tejto časti formulára do vášho systému.		
Vyberte hodnoty pre tieto polia v skupinovom profile:		
Názov poľa	**Odporúčaná voľba**	**Vaša voľba**
Názov skupinového profilu (Užívateľ)		
Heslo	*NONE	
Užívateľská trieda (Typ užívateľa)	*USER	
Aktuálna knižnica (Štandardná knižnica)	*rovnaké ako názov skupinového profilu*	
Úvodný volaný program (Prihlasovací program)		
Knižnica úvodného programu		
Úvodná ponuka (Prvá ponuka)		
Knižnica úvodnej ponuky		
Obmedziť schopnosti (Obmedziť používanie príkazového riadka)	*YES	
Text (Užívateľský opis)		
Opis úlohy	*rovnaké ako názov skupinového profilu*	
Knižnica opisu úlohy		
Názov skupinového profilu (Skupina užívateľov)	*NONE	
Tlačové zariadenie (štandardná tlačiareň)		
Výstupný front	*DEV	
Poznámka: Tieto polia sú v poradí, v akom sa objavia na obrazovke vytvorenia užívateľského profilu (s použitím F4).		
Použite systémom dodané hodnoty (štandardné nastavenia) pre nasledujúce polia:		

Účtovný kód	Použitie vyrovnávacej pamäte klávesnice	Verejné oprávnenie
Úroveň asistencie	ID jazyka	Nastavenie ukončenia platnosti hesla
Program upozornenia	Obmedzenie relácií zariadenia	Triediaca sekvencia
ID kódovanej sady znakov	Maximálny úložný priestor	Mimoriadne oprávnenie
ID krajiny alebo regiónu	Front správ	Špeciálne prostredie
Zobraziť prihlasovacie informácie	Interval ukončenia platnosti hesla	Stav
Heslo dokumentu	Prioritný limit	Užívateľské voľby
Poznámka: Polia v tomto zozname sú usporiadané v abecednom poradí.		

Formulár jednotlivého užívateľského profilu

Tabuľka 73. Formulár jednotlivého užívateľského profilu

Formulár jednotlivého užívateľského profilu						
Pripravil:				Dátum:		
Pokyny: • Naučte sa pripraviť tento formulár v téme Plánovanie jednotlivých užívateľských profilov.″ • Použite tento formulár na zaznamenanie informácií o jednotlivých užívateľoch systému. Vyplňte jeden formulár pre každú skupinu užívateľov (skupinový profil), ktorá je vo vašom systéme. • Použite prázdne stĺpce vpravo pre všetky dodatočné polia, ktoré chcete zadať pre jednotlivých užívateľov. • Naučte sa, ako zadať tento formulár, v téme ″Nastavenie jednotlivých užívateľov.″						
Názvy skupinových profilov:						
Vlastník vytvorených objektov:			Skupinové oprávnenie pre vytvorené objekty:			
Typ skupinového oprávnenia:						
Vytvorte položku pre každého člena skupiny:						
Užívateľský profil	Text (opis)	Užívateľská trieda	Obmedzenie schopnosti			

Formulár autorizačného zoznamu

Tabuľka 74. Formulár autorizačného zoznamu

Formulár autorizačného zoznamu	
Pripravil:	Dátum:

Tabuľka 74. Formulár autorizačného zoznamu (pokračovanie)

Pokyny • Oboznámte sa s týmto formulárom v téme ″Plánovanie zabezpečenia prostriedkov.″ • Pripravte jeden formulár pre každý autorizačný zoznam. • Použite ten formulár na výpis objektov, ktoré zoznam a skupiny a jednotlivcov, ktorí majú prístup do zoznamu, zabezpečujú. • Naučte sa, ako zadať tento formulár, v téme ″Nastavenie zabezpečenia prostriedkov.″					
Názov autorizačného zoznamu:					
Opis:					
Vypíšte objekty, ktoré zoznam zabezpečuje					
Názov objektu	Typ objektu	Knižnica objektov	Názov objektu	Typ objektu	Knižnica objektov
Vypíšte skupiny a užívateľov, ktorí majú prístup do zoznamu					
Skupina alebo užívateľ	Typ povoleného prístupu	Vypísať riadenie?	Skupina alebo užívateľ	Typ povoleného prístupu	Vypísať riadenie?

Formulár zabezpečenia výstupného frontu tlačiarne a pracovnej stanice

Tabuľka 75. Formulár zabezpečenia výstupného frontu tlačiarne a pracovnej stanice

Formulár zabezpečenia výstupného frontu tlačiarne a pracovnej stanice				
Pripravil:		Dátum:		
Pokyny • Oboznámte sa s týmto formulárom v téme ″Ochrana tlačového výstupu.″ • Vytvorte v tomto formulári položku pre každú pracovnú stanicu alebo výstupný front, ktorý potrebuje špeciálnu ochranu. • Naučte sa, ako zadať tento formulár, v téme ″Ochrana pracovných staníc.″				
Vypíšte parametre pre obmedzené výstupné fronty:				
Názov výstupného frontu	Knižnica výstupného frontu	Zobraziť každý súbor (DSPDTA)	Oprávnenie na označenie (AUTCHK)	Riadenie operátorom (OPRCTL)

Tabuľka 75. Formulár zabezpečenia výstupného frontu tlačiarne a pracovnej stanice (pokračovanie)

Pracovné stanice správcu bezpečnosti: Ak obmedzíte správcu bezpečnosti na určité pracovné stanice (systémová hodnota QLMTSECOFR je yes), vypíšte nižšie pracovné stanice s oprávnením pre správcu bezpečnosti a každého s oprávnením *ALLOBJ:	
Vypíšte nižšie oprávnenia pre obmedzené pracovné stanice:	
Názov pracovnej stanice	Skupiny alebo užívatelia, ktorí majú oprávnenie (oprávnenie *CHANGE)
Poznámka: Obmedzené pracovné stanice by mali mať verejné oprávnenie nastavené na *EXCLUDE.	

Formulár inštalácie aplikácie

Tabuľka 76. Formulár inštalácie aplikácie

Formulár inštalácie aplikácie		1. časť z 2
Pripravil:		Dátum:
Pokyny • Oboznámte sa s týmto formulárom v téme ″Plánovanie inštalácie aplikácie.″ • Pripravte jeden formulár pre každú aplikáciu, ktorú budete inštalovať. • Použite tento formulár na plánovanie, ako budete vytvárať vlastníctvo a verejné oprávnenie pre vaše aplikácie po ich zavedení. • Naučte sa, ako zadať tento formulár, v téme ″Nastavenie zabezpečenia prostriedkov.″		
Názov aplikácie:		
Opis:		
Vypíšte a vysvetlite všetky profily, ktoré musia byť vytvorené pre inštaláciu aplikácie:		
Názov knižnice:		
	Pred inštaláciou	Po inštalácii
Vlastník knižnice		
Vlastník objektu		
Verejné oprávnenie pre knižnicu		
Verejné oprávnenie pre objekt		
Verejné oprávnenie pre nové objekty		
Názov knižnice:		
	Pred inštaláciou	Po inštalácii
Vlastník knižnice		
Vlastník objektu		
Verejné oprávnenie pre knižnicu		
Verejné oprávnenie pre objekt		
Verejné oprávnenie pre nové objekty		

Formulár inštalácie aplikácie		2. časť z 2
Názov knižnice:		
	Pred inštaláciou	Po inštalácii
Vlastník knižnice		

Vlastník objektu		
Verejné oprávnenie pre knižnicu		
Verejné oprávnenie pre objekt		
Verejné oprávnenie pre nové objekty		
Názov knižnice:		
	Pred inštaláciou	Po inštalácii
Vlastník knižnice		
Vlastník objektu		
Verejné oprávnenie pre knižnicu		
Verejné oprávnenie pre objekt		
Verejné oprávnenie pre nové objekty		
Názov knižnice:		
	Pred inštaláciou	Po inštalácii
Vlastník knižnice		
Vlastník objektu		
Verejné oprávnenie pre knižnicu		
Verejné oprávnenie pre objekt		
Verejné oprávnenie pre nové objekty		

Príloha. Oznamy

Tieto informácie boli vytvorené pre produkty a služby ponúkané v USA.

IBM nemusí produkty, služby alebo komponenty, o ktorých sa hovorí v tomto dokumente, ponúkať vo všetkých krajinách. Informácie o produktoch a službách, aktuálne dostupných vo vašej krajine, môžete získať od zástupcu spoločnosti IBM. Žiadne odkazy na produkt, program alebo službu spoločnosti IBM neznamenajú, ani z nich nevyplýva, že musí byť použitý len tento produkt, program alebo služba spoločnosti IBM. Môžete použiť ľubovoľný funkčne ekvivalentný produkt, program alebo službu, ktoré neporušujú práva duševného vlastníctva IBM. Užívateľ však zodpovedá za to, aby zhodnotil a overil používanie takéhoto produktu, programu alebo služby.

Spoločnosť IBM môže vlastniť patenty alebo patenty v schvaľovacom konaní pokrývajúce predmetné záležitosti opísané v tomto dokumente. Text tohto dokumentu vám neudeľuje licenciu na tieto patenty. Písomné žiadosti o licencie môžete zaslať na adresu:

IBM Director of Licensing
IBM Corporation
500 Columbus Avenue
Thornwood, NY 10594-1785
U.S.A.

Požiadavky na licencie ohľadne dvojbajtových (DBCS) informácií získate od IBM Intellectual Property Department vo vašej krajine alebo ich zašlite písomne na adresu:

IBM World Trade Asia Corporation
Licensing
2-31 Roppongi 3-chome, Minato-ku
Tokyo 106, Japan

Nasledujúci odsek sa netýka Veľkej Británie ani žiadnej inej krajiny, kde sú takéto vyhlásenia nezlučiteľné s miestnym zákonom: SPOLOČNOSŤ INTERNATIONAL BUSINESS MACHINES POSKYTUJE TÚTO PUBLIKÁCIU "TAK AKO JE", BEZ AKÝCHKOĽVEK VÝSLOVNÝCH ALEBO MLČKY PREDPOKLADANÝCH ZÁRUK, VRÁTANE, ALE BEZ OBMEDZENIA NA ZÁRUKY NEPORUŠENIA PRÁV, PREDAJNOSTI ALEBO VHODNOSTI NA KONKRÉTNY ÚČEL. Niektoré štáty nepovoľujú zrieknutie sa výslovných ani mlčky predpokladaných záruk v určitých operáciách, preto sa na vás toto vyhlásenie nemusí vzťahovať.

Tento dokument môže obsahovať technické nepresnosti alebo tlačové chyby. Informácie uvedené v tomto dokumente podliehajú priebežným zmenám; tieto zmeny budú zapracované do nových vydaní. IBM môže kedykoľvek bez ohlásenia urobiť vylepšenia a/alebo zmeny v produktoch alebo programoch opísaných v tejto publikácii.

Akékoľvek odkazy v tejto publikácii na iné webové stránky, než stránky firmy IBM, sú poskytované len pre vaše pohodlie a v žiadnom prípade neslúžia ako súhlas s týmito webovými stránkami. Materiály na týchto webových stránkach nie sú súčasťou materiálov k tomuto produktu firmy IBM a ich použitie je na vaše vlastné riziko.

Držitelia licencií tohto programu, ktorí si želajú mať informácie o tomto programe kvôli povoleniu: (i) výmeny informácií medzi nezávisle vytvorenými programami a inými programami (vrátane tohto programu) a (ii) spoločného používania vymenených informácií by mali kontaktovať:

IBM Corporation
Software Interoperability Coordinator, Department 49XA
3605 Highway 52 N
Rochester, MN 55901
U.S.A.

Takéto informácie môžu byť v niektorých prípadoch dostupné až po zaplatení príslušného poplatku.

Licenčný program spomínaný v týchto informáciách a všetky pre tento program dostupné licenčné materiály poskytuje spoločnosť IBM podľa podmienok zmluvy IBM Customer Agreement, IBM International Program License Agreement alebo ľubovoľnej ekvivalentnej zmluvy medzi nami.

Informácie týkajúce sa produktov iných spoločností ako IBM boli získané od dodávateľov týchto produktov, z ich publikovaných oznámení alebo iných verejne prístupných zdrojov. Spoločnosť IBM tieto produkty netestovala a nemôže potvrdiť presnosť ich výkonu, kompatibilitu ani iné parametre týkajúce sa produktov nepochádzajúcich od IBM. Otázky o schopnostiach produktov nepochádzajúcich od IBM adresujte dodávateľom týchto produktov.

Tieto informácie slúžia len na plánovacie účely. Tu uvedené informácie môžu byť pred sprístupnením opisovaných produktov zmenené.

Tieto informácie obsahujú príklady údajov a hlásení používaných v každodenných obchodných operáciách. Kvôli čo najúplnejšiemu vysvetleniu obsahujú príklady konkrétne mená jednotlivcov, názvy spoločností, značiek a výrobkov. Všetky tieto názvy sú fiktívne a akákoľvek ich podobnosť s názvami a adresami používanými skutočným obchodným podnikom je úplne náhodná.

Ochranné známky

Nasledujúce pojmy sú ochrannými známkami spoločnosti International Business Machines Corporation v USA alebo iných krajinách:

Application System/400
AS/400
e (logo)
IBM
iSeries
Operating System/400
OS/400
400

Lotus, Freelance a WordPro sú ochranné známky spoločnosti International Business Machines Corporation a Lotus Development Corporation v USA alebo iných krajinách.

C-bus je ochranná známka spoločnosti Corollary Microsystems,Inc. v USA alebo iných krajinách.

ActionMedia, LANDesk, MMX, Pentium a ProShare sú ochranné známky alebo zaregistrované ochranné známky spoločnosti Intel Corporation v USA alebo iných krajinách.

Microsoft, Windows, Windows NT a logo Windows sú ochrannými známkami spoločnosti Microsoft Corporation v USA alebo iných krajinách.

SET a logo SET sú ochranné známky vlastnené spoločnosťou SET Secure Electronic Transaction LLC.

Java a všetky s ňou súvisiace ochranné známky sú ochranné známky spoločnosti Sun Microsystems, Inc. v USA alebo iných krajinách.

UNIX je zaregistrovaná ochranná známka spoločnosti The Open Group v USA a iných krajinách.

Ďalšie názvy spoločností, produktov alebo služieb môžu byť ochrannými známkami alebo servisnými známkami iných subjektov.

Podmienky sťahovania a tlače publikácií

Povolenie na používanie vybratých publikácií, ktoré si chcete stiahnuť, je podmienené vaším súhlasom s nasledujúcimi podmienkami.

Osobné použitie: Tieto publikácie môžete kopírovať len na svoje osobné nekomerčné použitie pod podmienkou, že dodržíte všetky oznámenia o vlastníckych právach. Tieto publikácie nemôžete distribuovať, zobrazovať ani z nich alebo zo žiadnej ich časti robiť odvodené práce, bez výslovného súhlasu spoločnosti IBM.

Komerčné použitie: V rámci vášho podniku môžete kopírovať, distribuovať a prezentovať tieto publikácie len za predpokladu, že dodržíte všetky oznámenia o vlastníckych právach. Z týchto publikácií ani zo žiadnej ich časti, nesmiete robiť odvodené práce, ani reprodukovať, distribuovať alebo zobrazovať tieto publikácie, ani ich časti, mimo váš podnik, bez výslovného súhlasu IBM.

Okrem povolení výslovne vyjadrených v tomto dokumente, nie sú pre uvedené publikácie alebo informácie, údaje, softvér alebo iné duševné vlastníctvo v nich obsiahnuté, udelené žiadne iné výslovné alebo mlčky predpokladané povolenia, oprávnenia alebo práva.

IBM si vyhradzuje právo vypovedať oprávnenia uvedené v tomto dokumente kedykoľvek, keď usúdi, že používanie týchto publikácií poškodzuje jej záujmy, alebo ak spoločnosť IBM zistí, že vyššie uvedené inštrukcie neboli náležite dodržiavané.

Stiahnuť, exportovať a re-exportovať môžete tieto informácie len v tom prípade, ak vyhovujú všetkým platným zákonom a predpisom, vrátane zákonov a predpisov USA týkajúcich sa exportu. IBM NEPOSKYTUJE ŽIADNU ZÁRUKU NA OBSAH TÝCHTO PUBLIKÁCIÍ. TIETO PUBLIKÁCIE SA POSKYTUJÚ ″TAK AKO SÚ″ BEZ AKÝCHKOĽVEK VÝSLOVNÝCH ALEBO MLČKY PREDPOKLADANÝCH ZÁRUK, VRÁTANE, ALE BEZ OBMEDZENIA NA ZÁRUKY NEPORUŠENIA PRÁV, PREDAJNOSTI ALEBO VHODNOSTI NA KONKRÉTNY ÚČEL.

Na všetky materiály má autorské práva spoločnosť IBM Corporation.

Stiahnutím alebo vytlačením publikácie z týchto stránok vyjadrujete svoj súhlas s týmito podmienkami.

Vytlačené v USA