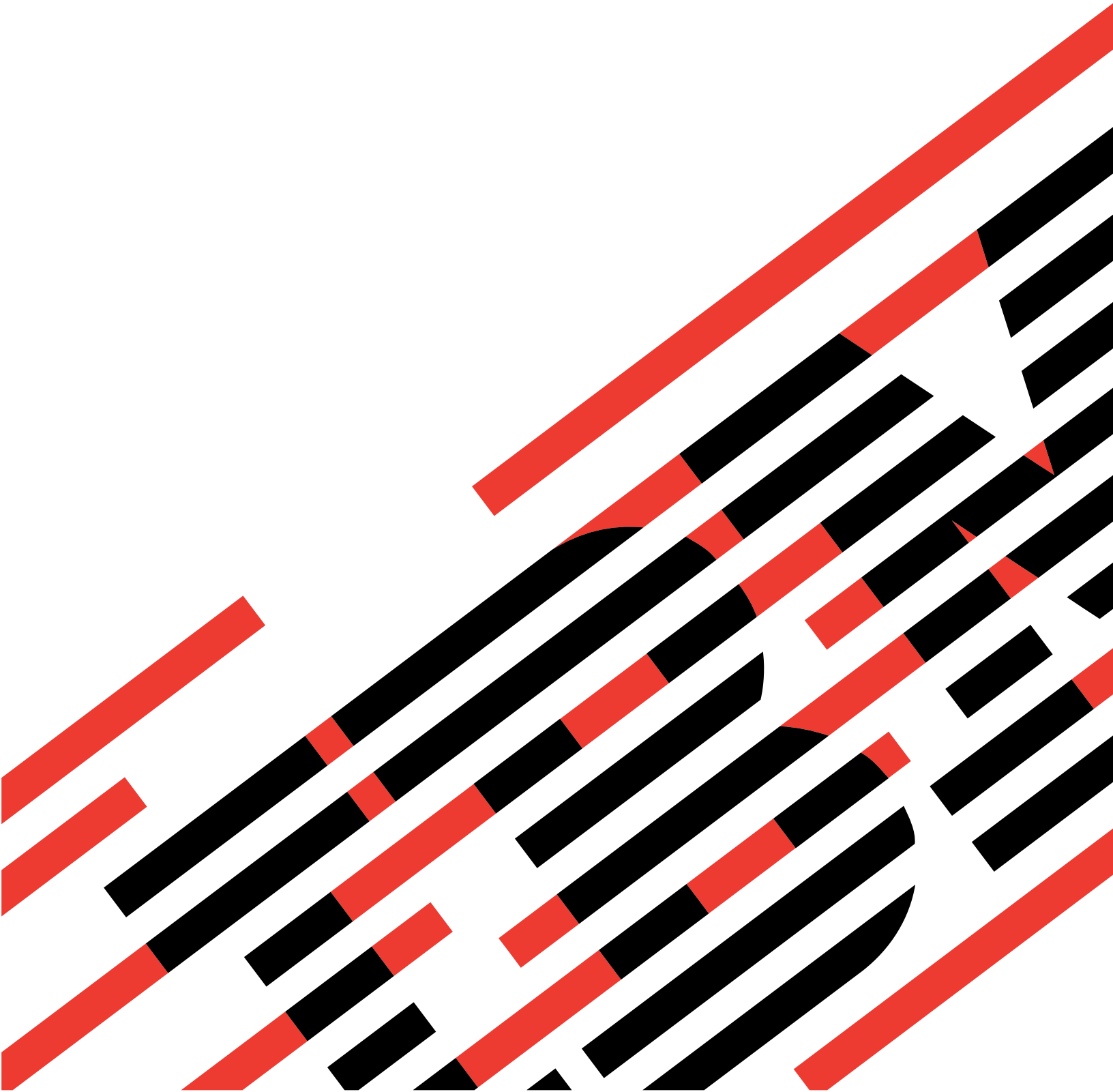
IBM

eserver

iSeries

Základní zabezpečení a plánování systému

Verze 5, vydání 3



IBM

@server

iSeries

Základní zabezpečení a plánování systému

Verze 5, vydání 3

Poznámky

Před použitím těchto informací a produktu, ke kterému se vztahují, si nezapomeňte přečíst informace uvedené v tématu “Poznámky”, na stránce 129.

Čtvrté vydání (srpen 2005)

Toto vydání se vztahuje k verzi 5, vydání 3, modifikaci 0 licencovaného programu IBM Operating System/400 (číslo produktu 5722-SS1) a ke všem následným vydáním a modifikacím, dokud nebude v nových vydáních uvedeno jinak. Tato verze nemůže být spuštěna na žádném počítači RISC (reduced instruction set computer), ani na modelech CISC.

Obsah

Základní zabezpečení a plánování systému

Publikace Základní zabezpečení a plánování systému uvádí podrobné informace o plánování a nastavení zabezpečení systému iSeries. Toto téma klade důraz na proces plánování a obsahuje formuláře, které můžete použít k naplánování a zaznamenání vašich rozhodnutí v oblasti zabezpečení systému. Dále uvádí podrobné pokyny týkající se nastavení základního zabezpečení systému. Vzhledem k povaze tohoto tématu si možná budete chtít téma vytisknout, abyste si mohli informace prostudovat podrobněji.

Nastavení nejlepšího zabezpečení serveru iSeries zahrnuje dvě hlavní množiny činností: úlohy týkající se plánování a úlohy týkající se konfigurace. Chcete-li zabezpečení systému nastavit tak, aby splňovalo potřeby vaší organizace, nezapomeňte si prostudovat níže uvedená témata:

- Téma Začínáme se základním zabezpečením systému poskytuje přehled o všeobecných koncepcích zabezpečení a odpovídá na otázky týkající se základního zabezpečení systému.
- Téma Plánování zabezpečení uživatelů poskytuje informace o plánování zabezpečení, které ovlivní uživatele ve vašem systému. To zahrnuje fyzické zabezpečení, zabezpečení aplikací, vaši celkovou strategii zabezpečení a uživatelské profily v systému.
- Téma Plánování zabezpečení prostředků poskytuje informace o tom, jak naplánovat zabezpečení objektů v systému, včetně knihoven a objektů v nich umístěných, tiskáren, tiskového výstupu a pracovních stanic.

Poté, co dokončíte aktivity související s plánováním, měli byste si prostudovat níže uvedená témata, která vám pomohou s nastavením zabezpečení systému:

- Téma Nastavení zabezpečení uživatelů popisuje proces nastavení zabezpečení uživatelů a skupin uživatelů.
- Téma Nastavení zabezpečení prostředků poskytuje informace o tom, jak nastavit vlastnictví objektů, veřejná a specifická oprávnění k objektům a jak nastavit zabezpečení tiskáren a pracovních stanic.
- Téma Testování zabezpečení popisuje, jak otestovat zabezpečení.
- Téma Změna informací o zabezpečení popisuje postup aktualizace a změny uživatelských a skupinových profilů a zabezpečení prostředků.
- Téma Uložení informací o zabezpečení poskytuje informace o zálohování informací týkajících se zabezpečení.
- Téma Monitorování zabezpečení obsahuje pracovní listy, s jejichž pomocí můžete sledovat zabezpečení, a informace o kontrole zabezpečení.

Kromě těchto témat můžete použít plánovací formuláře ke zdokumentování vašich strategií v oblasti plánování a vašich rozhodnutí týkajících se zabezpečení systému.

Tisk tohoto tématu

PDF verzi tohoto dokumentu můžete prohlížet nebo ji můžete stáhnout a vytisknout. Chcete-li pohlížet PDF soubory, musíte mít nainstalovanou aplikaci Adobe® Acrobat® Reader. Můžete si ji stáhnout z domovské stránky společnosti Adobe.

Chcete-li prohlížet nebo stáhnout PDF verzi, označte publikaci Základní zabezpečení a plánování systému (950 KB nebo 164 stran).

Chcete-li uložit PDF soubory na pracovní stanici, abyste je později mohli prohlížet nebo tisknout, postupujte takto:

1. Otevřete PDF v prohlížeči (klepněte na odkaz nahoře).
2. Klepněte na menu **Soubor** v prohlížeči.
3. Klepněte na příkaz **Uložit jako...**.
4. Přejděte do adresáře, do kterého chcete PDF soubor uložit.
5. Klepněte na tlačítko **Uložit**.

Začínáme se základním zabezpečením systému

O zabezpečení systému by se měl zajímat každý, od administrátora systému po uživatele. Zabezpečení systému chrání server iSeries a citlivé obchodní informace před úmyslným i neúmyslným prolomením zabezpečení.

Zabezpečení systému můžete přizpůsobit svému prostředí a svým potřebám.

Uvažujte o zabezpečení jako o vstupní bráně do systému. Funkce zabezpečení používáte, chcete-li informace **zamknout** nebo chránit před neoprávněným použitím.

Tyto funkce zabezpečení také používáte, chcete-li **zpřístupnit** flexibilitu systému a přizpůsobit systém pro každého uživatele.

Dobře sestavený plán zabezpečení může systém chránit, ale nemůže zaručit bezpečnost vybavení ani bezpečnost informací. Odpovědnost za systém by měla být rozdělena mezi několik zaměstnanců, aby bylo zajištěno, že kontrolu nad systémem nebude mít nikdy jen jedna osoba.

Základní zabezpečení a plánování systému vás postupně seznamuje s pojetím plánování a nastavení základního zabezpečení systému. Toto téma klade důraz na plánování zabezpečení systému a obsahuje také plánovací formuláře, do kterých budete zaznamenávat svá rozhodnutí týkající se zabezpečení. Rozhodování vám usnadní příklad podniku plánujícího zabezpečení, na kterém je celé toto téma ilustrováno.

Správné a důkladné plánování je podstatou úspěšného zabezpečení systému. Informace o základních potřebách zabezpečení a o významu plánování zabezpečení najdete v těchto tématech:

- Časté otázky o základním zabezpečení systému.
- Přehled základního zabezpečení systému.
- Způsob plánování základního zabezpečení systému.

Také byste měli mít dobře sestavený plán zálohování a obnovy všech informací v systému. Dále byste měli v plánu počítat s výměnou vybavení v případě pohromy. Další informace o vytváření správného plánu zálohování najdete v tématu Zálohování a obnova v aplikaci Information Center.

Podrobné informace o plánování zabezpečení pro uživatele

Následující témata se věnují technikám plánování zabezpečení pro uživatele:

- Plánování zabezpečení aplikací.
- Plánování zásad zabezpečení.
- Plánování skupin uživatelů.
- Plánování profilů individuálních uživatelů.

Podrobné informace o plánování zabezpečení prostředků

Následující témata vás systematicky seznámí s pojetím plánování zabezpečení prostředků pro uživatele.

- Seznámení s typy oprávnění.
- Plánování zabezpečení knihoven aplikací.
- Určení vlastnictví knihoven a objektů.
- Seskupování objektů.
- Zabezpečení tiskových výstupů.
- Zabezpečení pracovních stanic.
- Plánování instalace aplikací.

Tisknutelné plánovací formuláře

Publikace Základní zabezpečení a plánování systému obsahuje tisknutelné plánovací formuláře, do kterých můžete zaznamenávat všechna svá rozhodnutí související se zabezpečením. Celé téma můžete vytisknout ve formátu PDF, jednotlivé plánovací formuláře můžete vytisknout pomocí tlačítka Tisk v prohlížeči.

Podrobné pokyny pro nastavení základního zabezpečení systému

Až dokončíte plánování zabezpečení, začněte plán zabezpečení realizovat. Následující témata vám pomohou s nastavením zabezpečení systému.
- Nastavení zabezpečení uživatelů.
- Nastavení zabezpečení prostředků.

Časté otázky o základním zabezpečení systému

Odpovědi na tyto časté otázky o zabezpečení systému vám pomohou snáze pochopit význam zabezpečení systému.

Proč je zabezpečení důležité?

Informace uložené v systému jsou jednou z nejdůležitějších majetkových aktiv společnosti. Když přemýšlíte o tom, jak tato aktiva, mějte na paměti tři důležité úkoly:
- **Důvěrnost:** Dobrá bezpečnostní opatření mohou lidem zabránit v přístupu k důvěrným informacím, neumožní jim takové informace vidět ani je předávat dál.
- **Integrita:** Dobře navržený systém zabezpečení může do jisté míry zajistit přesnost informací v počítači. Se správným zabezpečením můžete zabránit neoprávněným změnám nebo vymazání dat.
- **Dostupnost:** Pokud někdo poškodí data v systému, ať náhodně či úmyslně, nemáte k těmto prostředkům přístup, dokud je neobnovíte. Dobrý systém zabezpečení může takovým poškozením zabránit.

Když lidé myslí na zabezpečení systému, obvykle mají na mysli ochranu systému před lidmi mimo společnost, například z konkurenční společnosti. Ve skutečnosti je ochrana před zvědavostí řádných uživatelů nebo před nehodami systému, které tito uživatelé způsobili, často největší výhodou dobře navrženého systému zabezpečení. V systému, který nemá dobré funkce zabezpečení, by mohl uživatel neúmyslně vymazat důležitý soubor. Dobře navržený systém zabezpečení dokáže těmto typům nehod zabránit.

Při rozhodování o tom, jakou úroveň budete v systému potřebovat, odpovězte na tyto otázky:
- Jak důležitý je váš počítač (a data, která jsou na něm uložená) pro vaše podnikání?
- Má vaše společnost strategii, která vyžaduje určitou úroveň zabezpečení?
- Vyžadují auditoři společnosti určitou úroveň zabezpečení pro informace uložené ve vašem počítači?
- Budete potřebovat nějaký stupeň zabezpečení v nejbližší budoucnosti?

Proč má být systém uživatelsky přizpůsoben?

Server iSeries slouží mnoha uživatelům. Malý systém by mohl mít 3 až 5 uživatelů, kteří pracují jen s několika aplikacemi. Větší systém by mohl mít tisíce uživatelů v rozsáhlé komunikační síti, kteří pracují s mnoha aplikacemi.

Design serveru iSeries poskytuje velkou flexibilitu, pokud jde o přizpůsobení různým typům uživatelů a situací. Mnohé vlastnosti systému týkající se jeho vzhledu vůči uživatelům a způsobu práce můžete změnit.

Když je systém nový, pravděpodobně žádné velké přizpůsobení nebudete potřebovat ani vyžadovat. IBM dodává systém s počátečním nastavením mnoha voleb zvaným **předvolby**. Tyto předvolby jsou hodnoty, které v nových instalacích obvykle fungují nejlépe.

Poznámka: Všechny nové systémy jsou dodávány s předvolenou úrovní zabezpečení **40**. Tato úroveň zabezpečení zajišťuje, že systém smějí používat pouze uživatelé, které jste definovali. Zabraňuje také možným rizikům narušení integrity a bezpečnostním rizikům z programů, které umějí zabezpečení obejít.

Pokud ale nějaké přizpůsobení provedete, může se systém stát jednodušším a efektivnějším nástrojem pro uživatele. Můžete například zajistit, aby vždy při přihlášení získali uživatelé správné menu. Nebo můžete zajistit, aby se sestavy uživatelů tiskly na správné tiskárně. Uživatelé budou systému více důvěřovat, když počáteční přizpůsobení způsobí, že systém bude vypadat a chovat se jako jejich vlastní systém.

Proč máte být odpovědní?

Různé společnosti mají k zabezpečení různý přístup. Někdy mají za všechny aspekty zabezpečení odpovědnost programátoři. Jindy jsou za systém odpovědné osoby, které ho spravují. Pokud si nejste jisti, jak mají být odpovědnosti ve společnosti přiřazeny, použijte tento přístup:

- Způsob plánování zabezpečení prostředků závisí na tom, zda vaše společnost aplikace kupuje nebo vyvíjí. Pokud vyvíjíte vlastní aplikace, konzultujte potřeby zabezpečení prostředků během procesu vývoje. Kupujete-li aplikace, spolupracujte s autorem návrhu aplikace. V obou případech by lidé, kteří aplikace navrhují, měli vzít zabezpečení v úvahu jako součást návrhu.
- Za nastavení zabezpečení by měl být odpovědný správce systému. Správce systému definuje uživatele systému a jejich přístup k systému. Správce systému je také odpovědný za ostatní zabezpečení v systému, jako je například zálohování a obnova informací.
- Správce systému by také měl systém přizpůsobit, protože mnohé prvky zabezpečení mají důležitou roli v přizpůsobení systému.

Ať už používáte kteroukoliv metodu přiřazení odpovědnosti za zabezpečení, **diskutujte o zásadách zabezpečení**. Jeden z vedoucích pracovníků vaší společnosti by měl každému sdělit, nejlépe písemně, že informace v počítačích jsou důležitým majetkem. Tyto informace byste měli chránit tak, jako chráníte jakýkoliv jiný majetek. Příklad zásad zabezpečení najdete v tématu Příklad: Zásady zabezpečení společnosti JKL Toy Company.

Když jste se pochopili potřebu zabezpečení ve svém systému, můžete si prostudovat přehled úvah o zabezpečení systému.

Přehled základního zabezpečení systému

Chcete-li plánovat efektivně, měli byste porozumět, jak souvisí váš pohled na to, čeho chcete dosáhnout, s nástroji, které systém nabízí. Potřebujete znát, jak uživatelské a systémové funkce spolupracují a pomohou vám dosáhnout požadovaných cílů.

Následující témata představí důležité části zabezpečení a přizpůsobení a jejich vzájemné vztahy. Cílem těchto témat je, abyste před vlastním plánováním získali potřebný přehled. Všechny koncepce, které jsou zde stručně uvedeny, budou podle potřeby popsány podrobněji v průběhu procesu plánování.

- Vestavěné zabezpečení systému.
- Základní terminologie.
- Zabezpečení z hlediska uživatele.
- Systémové nástroje pro zabezpečení a přizpůsobení.

Vestavěné zabezpečení systému

Všechny části systémové strany zabezpečení jsou vestavěny v systému. Nemusíte kupovat samostatný produkt. Tento integrovaný přístup má několik výhod:

- Zabezpečení je konzistentní se zbytkem operačního systému. Používají se stejné obrazovky, příkazy a terminologie.
- Uživatelé nemohou zabezpečení obcházet, protože není samostatným softwarem.
- Řádně navržené zabezpečení má minimální vliv na výkonnost.
- Zabezpečení stále drží krok s vývojem nového softwaru. Když se objeví nové funkce, je k dispozici i zabezpečení těchto funkcí.

Systém iSeries se dodává s úrovní zabezpečení 40, která brání neoprávněným uživatelům přihlásit se do systému. Zabraňuje také možným ohrožením integrity a zabezpečení ze strany programů, které by chtěly obejít zabezpečení. Určitá nastavení zabezpečení však lze přizpůsobit nebo změnit úrovně zabezpečení. Úrovně zabezpečení jsou popsány v tématu Výběr úrovně zabezpečení.

Nyní, když lépe rozumíte principům vestavěného zabezpečení, byste se měli seznámit s běžnou terminologií systému iSeries.

Základní terminologie

Tato sada základní terminologie je velmi důležitá pro porozumění systému iSeries a jeho zabezpečení:

Objekt Objekt je pojmenovaný prostor v systému, se kterým lze manipulovat. Nejběžnějšími příklady objektů jsou soubory a programy. K dalším typům objektů patří příkazy, fronty, knihovny a složky. Objekty jsou v systému identifikovány podle jména objektu, typu objektu a knihovny, ve které je objekt umístěn. Každý objekt v systému může být zabezpečen.

Knihovna
Knihovna je zvláštní typ objektu, který se používá k seskupování jiných objektů. Mnoho objektů v systému je umístěno v knihovnách.

Adresář
Adresář je další způsob, jak seskupovat objekty v systému. Objekty mohou být umístěny v adresáři. Adresář může být obsažen v jiném adresáři, čímž vzniká hierarchická struktura.

Nyní, když lépe rozumíte základní terminologii zabezpečení systému iSeries, byste se měli seznámit se zabezpečením z hlediska uživatele.

Zabezpečení z hlediska uživatele

Uživatelé vnímají zabezpečení na základě toho, jak mohou používat a provádět úlohy v systému. Patří k tomu i možnosti, které uživatelé mají při provádění těchto úkolů při interakci se systémem. U zabezpečení je důležité vzít v úvahu uživatelské hledisko. Pokud například nastavíte dobu vypršení platnosti hesel na pět dní, budou se uživatelé rozčilovat a narušíte tím jejich schopnost vykonávat práci. Příliš uvolněná zásada obnovování hesel však na druhou stranu může přinést problémy se zabezpečením.

Chcete-li zabezpečit systém správným způsobem, měli byste zabezpečení rozdělit na určité části, které budete moci plánovat, spravovat a monitorovat. Z hlediska uživatelů můžete zabezpečení systému rozdělit do následujících několika částí:

Fyzický přístup k systému

Fyzické zabezpečení chrání systémovou jednotku, všechna systémová zařízení a záložní paměťová média, jako jsou diskety, pásky a disky CD-ROM, před náhodnou nebo záměrnou ztrátou či poškozením.

Většina opatření, která k zajištění fyzického zabezpečení systému podniknete, jsou vůči systému externí. Systém je však dodáván s blokovacím zámkem nebo elektronickým zámkem, který zabraňuje neoprávněnému provádění činností na systémové jednotce.

Podrobnější informace o plánování fyzického zabezpečení systému najdete v tématu Plánování fyzického zabezpečení.

Jak se uživatelé přihlašují

Zabezpečení přihlášení zabraňuje osobám, které nejsou v systému identifikovány, aby se přihlásily do systému. Chce-li se uživatel přihlásit, musí zadat platnou kombinaci ID uživatele a hesla.

Chcete-li zajistit, aby nebylo narušeno zabezpečení přihlášení, můžete použít systémové hodnoty a profily individuálních uživatelů. Můžete například vyžadovat, aby se pravidelně měnila hesla. Uživatelům lze také zabránit, aby používali hesla, která lze snadno uhádnout.

Co smějí uživatelé dělat

Důležitou úlohou zabezpečení a přizpůsobení systému je definovat, co smějí uživatelé dělat. Z hlediska zabezpečení je to často **omezující** funkce, například zabránění uživatelům, aby mohli zobrazit určité informace. Z hlediska přizpůsobení systému je to **zplnomocňující** funkce. Řádně přizpůsobený systém umožňuje uživatelům kvalitní plnění úkolů, tím že odstraňuje nadbytečné úkoly a informace.

Některé metody definování pravomocí uživatelů jsou v kompetenci správce systému, za jiné odpovídají programátoři. Zde se zaměříme především na činnosti, které provádí správce systému. Popisy všech systémových hodnot najdete v kapitole 3, Systémové hodnoty zabezpečení v publikaci *Zabezpečení - referenční informace* (SC41-5302).

V profilech individuálních uživatelů, popisech úloh a třídách jsou k dispozici parametry, které umožňují určovat, co může uživatel provádět v systému. Následující seznam stručně popisuje dostupné metody:

Omezení uživatelů na několik funkcí
: Uživatele lze na základě jejich uživatelských profilů omezit tak, aby mohli používat pouze určitý program, menu nebo sadu menu a několik systémových příkazů. Uživatelské profily obvykle vytváří a řídí správce systému.

Omezení systémových funkcí
: Systémové funkce umožňují ukládat a obnovovat informace, spravovat tiskový výstup a vytvářet nové uživatele systému. Každý uživatelský profil určuje, které z běžných systémových funkcí může daný uživatel provádět.

  V systému iSeries provádíte systémové funkce pomocí příkazů jazyka CL (control Language) a pomocí rozhraní API. Protože každý příkaz a rozhraní API je objekt, lze pomocí oprávnění k objektu řídit, kdo může daný příkaz nebo rozhraní používat k provádění systémových funkcí.

Určení, kdo může používat soubory a programy
: Zabezpečení prostředků umožňuje řídit používání všech objektů v systému. U každého objektu lze určit, kdo ho smí používat a jakým způsobem. Můžete například zadat, že určitý uživatel může pouze prohlížet informace obsažené v nějakém souboru, zatímco jiný uživatel smí tyto údaje měnit; třetí uživatel může soubor nejen měnit, ale může celý soubor i smazat.

Zabránění zneužití systémových prostředků
: Výkon zpracování systému může být pro firmu stejně důležitý jako data, která jsou v systému uložena. Správce systému může zajistit, aby uživatelé nezneužívali systémové prostředky tím, že budou spouštět své úlohy s vysokou prioritou, tisknout své sestavy jako první nebo používat příliš mnoho diskové paměti.

Jak systém komunikuje s jinými počítači

Pokud systém komunikuje s jinými počítači nebo programovatelnými pracovními stanicemi, mohou být nutná další bezpečnostní opatření. Při nesprávném zabezpečení by mohl nějaký uživatel z jiného počítače v síti spustit úlohu nebo přistupovat k informacím na vašem počítači a neprojít procesem přihlášení.

Systémové hodnoty a atributy sítě slouží k tomu, abyste mohli určit, zda v systému povolíte vzdálené spouštění úloh, vzdálený přístup k datům nebo vzdálený přístup k počítači. Pokud vzdálený přístup povolíte, můžete určit, jaké zabezpečení chcete vynutit. Popis všech systémových hodnot najdete v kapitole 3 nazvané ″Systémové hodnoty zabezpečení″ v publikaci *Zabezpečení - referenční informace* (SC41-5302).

Jak ukládat informace o zabezpečení

Informace v systému je nutné pravidelně zálohovat. Spolu s daty je třeba ukládat také informace o zabezpečení. Zhroutí-li se systém, musíte být schopni obnovit informace o uživatelích systému, informace o oprávněních a samotná data.

V tématu Uložení informací o zabezpečení je vysvětleno, jak ukládat informace o zabezpečení. Podrobnější informace o zálohování a obnově informací o zabezpečení najdete v tématu Zálohování a obnova v aplikaci Information Center.

Jak monitorovat plán zabezpečení

Systém nabízí několik nástrojů k monitorování účinnosti zabezpečení:

- Dojde-li k narušení zabezpečení, systémovému operátorovi je odeslána příslušná zpráva.
- Různé transakce související se zabezpečením mohou být zaznamenávány do zvláštního monitorovacího žurnálu.

Obecné použití těchto nástrojů je popsáno v tématu Monitorování zabezpečení. Podrobnější informace o prověřování zabezpečení najdete v kapitole 9 nazvané ″Prověřování zabezpečení systému″ v publikaci *Zabezpečení - referenční informace* (SC41-5302).

Chcete-li lépe pochopit, jak přizpůsobit systém, měli byste porozumět přizpůsobení z hlediska uživatele.

Přizpůsobení systému z hlediska uživatele: Systém lze přizpůsobit tak, aby uživatelé mohli lépe plnit své každodenní úkoly. Nejlepšího přizpůsobení systému pro uživatele dosáhnete, budete-li přemýšlet o tom, co uživatelé potřebují k úspěšné práci. Systém lze přizpůsobit tak, aby zobrazoval menu a aplikace různými způsoby:

Nabídka vyhovující potřebám uživatelů

Většina z nás si uspořádá pracovní stoly a kanceláře tak, aby nejčastěji používané věci byly snadno dostupné. Přemýšlejte o přístupu uživatelů k systému stejným způsobem. Uživateli by se po přihlášení do systému mělo zobrazit menu (obrazovka), které používá nejčastěji. Uživatelské profily lze snadno navrhnout tak, aby byl tento požadavek splněn.

Odstranění nepotřebného

Ve většině systémů existuje mnoho různých aplikací. Většina uživatelů chce vidět pouze to, co potřebují ke své práci. Vyhradíte-li jim v systému pouze několik funkcí, usnadníte jim práci. Pomocí uživatelských profilů, popisů úloh a odpovídajících menu můžete každému uživateli poskytnout specifický pohled na systém.

Odesílání na správná místa

Uživatelé se nemají starat o to, jak dostat své sestavy na správnou tiskárnu nebo jak by měly být spouštěny dávkové úlohy. Tyto záležitosti řeší systémové hodnoty, uživatelské profily a popisy úloh.

Poskytování asistence

I když se vám podaří přizpůsobit systém požadavkům uživatelů, stále budou vznikat dotazy typu: ″Kde je má sestava?″ nebo ″Byla má úloha již provedena?″ Jednoduché rozhraní k systémovým funkcím poskytuje **Provozní asistent** a pomáhá tak uživatelům nalézt odpovědi na tyto otázky. Uživatelům s různou úrovní technických znalostí poskytují pomoc různé verze systémových obrazovek, nazývané jako **úrovně asistence**. Při dodání systému jsou obrazovky Provozního asistenta k dispozici všem uživatelům. Způsob navržení aplikací však může vyžadovat, abyste změnili metodu, kterou uživatelé přistupují k menu Provozního asistenta.

Systém iSeries nabízí systémové nástroje, které umožňují přizpůsobit zabezpečení systému tak, aby byla zajištěna ochrana prostředků, a uživatelé přitom měli k těmto prostředkům přístup.

Systémové nástroje pro zabezpečení a přizpůsobení

Chcete-li plánovat efektivně, měli byste porozumět, jak souvisí váš pohled na cíle v oblasti zabezpečení s nástroji, které vám systém nabízí. Tyto systémové nástroje můžete používat k přizpůsobení zabezpečení systému.

Úroveň zabezpečení

IBM dodává všechny nové systémy iSeries s úrovní zabezpečení 40. Úroveň zabezpečení 40 poskytuje zabezpečení hesel a prostředků a integritu systému. Chcete-li změnit aktivní úroveň zabezpečení systému, můžete změnit systémovou hodnotu QSECURITY. IBM však důrazně doporučuje ponechat úroveň zabezpečení nastavenou na hodnotu 40. Uživatel, který chce změnit úroveň zabezpečení, musí mít třídu uživatele *SECOFR nebo zvláštní oprávnění *ALLOBJ a * SECADM.

Systém nabízí čtyři úrovně zabezpečení, jak je ukázáno v této tabulce:

Tabulka 1. Úrovně zabezpečení dostupné v systému

Úroveň zabezpečení	**Popis**
Úroveň zabezpečení 20	Poskytuje pouze zabezpečení hesel.
Úroveň zabezpečení 30	Poskytuje zabezpečení hesel a prostředků.
Úroveň zabezpečení 40	Poskytuje zabezpečení hesel a prostředků; zabezpečení integrity.
Úroveň zabezpečení 50	Poskytuje zabezpečení hesel a prostředků; rozšířené zabezpečení integrity.

V tématu Výběr úrovně zabezpečení najdete podrobné informace, jak určit, která úroveň zabezpečení bude pro vaše potřeby nejvhodnější.

Systémové hodnoty

Nastavením systémových hodnot lze řídit, jak budou určité funkce operačního systému v systému iSeries fungovat. Představte si systémové hodnoty jako strategii firmy. Systémové hodnoty platí pro každého uživatele systému, pokud něco určitějšího, například uživatelský profil, nepředefinuje systémovou hodnotu.

Systémové hodnoty určují například hlavní tiskárnu, formát zobrazení data, časovou periodu požadovaných změn hesla.

Atributy sítě

Atributy sítě definují některé charakteristiky způsobu, jakým systém komunikuje s jinými počítači včetně osobních počítačů. Atributy sítě platí pro celý systém.

Skupinové profily

Skupinový profil definuje skupinu uživatelů. Představte si skupinový profil jako strategii oddělení. Skupinové profily lze používat jako vzory k vytváření profilů individuálních uživatelů. Skupinové profily lze také používat k definování způsobů, jakými budou členové skupiny smět přistupovat k objektům v systému. Další informace o skupinových profilech najdete v tématu Plánování skupin uživatelů.

Uživatelské profily

Uživatelský profil je jeden z nejmocnějších a nejuniverzálnějších objektů v systému. Obsahuje například heslo uživatele a určení menu, které se uživateli zobrazí po přihlášení. Uživatelský profil definuje, co smí a nesmí daný uživatel provádět v systému. Určuje jedinečný pohled uživatele na systém. V tématu Plánování zabezpečení uživatelů najdete rady pro plánování uživatelských profilů.

Popisy úloh

Popis úlohy využívá systémové hodnoty a uživatelské profily k určení způsobu, jakým bude systém zpracovávat úlohy uživatele. Popis úlohy nastavuje počáteční seznam knihoven uživatele; tento seznam určuje knihovny, k nimž uživatel po přihlášení automaticky získá přístup.

Zabezpečení prostředků

Správce systému nastavuje ochranu prostředků v systému tím, že určí, kdo bude oprávněn je používat a jakým způsobem k nim budou moci uživatelé přistupovat. Správce systému může nastavit oprávnění k jednotlivým objektům nebo ke skupinám objektů (seznamy oprávnění). Nejčastějšími objekty, které je třeba chránit, jsou soubory, programy a knihovny, avšak zabezpečení systému umožňuje nastavit oprávnění k libovolnému objektu v systému.

Naplánujete-li předem obecné a přehledné schéma zabezpečení, budete moci spravovat zabezpečení prostředků jednoduše a efektivně. Schéma zabezpečení prostředků vytvořené bez plánování se může stát komplikovaným a neefektivním. V tématu Plánování zabezpečení prostředků jsou popsány metody plánování zabezpečení prostředků.

Systém poskytuje několik nástrojů usnadňujících návrh přehledného schématu zabezpečení prostředků:

- **Skupinové profily:** Podobné uživatele lze seskupit do jednoho skupinového profilu. Všichni členové skupiny uživatelů pak mohou sdílet stejná oprávnění k objektům.
- **Seznamy oprávnění:** Objekty se stejnými potřebami zabezpečení lze seskupit do jednoho seznamu. Místo udělování oprávnění k jednotlivým objektům pak můžete udělit oprávnění k seznamu.
- **Vlastnictví objektů:** Každý objekt v systému má vlastníka. Vlastníky objektů mohou být skupinové profily nebo individuální uživatelé. Správné přiřazení vlastnictví objektů vám pomůže: (1) spravovat aplikace, (2) přenášet (delegovat) odpovědnost za zabezpečení informací.
- **Primární skupina:** K objektu lze určit primární skupinové oprávnění. Systém uloží primární skupinové oprávnění spolu s objektem. Použitím primárního skupinového oprávnění můžete zjednodušit správu oprávnění a zlepšit výkonnost kontroly oprávnění.
- **Oprávnění ke knihovně:** Soubory a programy, které je třeba chránit, můžete vložit do knihovny a omezit přístup k této knihovně. Je to často jednodušší než omezit přístup ke každému jednotlivému objektu. Chcete-li chránit důležité objekty, měli byste zabezpečit jak jednotlivé objekty, tak knihovnu.
- **Oprávnění k objektu:** V případech, kdy nejsou práva omezující přístup ke knihovně dostatečně přesná, můžete omezit oprávnění k jednotlivým objektům, například k souborům.
- **Veřejné oprávnění:** U každého objektu lze definovat, jaký druh přístupu bude k dispozici jakémukoliv uživateli systému, který nemá k objektu žádné jiné oprávnění. Veřejné oprávnění je účinný způsob, jak zajistit objekty, které nejsou důvěrné. Poskytuje dobrou výkonnost systému.
- **Oprávnění k adresáři:** Oprávnění k adresáři se používá stejným způsobem jako oprávnění ke knihovně. Objekty lze seskupit do adresáře a pak místo jednotlivých objektů zabezpečit celý adresář.
- **Vlastník (držitel) oprávnění:** Při vymazání objektu se odstraní také informace o oprávnění k tomuto objektu. Držitele oprávnění udržují informace o oprávněních pro programově definované soubory, které jsou mazány a opět vytvářeny aplikací. Držitele oprávnění lze využít při migraci ze systému System/36.

Nástroje zabezpečení

Nástroje zabezpečení slouží ke správě a monitorování prostředí zabezpečení systému iSeries. Pomocí nástrojů pro práci s uživatelskými profily můžete provádět tyto činnosti:

- Vyhledat, které uživatelské profily mají předvolená hesla.
- Naplánovat nedostupnost uživatelských profilů v určitou denní dobu a v určité dny v týdnu.
- Naplánovat odstranění uživatelského profilu pro případ, že zaměstnanec opustí firmu.
- Zjistit, které uživatelské profily mají zvláštní oprávnění.
- Zjistit, kdo přebírá oprávnění k objektům v systému.

Pomocí nástrojů pro zabezpečení objektů můžete sledovat veřejná a soukromá oprávnění, která jsou asociována s důvěrnými objekty. Tyto sestavy můžete pravidelně tisknout (například měsíčně), a zaměřit se tak při zabezpečování systému na aktuální problémy. Sestavy lze tisknout tak, aby obsahovaly pouze změny vzhledem k minulé sestavě.

Další nástroje umožňují monitorovat:

- spouštěcí programy

- hodnoty vztahující se k zabezpečení - v záznamech komunikace, v popisech podsystémů, výstupních frontách, frontách úloh a popisech úloh
- pozměněné nebo porušené programy

Nyní, když rozumíte důležitosti zabezpečení systému, byste se měli seznámit s popisem způsobu plánování, který je v tomto tématu použit jako příklad.

Způsob plánování základního zabezpečení systému

Témata o plánování v tomto tématu jsou koncipována tak, že postupují zvenku dovnitř a od obecného ke konkrétnímu. Plánujete-li například uživatelské profily, musíte nejprve přemýšlet o tom, co by měl uživatel vidět (vnější pohled), a potom rozhodnout, jak to provedete (pohled zevnitř). Nejprve plánujete systémové hodnoty a skupinové profily (obecné) a potom rozhodnete o výjimkách pro určité uživatele (konkrétní). Jednotlivé kroky při plánování v tématu Plánování zabezpečení uživatelů mají být prováděny v uvedeném pořadí. Představují logický postup pro popisování způsobu používání systému a pro rozhodování, jak ho zabezpečit a upravit.

Když plánujete a navrhujete zabezpečení systému, budujete ho od základů, od nejzásadnějších forem zabezpečení až po komplexnější otázky zabezpečení. Začněte s fyzickým zabezpečením systému, přejděte k popisu aplikací a systémových hodnot. Nakonec musíte uvažovat o zabezpečení pro uživatele a objekty v systému.

Tento přístup je ve všech těchto tématech o plánování ilustrován na příkladech, které používají vzorovou společnost JKL Toy Company. Téma Příklad: Představení společnosti JKL Toy Company popisuje společnost, která je používána ve všech tématech o plánování.

Stručný popis každého kroku a vztahy mezi jednotlivými kroky najdete v tématu Kroky v procesu plánování zabezpečení.

Příklad: Představení společnosti JKL Toy Company

Příklady usnadňují vysvětlování a pomáhají problematiku snáze pochopit. Proto toto téma používá společnost JKL Toy Company jako příklad. Společnost JKL Toy Company, malý, ale rychle rostoucí výrobce hraček, chce nastavit zabezpečení v systému iSeries. Prezident společnosti, pan John Smith, chce, aby nový systém iSeries pomohl společnosti JKL Toy Company zvládnout prudce stoupající růst.

Pan Smith předal paní Sharon Jonesové, hlavní účetní, odpovědnost administrátora systému a správce systému. Paní Jonesová se chce ujistit, že celá instalace včetně zabezpečení proběhne bez problémů. Považuje plánování za velmi důležité. Dnes je společnost malá a většina zaměstnanců má přístup k většině informací. Ale paní Jonesová ví, že se to s růstem společnosti změní. Snaží se řešit problémy s předstihem.

Společnost JKL Toy Company plánuje, že bude v systému zpočátku používat následující aplikace: Zákaznické objednávky, Řízení zásob, Smlouvy a ceníky a Pohledávky. Při pročítání témat o plánování se podrobněji seznámíte s tím, jak společnost JKL Toy Company pracuje se zabezpečením.

Téma Kroky v procesu plánování vysvětluje jednotlivé kroky, které musíte při plánování zabezpečení systému provést.

Kroky v procesu plánování zabezpečení

Následující diagram popisuje všechny kroky procesu plánování zabezpečení a znázorňuje, jak každý krok souvisí se zbytkem procesu.

Tabulka 2. Kroky v procesu plánování zabezpečení

Krok	Akce prováděné v tomto kroku	Souvislost s ostatními kroky
Plánování fyzického zabezpečení	Určíte, jak chcete chránit systémovou jednotku, zařízení a zálohovací média.	Většina těchto informací závisí na zbytku procesu. Informace o plánování fyzického zabezpečení nezadáváte do systému. Některé z těchto informací ale budete potřebovat při plánování systémových hodnot.

Tabulka 2. Kroky v procesu plánování zabezpečení (pokračování)

Krok	Akce prováděné v tomto kroku	Souvislost s ostatními kroky
Plánování aplikace	Popíšete účel, hlavní menu a knihovny všech aplikací.	Poskytuje základnu pro zbytek procesu plánování a další vaše rozhodnutí o zabezpečení. Tyto informace nezadáváte do systému.
Plánování celkové strategie zabezpečení	Rozhodnete, jaká bude vaše celková strategie zabezpečení. Zvolíte systémové hodnoty, které budou tento přístup k zabezpečení podporovat.	Při určování celkové strategie zabezpečení použijte informace o plánování aplikací. Zvolené systémové hodnoty ovlivní plánování uživatelských a skupinových profilů.
Plánování skupin uživatelů	Rozhodnete, jak rozdělíte uživatele do skupin. Rozhodnete, jakou charakteristiku bude mít každá skupina a jak je v systému definujete.	Při definování skupin v systému použijte popisy aplikací. Skupiny uživatelů, které definujete, ovlivní plánování individuálních uživatelů v systému.
Plánování profilů individuálních uživatelů	Každého uživatele systému zařadíte do skupiny. Definujete uživatele včetně charakteristiky, kterou se liší od zbytku skupiny. Někteří uživatelé mohou například potřebovat jiný přístup k aplikaci nebo knihovně než zbytek skupiny.	Při definování individuálních uživatelů použijte plánování aplikací a plánování skupin uživatelů.
Plánování zabezpečení prostředků	Rozhodnete, které aplikace by měly být každému v systému dostupné. Chcete-li omezit určité aplikace, rozhodnete, kteří uživatelé a které skupiny by je směly používat.	Při plánování zabezpečení prostředků použijte plánování aplikací a plánování skupinových profilů.
Plánování instalace aplikací	Rozhodnete, jak stanovit vlastníky knihoven aplikací a veřejná oprávnění k nim.	Při plánování instalace aplikací použijte informace plánování zabezpečení prostředků.

Proces plánování zabezpečení byste měli zahájit plánováním zabezpečení uživatelů.

Plánování zabezpečení uživatelů

Plánování zabezpečení uživatelů zahrnuje plánování všech oblastí, ve kterých má zabezpečení vliv na uživatele v systému. Je nezbytné, abyste popsali následující oblasti:

Fyzické zabezpečení
Fyzické zabezpečení zahrnuje ochranu serveru iSeries před náhodným (nebo úmyslným) poškozením a krádeží. Dále zahrnuje ochranu všech pracovních stanic, tiskáren a paměťových médií. Téma ″Plánování fyzického zabezpečení″ obsahuje další informace o plánování fyzického zabezpečení, rizicích a doporučeních ze strany IBM.

Zabezpečení aplikací
Zabezpečení aplikací se zabývá tím, jaké aplikace uložíte v systému, jak je budete chránit a jak zároveň uživatelům umožníte přístup k těmto aplikacím. Téma Plánování zabezpečení aplikací podrobně popisuje aplikace a jejich konvence pojmenování.

Strategie celkového zabezpečení
Plánování celkového zabezpečení zahrnuje vytvoření plánu zabezpečení, který bere v úvahu jak současnou situaci, tak budoucí plány vašeho podnikání. Téma Plánování celkové strategie zabezpečení poskytuje další informace o určování zásad zabezpečení, úrovně zabezpečení, důležitosti hesel a systémových hodnot.

Zabezpečení skupin uživatelů
Uživatelé ve skupině uživatelů potřebují používat stejné aplikace stejným způsobem. Plánování skupin

uživatelů zahrnuje určování pracovních skupin, které chtějí systém používat, a požadavků těchto skupin na aplikace. Téma Plánování skupin uživatelů poskytuje podrobné informace o identifikaci skupin uživatelů, plánování skupinových profilů, výběru systémových hodnot a určování prostředí uživatele.

Zabezpečení individuálních uživatelů
Poté, co jste určili, které skupiny uživatelů potřebujete, můžete plánovat profily individuálních uživatelů. Téma Plánování profilů individuálních uživatelů poskytuje další informace o pojmenování uživatelů v systému, určování odpovědností individuálních uživatelů a výběru systémových hodnot.

Ve všech tématech o plánování najdete odkazy na plánovací formuláře, do kterých můžete zaznamenat svá rozhodnutí týkající se plánování.

Plánování fyzického zabezpečení

Když připravujete instalaci serveru iSeries, měli byste vytvořit plán fyzického zabezpečení pomocí těchto otázek:

- Kam umístíte systémovou jednotku?
- Kam umístíte jednotlivé obrazovkové stanice?
- Kam umístíte tiskárny?
- Jaké další vybavení potřebujete (kabely, telefonní linky, nábytek nebo paměťové oblasti)?
- Jaká učiníte opatření na ochranu systému pro případy nouze, jako je například požár nebo výpadek napájení?

Fyzické zabezpečení by mělo být součástí plánování celkového zabezpečení. Možná budou tato opatření závislá na tom, kam umístíte systém a jeho zařízení.

Svá rozhodnutí o fyzickém zabezpečení systému můžete zaznamenat do formuláře Plánování fyzického zabezpečení. Chcete-li zajistit pokrytí všech aspektů fyzického zabezpečení, prostudujte si tato témata:

- Fyzické zabezpečení systémové jednotky: Toto téma uvádí podrobné informace o zabezpečení samotného systému.
- Fyzické zabezpečení dokumentace systému a paměťových médií: Toto téma obsahuje informace o zabezpečení dokumentů systému a paměťových médií.
- Fyzické zabezpečení pracovních stanic: Toto téma pojednává o způsobech zabezpečení pracovních stanic.
- Fyzické zabezpečení tiskáren a tiskových výstupů: Toto téma uvádí podrobné informace o fyzické ochraně tiskáren a jejich výstupů.
- Plánování zásad zabezpečení: Toto téma vysvětluje, jak vypracovat směrnice pro uživatele a zásady zabezpečení.

Každá systémová jednotka má ovládací panel, ze kterého se počítač obsluhuje a ze kterého se provádějí speciální systémové operace, jako je například zapínání a vypínání systému. Chcete-li zabránit neoprávněnému použití těchto systémových operací, měla by každá systémová jednotka mít buď přepínač s klíčkem, nebo elektronický zámek. Poskytují sice systémové jednotce nějakou ochranu, ale přepínač s klíčkem ani elektronický zámek nemohou nahradit adekvátní fyzické zabezpečení.

Fyzické zabezpečení systémové jednotky

Server iSeries nevyžaduje počítačovou místnost se speciálními ovládacími prvky. Systémovou jednotku často naleznete uprostřed kancelářské místnosti, do které má přístup mnoho lidí. Zákazníkům se líbí, že je server iSeries prostorově nenáročný a že se snadno udržuje. Ale tyto vlastnosti mohou znamenat také určitá bezpečnostní rizika. Jedna osoba by například mohla systémovou jednotku snadno ukrást nebo z ní vyjmout důležité komponenty.

Měli byste učinit taková opatření, která by zajistila, že systémová jednotka bude na bezpečném místě. Nejlepším umístěním je vlastní zamčená místnost. Systémová jednotka by měla být alespoň na místě, které lze mimo pravidelnou pracovní dobu zamknout.

Rizika pro systémovou jednotku

Kromě krádeže systémové jednotky nebo jejích komponent existují další rizika plynoucí z nedostatečného fyzického zabezpečení systémové jednotky:

Neúmyslné přerušení operací systému

Mnohé problémy se zabezpečením pocházejí od oprávněných uživatelů systému. Předpokládejme, že jedna z obrazovkových stanic v systému je uzamčena. Systémový operátor odešel z pracoviště na pracovní schůzku. Zoufalý uživatel obrazovkové stanice chodí kolem systémové jednotky a říká si: ″Možná, že stačí stisknout jedno tlačítko a bude po problému″. Ale tím tlačítkem může systém vypnout nebo ho znovu zavést, zatímco je spuštěno mnoho jiných úloh. K obnovení částečně aktualizovaných souborů pak budete potřebovat několik hodin. Pomocí přepínače s klíčkem u systémové jednotky tomu můžete zabránit.

Obcházení zabezpečení pomocí funkce nástrojů DST (Dedicated Service Tools)

Zabezpečení neřídí servisní funkce prováděné systémem, protože systémový software by možná nepracoval správně, pokud byste chtěli tyto funkce provádět. Šikovný člověk, který zná nebo uhodne ID uživatele a heslo SST, by mohl systému způsobit značné škody. Další informace o servisních nástrojích najdete v tématu SST v rámci aplikace Information Center.

Doporučení

- V ideálním případě by měla být systémová jednotka umístěna v zamčené místnosti. Pokud to není možné, umístěte ji tam, kam nemají přístup cizí osoby. Zvolte takové umístění, které mohou odpovědní zaměstnanci monitorovat. Následující pokyny vám pomohou chránit systém před náhodným nebo úmyslným vměšováním:
- Použijte elektronický zámek nebo uzamčení klíčem:
  - Nastavte normální provozní režim, pokud chcete mít možnost spustit systém bez použití klíče.
  - Nastavte provozní režim Auto, pokud chcete při spuštění a zastavení systému použít funkci automatického zapnutí a vypnutí.
  - Vyjměte klíč a uložte ho na bezpečné místo.
- Okamžitě po instalaci systému a po každém použití systému obslužným personálem změňte ID uživatele a heslo SST. Podrobné informace o tom, jak ID uživatele a heslo servisních nástrojů DST změníte, najdete v tématu SST v aplikaci Information Center.

Možná budete chtít prostudovat příklad plánu společnosti JKL Toy Company na zabezpečení jednotky ještě předtím, než budete plánovat fyzické zabezpečení dokumentace systému a paměťových médií.

Příklad: Formulář společnosti JKL Toy Company: Plánování fyzického zabezpečení — systémová jednotka: Níže najdete příklad formuláře Plánování fyzického zabezpečení systémové jednotky, který Sharon Jonesová použila pro svůj systém:

Tabulka 3. Příklad: Formulář společnosti JKL Toy Company: Plánování fyzického zabezpečení - systémová jednotka

Formulář Plánování fyzického zabezpečení systému	
Zhotovila: Sharon Jonesová	Datum: 9/2/99
Systémová jednotka:	
Popište svá bezpečnostní opatření sloužící k ochraně systémové jednotky (například uzamčené místnosti):	Systémová jednotka je umístěna v účtárně. Během dne jsou nablízku lidé z účtárny, kteří mají systémovou jednotku neustále pod dohledem. Lidé z účtárny jsou odpovědní také za menší hotovost a důležité záznamy. Mimo řádnou pracovní dobu je místnost uzamčená.
Jaké nastavení uzamčení klíčem se obvykle používá?	Obvyklé
Kde je uložen klíč?	Malý trezor v Sharonině kanceláři.
Další poznámky týkající se systémové jednotky:	Systémová jednotka bude snadno dostupná. Sdělte lidem z účtárny, aby nepovolaným osobám nedovolili manipulaci se systémovou jednotkou.

Jakmile naplánujete fyzické zabezpečení systémové jednotky, můžete začít plánovat fyzické zabezpečení systémové dokumentace a paměťových médií.

Fyzické zabezpečení dokumentace systému a paměťových médií

Další aspekt plánu fyzického zabezpečení se zabývá uložením důležité dokumentace systému a paměťových médií. Dokumentace systému zahrnuje informace, které IBM odesílá spolu se systémem: informace o hesle, plánovací formuláře a všechny sestavy, které systém generuje.

Zálohovací média mohou zahrnovat pásky, diskety, disky CD-ROM a DVD v závislosti na systému. Dokumentaci systému a zálohovací média byste měli uložit nejen na pracovišti, ale také na jiném vzdáleném místě. V případě pohromy budete tyto informace potřebovat, abyste mohli obnovit systém. Následující informace navrhují, jakým způsobem máte ukládat dokumentaci systému a paměťová média. Až se rozhodnete, zaznamenejte své volby do části Zálohovací média a dokumentace ve formuláři Plánování fyzického zabezpečení.

Bezpečné uložení dokumentace systému

Hesla SST a správce systému jsou pro činnost systému velmi důležitá. Měli byste je zapsat a uložit na bezpečném, tajném místě. Kopie těchto hesel uložte na vzdáleném místě mimo kancelář, abyste je mohli použít v případě pohromy.

Přemýšlejte o umístění další důležité dokumentace systému, jako jsou například nastavení konfigurace a knihovny hlavních aplikací, mimo pracoviště, abyste je mohli použít k obnově v případě pohromy.

Bezpečné uložení paměťových médií

Již při instalaci systému naplánujte pravidelné ukládání všech informací v systému na pásky nebo na jiná paměťová média. Tato záložní média vám umožní obnovit systém v případě potřeby. Také tato záložní média byste měli uložit na bezpečné místo mimo pracoviště.

Rizika

- Poškození záložních médií: Kdyby záložní média zničila živelná pohroma nebo vandalové, nemohli byste systém obnovit jinak, než z tiskových výstupů.
- Krádež záložních médií nebo hesel: Možná máte na záložních médiích uloženy důvěrné obchodní informace. Šikovný člověk by mohl tyto informace uložit na jiný počítač, vytisknout je nebo zpracovat.

Doporučení

- Uložte všechna hesla a zálohovací média do uzamčené ohnivzdorné skříňky.
- Kopie záložních médií pravidelně ukládejte na bezpečné místo mimo pracoviště, alespoň jednou týdně.

Možná si budete chtít prostudovat příklad plánu společnosti JKL Toy Company na ukládání dokumentace systému, než začnete s plánováním fyzického zabezpečení pracovních stanic.

Příklad: Formulář společnosti JKL Toy Company: Plánování fyzického zabezpečení — záložní média a dokumentace: Sharon Jonesová ze společnosti JKL Toy Company dokončila část formuláře Plánování fyzického zabezpečení nazvanou Záložní média a dokumentace, jak je vidět v níže uvedené tabulce:

Tabulka 4. Příklad: Formulář společnosti JKL Toy Company: Plánování fyzického zabezpečení - záložní média a dokumentace

Formulář Plánování fyzického zabezpečení systému	
Zhotovila: Sharon Jonesová	Datum: 9/2/99
Záložní média a dokumentace:	
Kde jsou na vašem pracovišti uloženy záložní pásky?	Ve velkém ohnivzdorném trezoru.
Kde jsou uloženy záložní pásky mimo vaše pracoviště?	V ohnivzdorném trezoru umístěném v kanceláři hlavního účetního společnosti.
Kde jsou uložena hesla správce systému, obsluhy a heslo DST?	V trezoru umístěném v kanceláři Johna Smithe.
Kde je uložena důležitá systémová dokumentace, jako je sériové číslo a konfigurace?	Ve velkém trezoru mimo pracoviště a v kanceláři hlavního účetního.

Jakmile naplánujete zabezpečení paměti a dokumentace, můžete začít plánovat fyzické zabezpečení pracovních stanic.

Plánování fyzického zabezpečení pracovních stanic

Ve většině případů chcete, aby všichni uživatelé měli možnost přihlásit se do systému z libovolné dostupné pracovní stanice a provádět všechny oprávněné funkce. Máte-li ale pracovní stanice, které jsou buď úplně veřejné, nebo úplně soukromé, můžete chtít zavést zvláštní opatření, například u obrazovkových stanic, které mohou ukládat úhozy, a u osobních počítačů, které vyžadují zvláštní pozornost. Myslete na to při vyplňování části 2 (Fyzické zabezpečení pracovních stanic a tiskáren) formuláře Plánování fyzického zabezpečení.

Rizika spojená s pracovními stanicemi

Neoprávněné použití veřejně umístěné pracovní stanice

Pokud lidé mimo vaši společnost mají snadný přístup na vaše pracoviště, mohli by vidět důvěrné informace. Pokud uživatel systému opustí pracovní stanici a zůstane přihlášen, mohl by cizí osobě umožnit přístup k důvěrným informacím.

Neoprávněné použití pracovní stanice umístěné v soukromí

Pracovní stanice umístěná v úplném soukromí dává vetřelci příležitost trávit dlouhé hodiny při pokusech obejít vaše zabezpečení, aniž by byl zpozorován.

Obcházení bezpečnostních opatření pomocí funkce přehrávání nebo programu pro přihlášení z PC na obrazovkové stanici

Mnoho obrazovkových stanic má funkci pro záznam a přehrávání, která uživatelům umožňuje ukládat často používané úhozy a opakovat je stisknutím jediné klávesy. Používáte-li osobní počítač jako pracovní stanici systému iSeries, můžete napsat program, který bude automatizovat proces přihlášení. Protože uživatelé často používají proces přihlášení, mohli by se rozhodnout, že ID uživatele a hesla uloží, místo aby je zadávali při každém přihlášení.

Doporučení

Až budete nastavovat fyzické zabezpečení pracovních stanic, vezměte v úvahu tato doporučení:

- Pokud je to možné, vyvarujte se umístění pracovních stanic na úplně veřejných nebo úplně soukromých místech.
- Zdůrazněte uživatelům systému význam odhlášení před opuštěním pracovní stanice. Procedury odhlášení by měly být zahrnuty do zásad zabezpečení.
- Zdůrazněte také, že zaznamenání hesla v obrazovkové stanici nebo v programu PC narušuje zabezpečení systému. Zaznamenání hesla by mělo být zahrnuto do zásad zabezpečení.
- Učiňte opatření, která uživatelům zabrání opustit pracovní stanice ve veřejných místech bez odhlášení, použijte k tomu systémové hodnoty QINACTITV a QINACTMSGQ.
- Omezte funkce, které mohou uživatelé provádět na veřejných pracovních stanicích tím, že poskytnete oprávnění pouze uživatelům s omezeným oprávněním k těmto pracovním stanicím.
- Zabraňte uživatelům se zabezpečovacím nebo servisním oprávněním v přihlášení na soukromých pracovních stanicích. Zkontrolujte, kam se uživatel s těmito oprávněními přihlásil, pomocí systémové hodnoty QLMTSECOFR.
- Nedovolte uživatelům přihlásit se na více pracovních stanicích najednou. Zkontrolujte, kam se uživatel přihlásil, pomocí systémové hodnoty QLMTDEVSSN, která omezuje počet relací zařízení.

Podrobné informace o tom, jak máte tato doporučení realizovat, najdete v tématech Výběr systémových hodnot ovlivňujících přihlášení a Plánování zabezpečení prostředků pracovních stanic.

U formuláře Plánování fyzického zabezpečení potřebujete zjistit, které pracovní stanice by mohly představovat riziko kvůli fyzickému umístění. Možná si budete chtít prostudovat příklad, jak paní Sharon Jonesová naplánovala fyzické zabezpečení pracovních stanic společnosti JKL Toy Company.

Až naplánujete zabezpečení pracovních stanic, můžete začít s plánováním fyzického zabezpečení tiskáren a tiskových výstupů.

Fyzické zabezpečení tiskáren a tiskových výstupů

Jakmile se spustí tisk informací, nemůže již zabezpečení systému kontrolovat, kdo tiskový výstup vidí. Chcete-li minimalizovat hrozbu, že někdo uvidí citlivé obchodní informace, měli byste zabezpečit tiskárny a tiskový výstup. Měli byste také vytvořit zásadu, která se bude zabývat tiskem důvěrných obchodních informací.

Rizika spojená s tiskárnami a tiskovým výstupem

Ve vaší situaci se mohou vyskytnout následující rizika. Jsou to nejobvyklejší bezpečnostní rizika, která jsou spojena s tiskárnou a tiskovým výstupem. Měli byste prozkoumat také další rizika, která se mohou v prostředí vašeho podniku vyskytnout.

- Tiskárna umístěná na veřejném místě by mohla neoprávněným osobám poskytnout přístup k důvěrným informacím.
- Tiskový výstup ponechaný na stole by mohl odhalit tajné informace.
- Systém by měl mít jen jednu nebo dvě tiskárny. Možná potřebujete tisknout cenné nebo důvěrné informace, například platební šeky, které by zaměstnanci vaší společnosti neměli vidět.

Doporučení

Následující doporučení vám mohou pomoci snížit bezpečnostní rizika, která jsou spojena s tiskárnami a jejich výstupy.

- Zdůrazněte uživatelům systému význam ochrany důvěrných tiskových výstupů. Oznamte jim rozhodnutí týkající se fyzického zabezpečení tiskáren v zásadách zabezpečení.
- Vyvarujte se umisťování tiskáren na veřejných místech.
- Naplánujte tisk přísně důvěrných výstupů a pověřte důvěryhodnou osobu, aby zůstala u tiskárny, dokud nebude tisk dokončen.

Téma Plánování zabezpečení pro tiskárny a tiskový výstup pojednává o návrzích na zacházení s důvěrným tiskovým výstupem.

Možná budete chtít prostudovat příklad plánu společnosti JKL Toy Company na zabezpečení tiskáren ještě předtím, než začnete plánovat zásady zabezpečení.

Příklad: Formulář společnosti JKL Toy Company: Plánování fyzického zabezpečení — pracovní stanice a tiskárna: Níže najdete příklad druhé části plánu fyzického zabezpečení, který Sharon Jonesová použila pro společnost JKL Toy Company:

Tabulka 5. Příklad: Formulář společnosti JKL Toy Company: Plánování fyzického zabezpečení - pracovní stanice a tiskárna

Formulář Plánování fyzického zabezpečení systému			část 2 ze 2
Fyzické zabezpečení pracovních stanic a tiskáren			
Jméno pracovní stanice nebo tiskárny	Její umístění nebo popis	Bezpečnostní riziko	Nezbytná ochranná opatření
DSP06	Nákladní prostor.	Příliš obecné.	Automatické odhlášení. Omezte funkce, které mohou být prováděny na pracovní stanici.
DSP09	Zákaznické středisko.	Příliš obecné.	Automatické odhlášení. Omezte funkce, které mohou být prováděny na pracovní stanici.
RMT12	Detašovaná prodejní kancelář.	Příliš soukromé.	Neumožnit správci systému přihlásit se zde do systému.

Tabulka 5. Příklad: Formulář společnosti JKL Toy Company: Plánování fyzického zabezpečení - pracovní stanice a tiskárna (pokračování)

PRT02	Účtárna, blízko systémové jednotky.	Mohly by být prohlíženy citlivé informace, jako jsou ceníky.	Určit někoho, kdo bude monitorovat tiskové výstupy.

Jakmile dokončíte Formulář Plánování fyzického zabezpečení systému, přejděte na téma ″Plánování celkové strategie zabezpečení″.

Plánování zásad zabezpečení

Rozeslání bezpečnostních směrnic všem zaměstnancům může být užitečné. Zdůrazníte tak význam zásad zabezpečení, které se týkají fyzického zabezpečení a zabezpečení systému. Stejné směrnice můžete dávat i novým uživatelům, které do systému přidáte později.

Do těchto směrnic byste měli zahrnout některé obecné pokyny týkající se zabezpečení systému, například, jak se odhlašovat z pracovních stanic a proč nesdílet hesla. Tyto směrnice by také měly obsahovat informace o specifických rozhodnutích, která jste provedli v souvislosti se zabezpečením.

Při čtení těchto plánovacích informací si poznamenejte, co by měly obsahovat vaše bezpečnostní směrnice. Nezapomeňte také na poznámky pro zásady zabezpečení.

Například paní Sharon Jonesová ze společnosti JKL Toy Company si při plánování fyzického zabezpečení zapsala tyto poznámky pro bezpečnostní směrnice:

```
Určitě zdůraznit odhlášení od mateřské stanice, zákaznické služby
a detašované prodejní kanceláře. Zaměstnanci účtárny budou dávat pozor na systémovou jednotku.
```

Až vyplníte formulář fyzického zabezpečení, můžete začít plánovat zabezpečení aplikací.

Plánování zabezpečení aplikací

Chcete-li plánovat správné zabezpečení pro své aplikace, musíte znát odpovědi na tyto otázky:

- Jaké informace chcete v systému ukládat?
- Kdo k těmto informacím má mít přístup?
- Jaký druh přístupu lidé potřebují? Budou informace měnit nebo jim stačí pouze je prohlížet?

Při procházení těchto témat o plánování aplikací odpovíte na první otázku, jaké informace chcete v systému ukládat. V dalších tématech se rozhodnete, kdo tyto informace potřebuje a jaký druh přístupu mají lidé mít. Informace o plánování aplikací se nezadávají do systému, ale budete je potřebovat, až budete nastavovat zabezpečení uživatelů a zabezpečení prostředků.

Co je aplikace?

V prvním kroku plánování aplikací musíte popsat, které aplikace chcete v systému používat. Aplikace je skupina funkcí, které k sobě logicky náleží. Například ve společnosti JKL Toy Company jsou funkce pro zadávání objednávek, dodávky objednaného zboží a tisk faktur součástí aplikace Zpracování objednávek.

V systému iSeries můžete obvykle používat dva různé typy aplikací:

- **Komerční aplikace**: Aplikace, které zakoupíte nebo vyvinete tak, aby prováděly určité komerční funkce, například zpracování objednávek nebo správu skladových zásob.
- **Speciální aplikace**: Aplikace, které jsou používány po celé společnosti a které provádějí mnoho různých činností nesouvisejících s procesem podnikání.

Jaké formuláře použít?

Následující formuláře vám pomohou s plánováním zabezpečení aplikací:

- Formulář Popis aplikace.
- Formulář Popis knihovny.
- Formulář Konvence pojmenování.

Chcete-li některý z těchto formulářů vytisknout, klepněte na příslušný odkaz, vyberte správný rámec a potom klepněte na ikonu **Tisk** v prohlížeči.

Prostudujte si následující informace, pomohou vám při vyplňování plánovacích formulářů.

- Popis aplikací.
- Popis konvencí pojmenování.
- Popis informací o knihovnách.
- Nakreslení diagramu aplikací.

Popis aplikací

V tuto chvíli musíte shromáždit základní informace o každé z vašich komerčních aplikací. Doplňte informace o aplikaci do příslušného pole formuláře Popis aplikace podle níže uvedeného popisu. Později můžete tyto informace využít při plánování zabezpečení skupin uživatelů a zabezpečení aplikací.

Jméno a zkratka aplikace
: Dejte aplikaci stručné jméno a zkratku, kterou pak můžete používat jako značku aplikace ve formuláři a při pojmenování objektů, které aplikace používá.

Popisné informace
: Stručně popište činnost aplikace.

Primární menu a knihovna
: Určete, které menu je primární pro přístup do aplikace. Označte knihovnu, ve které je toto menu uloženo. Primární menu obvykle vede k dalším menu se specifickými funkcemi aplikace. Uživatelé rádi vidí primární menu své hlavní aplikace hned po přihlášení do systému.

Počáteční program a knihovny
: Aplikace někdy spouštějí počáteční program, který pro uživatele nastaví informace na pozadí nebo provádí kontrolu zabezpečení. Pokud má aplikace počáteční program nebo instalační program, zadejte ho do seznamu ve formuláři.

Knihovny aplikací
: Každá aplikace obvykle má pro své soubory hlavní knihovnu. Zahrnuje všechny knihovny, které aplikace používá, včetně knihoven programů a knihoven, které vlastní jiné aplikace. Například aplikace Zákaznické objednávky společnosti JKL Toy Company používá knihovnu skladových zásob a získává z ní zůstatky a popisy položek.

  Ze vztahů mezi knihovnami a aplikacemi můžete pro každou knihovnu určit, kdo k ní má mít přístup.

Vyhledání informací o aplikacích

Další potřebné informace o aplikacích můžete získat od programátorů, kteří je vytvořili, nebo od dodavatelů aplikací.

Nemáte-li k informacím o některé aplikaci v systému přístup, můžete tyto informace shromáždit sami některým z níže uvedených způsobů.

- Uživatelé aplikace vám pravděpodobně sdělí jméno primárního menu a knihovny, nebo je můžete pozorovat při přihlašování do systému.
- Jakmile se po přihlášení uživatelů zobrazí na obrazovce aplikace, prohlédněte si pole **Počáteční program** v jejich uživatelském profilu. Toto pole obsahuje počáteční program aplikace. Pomocí příkazu DSPUSRPRF ho můžete ho prohlížet.
- Můžete procházet seznamem všech knihoven v systému, který zahrnuje jména i popisy knihoven. Použijte příkaz DSPOBJD *ALL *LIB. Zobrazí všechny knihovny v systému.

- Můžete pozorovat aktivní úlohy, když uživatelé spouštějí aplikaci. Pomocí příkazu WRKACTJOB (Práce s aktivními úlohami) se střední úrovní asistence můžete získat podrobné informace o interaktivních úlohách. Zobrazte úlohy a prohlédněte si seznam zamčených knihoven i seznam jejich zamčených objektů. Zjistíte tak, které knihovny jsou právě používány.
- Pomocí příkazu WRKUSRJOB (Práce s uživatelskými úlohami) můžete zobrazit dávkové úlohy v aplikaci.

Chcete-li mít jistotu, že jste shromáždili veškeré informace potřebné pro plánování zabezpečení aplikace, měli byste následující úkoly provést ještě předtím, než budete pokračovat:

- Pro každou komerční aplikaci vyplňte formulář Popis aplikace. Vyplňte celý formulář kromě části Požadavky na zabezpečení. Tuto sekci vyplníte, až budete pro aplikaci plánovat zabezpečení prostředků podle popisu v tématu Plánování zabezpečení prostředků.
- Připravte formulář Popis aplikace pro každou aplikaci, pokud je to možné. Použití formuláře vám pomůže určit, jak máte poskytovat přístup k aplikaci.

Poznámka: Příprava formuláře Popis aplikace pro speciální aplikace od IBM, jako je např. IBM Query for iSeries, není nutná. Přístup ke knihovnám používaným těmito aplikacemi nevyžaduje žádné zvláštní plánování. Sběr informací a příprava formulářů však mohou být užitečné.

Možná budete chtít prostudovat příklad formuláře Popis aplikace společnosti JKL Toy Company ještě předtím, než začnete s popisem konvencí pojmenování.

Příklad: Formulář společnosti JKL Toy Company: Popis aplikace: Sharon Jonesová sestavila seznam všech aplikací společností a napsala jejich zkratky do formuláře Popis aplikace. Dále stručně popsala, jak uživatelé s těmito aplikacemi pracují.

Zákaznické objednávky (CO)
Zadávání, sledování a odesílání objednávek. Tisk faktur.

Řízení zásob (IC)
Správa úrovní zásob pro hotové výrobky i pro materiál. Zpracování pohybu zásob.

Smlouvy a ceníky (CP)
Správa zvláštních ceníků a smluv se zákazníky.

Pohledávky (AC)
Sledování aktuálních bilancí. Tisk měsíčních přehledů.

Níže uvedená tabulka obsahuje popis, který Sharon Jonesová vytvořila pro aplikaci Zákaznické objednávky. Připravila tento formulář systematicky - začala s jednou aplikací a potom popsala ostatní.

Tabulka 6. Příklad: Formulář společnosti JKL Toy Company: Popis aplikace

Formulář Popis aplikace	
Zhotovila: Sharon Jonesová	Datum: 9/3/99
Název aplikace: Zákaznické objednávky	Zkratka: CO
Stručný popis aplikace:	Zadávání, vyhledávání a odesílání objednávek, tisk faktur a expedičních dokladů.
Jméno primárního menu: COMAIN	Knihovna: COPGMLIB
Jméno počátečního programu: NA	Knihovna: NA
Uveďte seznam knihoven, které aplikace používá pro soubory a programy: • CUSTLIB • ITEMLIB • CONTRACTS • COPGMLIB	

Tabulka 6. Příklad: Formulář společnosti JKL Toy Company: Popis aplikace (pokračování)

Definujte pro aplikace cíle v oblasti zabezpečení, jako například to, zda jsou některé informace důvěrné.	

Kromě aplikace Zákaznické objednávky připravila Sharon Jonesová také formuláře Popis aplikace pro následující aplikace v systému společnosti JKL Toy Company:

- Řízení zásob.
- Smlouvy a ceníky.
- Pohledávky.

Jako další krok můžete popsat konvence pojmenování pro objekty ve vašem systému.

Popis konvencí pojmenování

Když víte, jak systém vytváří jména objektů, můžete plánovat a monitorovat zabezpečení, řešit problémy a plánovat zálohování a obnovu. Většina aplikací má pravidla pro přiřazování jmen k objektům, například ke knihovnám, souborům a programům. Pokud vaše aplikace pocházejí z různých zdrojů, může mít každý z nich svůj vlastní jedinečný systém pojmenování.

Zajistěte, aby všechny konvence pojmenování aplikací a objektů byly zaznamenány do formuláře Konvence pojmenování. Do tohoto formuláře zapište pravidla, která aplikace používají při vytváření jmen knihoven a objektů. Prázdné řádky můžete použít pro další konvence pojmenování, například pro programy a menu. Pokud vaše aplikace pochází z různých zdrojů, může mít každý z nich vlastní jedinečné konvence pojmenování. Popište konvence pojmenování pro každou aplikaci. Možná budete potřebovat více než jeden formulář Konvence pojmenování.

Možná budete chtít prostudovat příklad, který uvádí, jaké konvence použila paní Sharon Jonesová při pojmenování objektů v systému společnosti JKL Toy Company ještě předtím, než začnete s popisem informací o knihovnách.

Příklad: Formulář společnosti JKL Toy Company: Konvence pojmenování: Níže uvedená tabulka zobrazuje konvence pojmenování pouze pro knihovny a soubory. Budete muset popsat také konvence pojmenování pro ostatní typy objektů v systému. Formulář Konvence pojmenování obsahuje několik běžných objektů. Můžete však mít i jiné objekty, které si budete muset připravit.

Tabulka 7. Příklad: Formulář společnosti JKL Toy Company: Konvence pojmenování

Formulář Konvence pojmenování	
Zhotovila: Sharon Jonesová	Datum: 9/3/99
Typ objektu	**Konvence pojmenování**
Knihovny	Knihovny obsahující soubory mají smysluplná jména jako CONTRACTS nebo ITEMLIB. Knihovny programů používají zkratky aplikací, po kterých následuje PGMLIB, například CPGMLIB.
Soubory	Většina souborů má smysluplná jména, například CUSTMAST pro hlavní soubor se záznamy zákazníků (Customer Master) nebo ITEMMAST pro hlavní soubor položek (Item Master). Ostatní aplikační soubory (používané z důvodů, kterým rozumí pouze programátoři) jsou pojmenovány zkratkami aplikací, po kterých následuje FILE a číslo, například ICFILE14.

Jakmile dokončíte formulář Konvence pojmenování, můžete začít pracovat na informacích popisujících knihovny..

Popis informací o knihovnách

Až dokončíte popis konvencí pojmenování, měli byste popsat knihovny v systému. Knihovny identifikují a organizují objekty v systému. Umístíte-li podobné soubory společně do jedné knihovny, umožníte uživatelům snadný přístup k nejdůležitějším informacím a souborům. Můžete také přizpůsobit uživatelská oprávnění tak, aby měli uživatelé přístup k některým knihovnám, ale k jiným ne. Pro každou aplikaci popište všechny knihovny, které jsou v systému. Možná budete potřebovat více než jeden formulář Popis knihovny

Poznámka: Vyplňte pouze popisné informace o knihovně. Až budete pro knihovny plánovat zabezpečení prostředků, vyplníte zbytek formuláře Popis knihovny. Informace o oprávněních ke knihovnám budete muset doplnit později. Podrobné informace o vyplnění zbytku formuláře Popis knihovny najdete v tématu Plánování zabezpečení pro knihovny aplikací.

Než budete pokračovat, zajistěte, aby byly vyplněny následující údaje:

- části o knihovnách a souborech ve formuláři Konvence pojmenování
- popisné informace pro každou knihovnu ve formuláři Popis knihovny

Možná budete chtít prostudovat příklad, jak paní Sharon Jonesová ze společnosti JKL Toy Company popsala knihovny, ještě předtím, než začnete kreslit diagram aplikace.

Příklad: Formulář společnosti JKL Toy Company: Popis knihovny: Dvě níže uvedené tabulky popisují dvě knihovny, které ve společnosti JKL Toy Company používá aplikace Zákaznické objednávky. První tabulka popisuje knihovnu obsahující soubory, druhá tabulka popisuje knihovnu obsahující programy.

Tabulka 8. Příklad: Formulář společnosti JKL Toy Company: Popis knihovny - knihovna obsahující soubory

Formulář Popis knihovny	
Zhotovila: Sharon Jonesová	Datum: 9/3/99
Jméno knihovny: CUSTLIB	Popisné jméno (text): Knihovna záznamů o zákaznících
Stručně popište funkci této knihovny:	Obsahuje veškeré soubory zákazníků včetně objednávek a pohledávek.

Tabulka 9. Příklad: Formulář společnosti JKL Toy Company: Popis knihovny - knihovna obsahující programy

Formulář Popis knihovny	
Zhotovila: Sharon Jonesová	Datum: 9/3/99
Jméno knihovny: COPGMLIB	Popisné jméno (text): Knihovna programů pro Zákaznické objednávky
Stručně popište funkci této knihovny:	Obsahuje veškeré programy pro aplikaci Zákaznické objednávky.

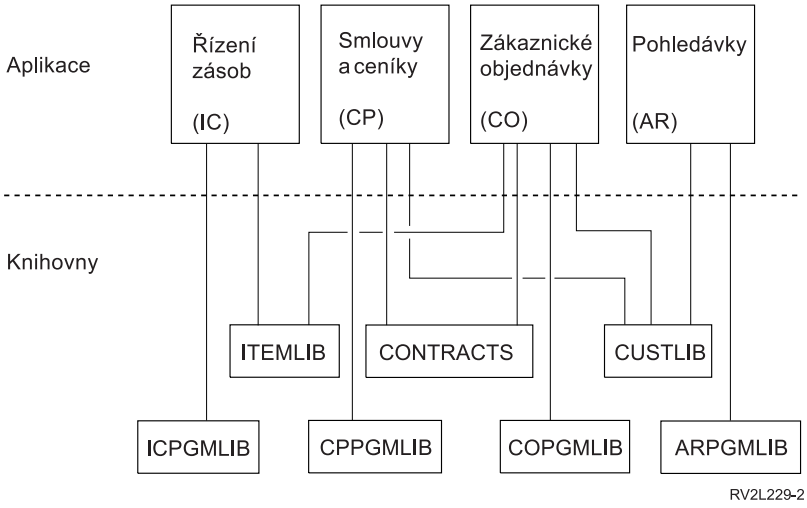
Jakmile popíšete knihovny, měli byste nakreslit diagram aplikací pro váš systém.

Nakreslení diagramu aplikací

Při přípravě formulářů Popis aplikace a Popis knihovny možná zjistíte, že by bylo užitečné nakreslit diagram znázorňující vztahy mezi aplikacemi a knihovnami. Diagram vám pomůže s plánováním zabezpečení skupin uživatelů i zabezpečení prostředků.

Níže uvedený obrázek ukazuje diagram, do kterého paní Sharon Jonesová nakreslila aplikace a knihovny společnosti JKL Toy Company:

Diagram aplikací a knihoven společnosti JKL Toy Company



Shromažďování některých informací o aplikacích a knihovnách vám pomůže při rozhodování o zabezpečení. Berte to jako příležitost k získání dalších znalostí o systému a aplikacích.

Chcete-li mít jistotu, že jste shromáždili potřebné informace o aplikacích, měli byste provést následující akce:
- Vyplnit formulář Popis aplikace pro každou komerční aplikaci v systému.
- Připravit formulář Popis aplikace pro každou aplikaci v systému.
- Vyplnit části pro knihovny a soubory ve formuláři Konvence pojmenování.
- Připravit formulář Popis knihovny pro každou knihovnu aplikací.
- Nakreslit diagram vztahů mezi aplikacemi a knihovnami.

Až dokončíte vyplňování těchto formulářů, můžete začít s plánováním celkové strategie zabezpečení.

Plánování celkové strategie zabezpečení

Poté, co jste si promysleli plánování zabezpečení aplikací, jste připraveni začít s přípravou celkové strategie zabezpečení. Nejprve je zapotřebí stanovit celkovou koncepci zabezpečení systému. Při rozhodování uvažujte o potřebách vašeho podniku v současnosti a budoucnosti.

Tyto poznatky vám pomohou v procesu plánování zásad a cílů v oblasti zabezpečení. Tyto informace můžete také využít při volbě nastavení základních systémových hodnot, které ovlivňují všechny uživatele systému.

Jaké formuláře použít?

Proces plánování ukončete vyplněním formuláře Výběr systémových hodnot..

Vyplněné formuláře Plánování fyzického zabezpečení a Popis aplikace budete potřebovat při studování témat, která vám pomohou při nastavení systémových hodnot.

Prostudujte tato témata týkající se plánování zásad zabezpečení systému.
- Vypracování zásad zabezpečení.
- Výběr úrovně zabezpečení.
- Výběr systémových hodnot ovlivňujících přihlášení.
- Výběr systémových hodnot ovlivňujících hesla.
- Přizpůsobení systému pomocí systémových hodnot.

Vypracování zásad zabezpečení

Než začnete s plánováním, připravte prohlášení o strategii zabezpečení vašeho podniku s ohledem na bezpečnost vašeho systému. Toto prohlášení o strategii zabezpečení bude dohodou mezi vámi a vedením vašeho podniku. Pomůže vám rozhodnout, co je důležité. Strategie zabezpečení by by měla stanovit, jaká bude celková koncepce zabezpečení a určit, která informační aktiva vyžadují ochranu.

Každý systém by měl být chráněn. Můžete přijmout jednu z těchto koncepcí zabezpečení:

- **Přísná**: Někteří lidé tomu říkají schéma zabezpečení typu need-to-knew (potřeba vědět). V prostředí s přísným zabezpečením mají uživatelé přístup pouze k těm informacím a funkcím, které potřebují ke své práci. Cokoliv jiného je vyloučeno. Mnoho auditorů doporučuje přísnou koncepci.
- **Průměrná**: Průměrná koncepce zabezpečení umožňuje uživatelům přístup k objektům založený na oprávněních, která jsou jim přidělena.
- **Volná**: V prostředí s volným zabezpečením mají uživatelé umožněn přístup k většině objektů v systému. Přístup se obvykle omezuje v případě určitých kritických nebo důvěrných objektů. Samostatná oddělení nebo malé podniky používají obvykle volnou koncepci zabezpečení svých systémů.

Celková koncepce vám pomůže rozhodnout o vašich specifických potřebách zabezpečení. Koncepce zabezpečení vašeho systému by měla odpovídat filosofii pro přístup k informacím v celém vašem podniku. Jestliže si nejste jisti, kterou koncepci zvolit, zkuste tento postup:

- Použije vyplněný formulář Popis aplikace a rozhodněte, kdo smí nebo nesmí mít přístup k těmto aplikacím.
- Prozkoumejte technologie používané ve vašem podniku. Pokud například plánujete připojení vašeho systému k Internetu, budete potřebovat mnohem přísnější zabezpečení na ochranu systému před vnějšími uživateli Internetu.
- Promluvte s ostatními členy vašeho podniku, například s auditory zabezpečení, abyste lépe určili potřeby zabezpečení.

Pamatujte na to, že můžete zásady zabezpečení nestále měnit. V mnoha podnicích, které se rozrůstají, zjišťují, že potřebují přísnější zabezpečení. Uvedené informace vám pomohou nastavit bezpečnostní schéma, které umožní zpřísnit bezpečnost později, aniž byste museli provádět množství změn a testů všech aplikací.

Co chránit

Kromě stanovení celkové koncepce pro strategii zabezpečení potřebujete určit, která informační aktiva v rámci vašeho podniku jsou kritická (životně důležitá). Bezpečnostní systém má být navržen tak, aby tyto informace chránil. Následující doporučení vám pomohou tato kritická aktiva stanovit.

- **Důvěrnost**: Informace, které nejsou všeobecně přístupné lidem ve vašem podniku. Příkladem důvěrných informací jsou mzdy.
- **Konkurenceschopnost**: Informace, které vám dávají konkurenční výhodu, například specifikace produktů a jejich výrobní předpisy.
- **Činnosti**: Informace ve vašem počítači, které jsou nepostradatelné pro denní činnosti ve vašem podniku, jako například záznamy o zákaznících nebo bilance zásob.

Sharon Jonesová, správce systému, a John Smith, ředitel společnosti, připravují společně prohlášení o strategii zabezpečení. John Smith používá zmíněné poznámky k návrhu zásad zabezpečení pro JKL Toy Company. Můžete prostudovat návrh zásad zabezpečení, který společnost JKL Toy Company poslala všem svým zaměstnancům poté, co bylo dokončeno plánování a nastavení zásad zabezpečení. Při práci na těchto koncepčních návrzích si nezapomeňte poznamenat, co byste chtěli přidat do vašich zásad zabezpečení.

Tabulka 10. Příklad: Zásady zabezpečení společnosti JKL Toy Company

Celková koncepce Uvolněná: Většina lidí potřebuje mít přístup k většině informací.
Kritické informace • Smlouvy a ceníky • Mzdy • Záznamy o zákaznících a zásobách jsou přístupné pouze zaměstnancům podniku.
Všeobecná pravidla • Každý uživatel systému bude mít uživatelský profil. Uživatel nesmí sdílet svůj profil nebo heslo. • Uživatel si musí změnit heslo každých 60 dní.

Poté, co jste si udělali poznámky týkající se zásad zabezpečení, můžete provést Výběr úrovně zabezpečení.

Výběr úrovně zabezpečení

Systémová hodnota QSECURITY vám umožní kontrolovat míru zabezpečení podle vašich požadavků. Abyste porozuměli, jak fungují úrovně zabezpečení, představte si váš systém jako budovu, do které se lidé pokoušejí vstoupit.

Úroveň 20: Zabezpečení heslem

Jestliže zvolíte úroveň 20, máte jakousi ochranu bezpečnosti. Stráž u dveří do budovy vás požádá o vaši identifikaci a tajné heslo. Dovnitř jsou vpuštění pouze lidé, kteří mají obojí. Avšak jakmile je někdo uvnitř, může jít kamkoliv a dělat co se mu zlíbí.

Jestliže někdo odposlechne tajné heslo a použije je k tomu, aby prošel přes stráž u dveří, pak nebudete mít žádnou ochranu.

Úroveň 30: Zabezpečení heslem a zabezpečení objektů

Úroveň 30 vám umožňuje totéž, jako úroveň 20, navíc však můžete kontrolovat, kdo smí vstoupit do určité části budovy a co tam smí dělat. Můžete označit některé části budovy jako veřejné, zatímco vstup do jiných bude vyhrazen a hlídán stráží.

Můžete určit, kteří lidé budou mít povolen přístup do vyhrazených sekcí budovy a budou tam smět dělat cokoliv, nebo můžete vyžadovat, aby vznesli požadavek na informace oprávněným informačním úředníkům (programům). Vetřelec, který vstoupí do budovy a použije přitom heslo někoho jiného, by musel do chráněných sekcí projít ještě přes vnitřní stráže.

Úroveň 40: Ochrana integrity

Na úrovní 40, získáte veškerou ochranu úrovně 30, avšak systém navíc ověřuje přístup uživatelů. Stráž u dveří uvnitř budovy kontroluje hesla a zapisuje do protokolu všechny uživatele, kteří vstoupí do místnosti.

Úroveň 50: Ochrana rozšířené integrity

Na úrovni 50 stráž prosazuje ještě přísnější sadu pravidel, aby zabránila vstupu osobám se speciálními znalostmi, jak projít hlídanými dveřmi, a to tak, že ověřuje identitu každé osoby, která podepíše protokol.

Doporučení

Systém iSeries se dodává se zabezpečením úrovně 40. Úroveň zabezpečení 40 je nejvýhodnější pro většinu instalací, ať už je strategie zabezpečení přísná, průměrná nebo volná. Jestliže zvolíte volnější koncepci, můžete nastavit veřejný přístup k většině prostředků vašeho systému. Použití úrovně zabezpečení 40 od samého začátku vám dává dostatečnou flexibilitu k pozdějšímu přísnějšímu zabezpečení systému bez velkých změn.

Při nákupu aplikačních programů si ověřte u dodavatele, zda byly programy otestovány při úrovni zabezpečení 40. Některé aplikace provádějí operace, které způsobují chyby při úrovni zabezpečení 40. Jestliže aplikace nebyly

testovány při úrovni 40 nebo 50, spusťte je při úrovni 30. Použijte žurnál monitorování, abyste zjistili chyby aplikací způsobené přihlašovacími oprávněními protokolu aplikací. Nevyskytnou-li se žádné chyby, můžete změnit úroveň na 40 nebo 50.

Úroveň zabezpečení 50 chrání před událostmi, které se obvykle u většiny systémů nevyskytují. Systém provede další dodatečnou kontrolu, kdykoliv v systému běží nějaké programy. Tato dodatečná kontrola může mít negativní dopad na výkon systému.

Poté, co ve formuláři Výběr systémových hodnot zadáte volbu úrovně zabezpečení, můžete provést výběr systémových hodnot ovlivňujících přihlášení do systému.

Výběr systémových hodnot ovlivňujících přihlášení do systému

Poté, co provedete volbu systémové úrovně, můžete pomocí systémových hodnot nastavit, co uživatelé uvidí na svých obrazovkách a jak budou se systémem komunikovat. Bude zapotřebí naplánovat tyto systémové hodnoty a zapsat volby do formuláře Výběr systémových hodnot.

Následující tabulka popisuje systémové hodnoty z tohoto tématu.

Tabulka 11. Systémové hodnoty iSeries a jejich popis

Systémová hodnota	Popis
QMAXSIGN	Omezuje počet za sebou jdoucích pokusů o přihlášení.
QMAXSGNACN	Definuje akci, kterou systém provede, jestliže je dosaženo určitého počtu po sobě jdoucích pokusů o přihlášení.
QLMTDEVSSN	Určuje, jestli se uživatel může přihlásit k více než jedné pracovní stanici pod stejným uživatelským profilem.
QINACTITV	Určuje, kdy systém provede nějakou akci u neaktivní úlohy.
QINACTMSGQ	Určuje, jakou akci systém provede, když je interaktivní úloha nečinná po dobu, kterou udává systémová hodnota QINACTITV.
QDSCJOBITV	Řídí, jestli a kdy systém ukončí úlohu, která byla dočasně odpojena.
QLMTSECOFR	Omezuje správce systému, který má oprávnění ke všem objektům v systému, na konkrétní zařízení.

Omezení počtu pokusů o přihlášení do systému (QMAXSIGN a QMAXSGNACN): Počet pokusů o přihlášení do systému a akce, kterou systém provede, když je dosaženo limitu, určují dvě systémové hodnoty.

Systémová hodnota QMXSIGN (maximální počet pokusů o přihlášení) omezuje maximální počet po sobě jdoucích nesprávných pokusů o přihlášení, které systém povolí, než provede nějakou akci. Chybným pokusem o přihlášení se rozumí, když se někdo pokusí použít konkrétní uživatelský profil zadáním chybného hesla nebo když má nedostatečná přístupová práva k pracovní stanici.

Systémová hodnota QMAXSGNACN určuje, co má systém udělat, když se někdo pokouší přihlásit příliš mnohokrát za sebou. Možné hodnoty jsou:

1 Zamezit jakýmkoliv dalším pokusům o přihlášení k zařízení. To je tzv. zablokování zařízení. K zařízení se nemůže nikdo přihlásit, dokud nějaká oprávněná osoba opět nepovolí toto zařízení pomocí příkazu WRKCFGSTS. Tento způsob ochrany je většinou nedostatečný, obzvlášť když jsou pokusy o přihlášení do systému činěny z osobního počítače nebo ze vzdáleného systému.

Systémový operátor nebo kdokoliv s oprávněním typu *USE k tomuto zařízení může zařízení znovu zpřístupnit.

2 Zakázání jakýchkoliv dalších pokusů o přihlášení pro daný uživatelský profil. To je tzv. zablokování

uživatelského profilu. K tomuto profilu se nikdo nemůže přihlásit, dokud nějaká oprávněná osoba opět nepovolí tento uživatelský profil pomocí příkazu CHGUSRPRF (Změna uživatelského profilu).

Povolení tohoto profilu (změnu stavu) smí provést administrátor systému s oprávněním k používání tohoto profilu.

3 Zablokování jak uživatelského profilu, tak zařízení.

Rizika a doporučení

Někteří škůdci se baví pokusy o uhodnutí hesla a proniknutí do systému. Omezením počtu povolených pokusů o přihlášení omezíte jejich možnosti.

Systémová hodnota QMAXSIGN (Maximální počet neúspěšných přihlášení) určuje, kolik pokusů o přihlášení máte povoleno. Nastavte ji dostatečně vysoko, abyste se vyvarovali frustrace uživatelů. Nastavte ji dostatečně nízkou, abyste odradili uživatele od bezstarostného zadávání, a nedávali tak prostor potenciálním škůdcům k mnoha pokusům. Měli byste nastavit tuto hodnotu pro maximální počet pokusů o přihlášení mezi 3 a 5.

Doporučená maximální hodnota pro QMAXSGNACN (Maximální počet akcí přihlášení) rovná se 3, i když zablokování zařízení nebo uživatelského profilu může uživatele obtěžovat. Pracovní stanice umístěná v soukromí poskytuje vetřelci příležitost, aby vyzkoušel mnoho různých uživatelských profilů a mnoho kombinací hesel. Jestliže váš systém nemá žádné pracovní stanice, které jsou rizikové z důvodu jejich umístění, pak zablokování uživatelského profilu bude patrně dostatečnou ochranou.

Zkontrolujte vyplněný formulář Fyzické zabezpečení. Jestliže máte pracovní stanice na vzdáleném místě nebo máte vzdálené uživatele (uživatele, kteří se připojují k systému pomocí telefonní linky nebo přes VPN, pak bude zapotřebí omezit možnosti připojení přísněji. Ujistěte se, že jste přidali volby pro hodnoty QMAXSIGN a QMAXSGNACN v části 2 formuláře Výběr systémových hodnot.

Bude jistě užitečné, když si prohlédnete příklad který ukazuje, jak tyto systémové hodnoty spolupracují při omezení pokusů o přihlášení dříve, než přistoupíte k tématu Výběr systémových hodnot omezujících uživatele na používání jedné pracovní stanice v daný okamžik.

Příklad: Omezení počtu pokusů o přihlášení: Sharon Jonesová omezila počet pokusů o přihlášení na 3 (QMAXSIGN rovná se 3) a zvolila zablokování jak profilu, tak zařízení, jestliže bude limit překročen (QMAXSGNACN rovná se 3). Co se stane, když je těchto hodnot dosaženo:

1. Roger zadal nesprávné heslo již dvakrát za sebou.
2. Po druhém nesprávném pokusu obdrží varovnou zprávu že další chybný pokus zablokuje uživatelský profil.
3. Roger se znovu spletl.
4. Systém zablokoval jeho uživatelský profil a pracovní stanice již nezobrazí obrazovku Přihlášení. Jestliže se Roger pokusí přihlásit z jiné pracovní stanice, dostane chybovou zprávu.
5. Nyní potřebuje požádat Sharon o povolení uživatelského profilu, aby to mohl znovu zkusit. Sharon nebo operátor systému tedy musí Rogerův profil zpřístupnit. Jestliže si Roger nevzpomene na své heslo, může mu Sharon přidělit dočasné heslo, které si Roger po novém přihlášení musí změnit.

Nyní si můžete prohlédnout systémové hodnoty, které omezí uživatele k používání jedné pracovní stanice v daném okamžiku.

Omezení uživatelů na používání jedné pracovní stanice v daném okamžiku: Systémová hodnota QLMTDEVSSN (Omezit relace zařízení) určuje, zda smí být tentýž uživatel přihlášen ve stejném okamžiku na více než jedné pracovní stanici. Možné hodnoty jsou:

0 Systém povolí přihlášení neomezeného počtu uživatelů ve stejný časový okamžik k témuž uživatelskému profilu.

1 Uživatelský profil smí používat v daný okamžik pouze jeden uživatel. Uživatel smí mít více než jednu relaci na stejném zařízení.

Rizika a doporučení

Povolit uživatelům, aby se směli ve stejný okamžik přihlásit pouze k jedné pracovní stanici podporuje dobré bezpečnostní návyky. Volnější bezpečnostní návyky představují bezpečnostní riziko.

- Omezením uživatelů k používání pouze jednoho zařízení je odradíte od vzájemného sdílení ID uživatele a hesla. Jestliže lidé sdílejí své ID uživatele, ztrácíte kontrolu nad uživatelskými účty. Ve skutečnosti pak nevíte, kdo jakou funkci v systému používá.
- Lidé si musí navyknout odhlásit se při opuštění pracovní stanice, ještě než začnou používat jinou. Opuštěná pracovní stanice, od které se uživatel neodhlásil, představuje bezpečnostní riziko.

Doporučené nastavení pro systémovou hodnotu QLMTDEVSSN je 1, což omezuje uživatele na používání jediného zařízení. Přidělte každému uživateli systému jedinečný ID uživatele ID a jedinečné heslo s příslušnými oprávněními a pak jej omezte na používání jediné pracovní stanice. Ujistěte se, že jste zadali svou volbu pro QLMTDEVSSN v části 2 formuláře Výběr systémových hodnot.

Potom můžete začít s plánováním systémových hodnot pro neaktivní úlohy.

Plánování systémových hodnot pro neaktivní úlohy: Jakou akci systém provede, když se uživatel zapomene odhlásit z pracovní stanice, určují tři systémové hodnoty.

QINACTITV (Časový interval nečinnosti úlohy)
Systémová hodnota QINACTITV určuje, zda systém provede nějakou akci, jestliže stanice byla přihlášena, ale je neaktivní po určitý časový úsek.

Poznámka: **Neaktivní** znamená, že uživatel nestiskl klávesu Enter nebo funkční klávesu po určitý časový interval.

QINACTMSGQ (Fronta zpráv neaktivní úlohy)
Nastavení systémové hodnoty QINACTMSGQ určuje, co systém provede, když vyprší časový limit, určený systémovou hodnotou QINACTITV. Jestliže zvolíte ENDJOB, systém ukončí každou úlohu, která bude neaktivní déle, než je interval nečinnosti, který jste zvolili pro QINACTITV. Zvolíte-li DSCJOB, systém odpojí neaktivní úlohu. Jestliže zadáte název fronty zpráv, server pošle do této fronty varovnou zprávu, že úloha je příliš dlouho neaktivní.

Když systém **odpojí** úlohu na pracovní stanici, tak tuto úlohu zároveň dočasně pozastaví. Na pracovní stanici se objeví obrazovka Přihlášení. Odpojená úloha bude pokračovat, když se tentýž uživatel znovu přihlásí k pracovní stanici.

QDSCJOBITV (Časový interval odpojené úlohy)
Systémová hodnota QDSCJOBITV určuje, jestli a kdy systém ukončí úlohu, která byla dočasně odpojena. Systém může automaticky odpojit úlohy na základě vyhodnocení systémových hodnot QINACTITV a QINACTMSGQ. Uživatelé mohou také požadovat, aby jejich úlohy byly dočasně odhlášeny (pozastaveny) pomocí volby v menu Provozního asistenta nebo použitím příkazu DSCJOB (Odpojení úlohy).

Rizika a doporučení

Jestliže se Sharon před svým odchodem zapomene odhlásit od pracovní stanice, může John přijít k pracovní stanici a provést libovolné činnosti, které má Sharon v systému povoleny.

Neaktivní obrazovky byste měli omezit zejména ze dvou důvodů:

- Jestliže máte přísně zabezpečené prostředí s důvěrnými informacemi, uloženými v systému.
- Jestliže máte pracovní stanice umístěny na místech, odkud k nim mohou snadno přistupovat lidé, kteří nejsou z vašeho podniku.

Běžné pracovní povinnosti často odvolají uživatele od jejich pracovních stanic. Výhodou použití všech těchto tří systémových hodnot je, že umožňuje běžné přerušení činnost, a přitom stále chrání bezpečnost vašeho systému.

K tomu, abyste vyloučili uvedená rizika, doporučuje IBM používat systémové hodnoty QINACTITV, QINACTMSGQ a QDSCJOBITV společně, což umožní běžná pracovní přerušení činnosti a přitom stálou ochranu bezpečnosti systému.

QINACTITV (Časový interval nečinnosti úlohy): Nastavte tento interval dostatečně krátký, abyste odradili uživatele od opuštění stanice bez jejího obsloužení, ale ne tak krátký, aby je obtěžoval. Doporučené nastavení je 30 minut. Jestliže úloha byla 30 minut neaktivní, systém provede akci specifikovanou ve frontě zpráv neaktivní úlohy.

QINACTMSGQ (Fronta zpráv neaktivní úlohy): Zvolte Odpojit úlohu. Systém odpojí všechny úlohy, které byly neaktivní po časový úsek, určený hodnotou Časový interval nečinnosti úlohy. Systém pozastaví úlohu a odhlásí stanici. Jestliže se tentýž uživatel znovu přihlásí, úloha bude pokračovat tam, kde byla opuštěna.

To je pro uživatele příjemnější, protože systém raději pozastaví jejich práci, než aby ji přerušil. Odpojení neaktivní úlohy poskytuje stejně dobrou ochranu systému, jako její ukončení.

Poznámka: Některé úlohy systém nemůže odpojit. Jestliže systém nemůže odpojit neaktivní úlohu, úlohu ukončí. To může způsobit ztrátu informací. Zvažte nastavení QINACTMSGQ k zasílání zpráv do fronty zpráv operátora systému.

QDSCJOBITV (Časový interval odpojení úlohy): Povzbuďte uživatele, aby se dočasně odhlásili od systému, když se potřebují krátce vzdálit a poté dodělat svou práci, a aby se trvale odhlásili při delším přerušení práce.

Ještě než systém spustí noční zpracování, například automatické vyčištění, ukončete pomocí příkazu QDSCJOBITV všechny odpojené programy. Interval nastavte dostatečně dlouhý, aby se uživatelé mohli během pracovního dne vrátit k pracovní stanici, avšak dostatečně krátký, aby úlohy skončily ještě před zahájením nočního zpracování. Zvolte 300 minut (pět hodin), což poskytuje nočnímu zpracování dostatek času, aby včas skončilo, aniž by rušilo práci uživatelů.

Poznámka: Aby se zabránilo případu, kdy se dva uživatelé pokoušejí změnit tutéž informaci, systém **zamkne** záznam před jeho aktualizací. Všechny zámky v prostředcích zůstávají nastaveny, i když systém odpojí úlohu. V závislosti na struktuře aplikace a počtu uživatelů systému mohou být zámky příčinou snížení výkonu systému. Ověřte si u programátora nebo dodavatele aplikace, zda má zamykání záznamů dopad na výkon systému.

Prostudujte si příklad, abyste viděli, jak tyto tři systémové hodnoty spolupracují při manipulaci s neaktivními úlohami v systému.

Poté, co zaznamenáte své rozhodnutí týkající se neaktivních úloh do formuláře Výběr systémových hodnot, můžete se rozhodnout pro omezení, kam se smí přihlásit správce systému.

Příklad: Zpracování neaktivních úloh se systémovými hodnotami QINACTITV, QINACTMSGQ a QDSCJOBITV:
Předpokládejme, že jste nastavili interval prodlevy neaktivní úlohy (QINACTITV) na 30 minut. Systém odpojí neaktivní úlohy (QINACTMSGQ je DSCJOB). Interval prodlevy odpojené úlohy (QDSCJOBITV) je 300 minut (5 hodin). Pokud se například Sharon zapomene odhlásit v 9:30 hod., systém odpojí její úlohu v 10:00 hod. a ukončí úlohu v 15:00 hod.

Zadejte velikost systémových hodnot QINACTITV, QINACTMSGQ a QDSCJOBITV v části 2 formuláře Výběr systémových hodnot.

Jakmile ve formuláři Výběr systémových hodnot zaznamenáte svá rozhodnutí pro neaktivní úlohy, můžete se rozhodnout, jak omezit, kde se může správce systému přihlásit do systému.

Omezení, kam se smí přihlásit správce systému: Možná si budete přát omezit uživatele, kteří mají oprávnění měnit zabezpečení a kontrolovat objekty, jen na určité stanice. To zabrání těmto uživatelům přihlásit se k pracovní stanici na vzdáleném místě, aniž by znali vaše přihlášení. Systémová hodnota QLMTSECOFR (omezení správce systému) vám to umožní. Jestliže nastavíte QLMTSECOFR na 1, pak uživatelé s oprávněním *ALLOBJ nebo *SERVICE se mohou přihlásit pouze ke konzoli, nebo k pracovní stanici, kterou jim přidělíte.

QLMTSECOFR omezí správce systému, uživatele s právem na všechny objekty v systému a operátory. Jestliže chcete těmto uživatelům přidělit uživatelský přístup k jinému zařízení, použijte příkaz příkaz GRTOBJAUT (Udělení oprávnění k objektu).

Poznámka: Aby bylo možno použít systémovou hodnotu QLMTSECOFR, musí být úroveň zabezpečení systému 30 nebo vyšší.

Rizika a doporučení

Systémovou hodnotu QLMTSECOFR byste měli nastavit na 1. Jestliže někdo vyslechne nebo uhodne heslo někoho s oprávněním správce systému, musí také získat přístup k zařízení, které mu umožní se přihlásit.

Po zadání voleb pro QLMTSECOFR v části 2 formuláře Výběr systémových hodnot můžete vybrat systémové hodnoty ovlivňující hesla.

Výběr systémových hodnot ovlivňujících hesla

Měli byste raději umožnit uživatelům volit si svá vlastní hesla, než aby jim hesla přiděloval správce systému. Když si uživatel vytvoří heslo, obvykle si je nepotřebuje nikam zapsat. Hesla, která si uživatel zapíše, bývají umístěna na obvyklých místech, což představuje bezpečnostní riziko.

Tip pro tvorbu hesla

Uživatelé mívají potíže s vymýšlením dobrého hesla. Doporučte jim tuto techniku: Použijte větu, která se snadno zapamatuje, jako pomoc při vytvoření těžko uhodnutelného hesla. Například po dovolené můžete použít větu ″Dne 4. června byl chabý úlovek″ k vytvoření hesla D4CBCU.

Některé systémové hodnoty ovlivňují hesla. Můžete nařídit, jak často si uživatelé mají měnit svá hasla. Můžete také vytvořit mnoho pravidel, abyste zamezili používání hesel, která se dají snadno uhodnout. Mnohé tyto systémové hodnoty jsou důležité pro velké organizace. Některé jsou důležité pro každého.

Uživatelé si mohou změnit vlastní heslo použitím volby v menu prostředí ASSIST nebo zadáním příkazu CHGPWD (Změna hesla). Když si uživatel změní heslo, porovná systém toto nové heslo se systémovými hodnotami hesla. Jestliže uživatel změní heslo pomocí příkazu CHGUSRPRF, systém neporovná nové heslo se systémovými hodnotami hesla.

Poznámka: Jestliže jste nastavili některou ze systémových hodnot hesla, systém nepovolí, aby nové heslo bylo shodné se jménem uživatelského profilu, ledaže byste použili pro nastavení hesla příkaz CHGUSRPRF.

Následující tabulka uvádí systémové proměnné, které ovlivňují zadávání hesla a jeho definici.

Tabulka 12. Systémové hodnoty iSeries pro hesla

Systémové hodnoty	Popis
QPWDEXPITV	Vyžaduje od uživatelů, aby si po stanovené době změnili heslo.
QPWDMAXLEN	Umožňuje zadat maximální délku hesla.
QPWDMINLEN	Umožňuje zadat minimální délku hesla.
QPWDRQDDIF	Zabraňuje uživatelům používat střídavě dvě různá hesla.

Dále toto téma přináší více podrobností o systémových proměnných pro hesla.

- Určení doby platnosti hesla
- Určení délky hesla
- Omezení duplicitních hesel

Zadejte v příkazovém řádku WRKSYSVAL *SEC a prohlédněte si online informace o systémových hodnotách začínajících znaky QPWD.

Určení doby platnosti hesla: Systémová hodnota QPWDEXPITV určuje, jak často jsou uživatelé vyzváni ke změně hesla.

Ještě před skončením doby platnosti hesla varuje systém uživatele, že platnost hesla brzy skončí. Po skončení doby platnosti hesla vyzve systém uživatele ke změně hesla při příštím přihlášení.

Doporučení

Uživatelé by si měli svá hesla pravidelně měnit. To je odradí od sdílení hesla s jinými uživateli systému. Když se tedy neoprávněný uživatel naučí něčí heslo, bude toto heslo použitelné jen po krátkou dobu. Nastavte interval pro změnu hesla dostatečně dlouhý, abyste nerozčilovali uživatele, ale dost krátký, abyste zajistili dostatečnou bezpečnost. Jestliže se chcete vyhnout podobným problémům, nastavte tento interval na 45 až 60 dní.

Poté, co v části 2 formuláře Výběr systémových hodnot, zadáte hodnotu systémové hodnoty PWDEXPITV, můžete pokračovat určením délky hesla.

Určení délky hesla: Někteří uživatelé neradi píší. Jestliže je necháte, zvolí si heslo, které se skládá z jednoho písmene, nebo z jejich iniciál. Naneštěstí jsou krátká hesla pro vetřelce snadněji uhodnutelná. Systémová hodnota QPWDMINLEN vám umožní nastavit minimální délku pro všechna hesla ve vašem systému.

Jestliže váš systém komunikuje s jinými systémy, mohou si uživatelé předávat hesla mezi dvěma různými počítači. Některé způsoby komunikace omezují délku hesla na maximálně 8 znaků. Systémová hodnota QPWDMAXLEN umožňuje učit maximální délku hesla.

Doporučení

Nastavte minimální délku hesla na 6. To vyloučí používání iniciál a povzbudí uživatele k poněkud tvůrčímu přístupu při volbě hesla. Jestliže váš systém komunikuje s jinými systémy, nastavte maximální délku hesla na 8.

Po zadání voleb pro systémové hodnoty QPWDMINLEN a QPWDMAXLEN ve druhé části formuláře Výběr systémových hodnot, se můžete rozhodnout, nakolik omezíte duplicitní hesla.

Omezení duplicitních hesel: Příkaz CHGPWD (Změna hesla) vyžaduje, aby nové heslo bylo jiné, než staré heslo. Avšak uživatelé mohou používat střídavě jen dvě různá hesla, pokud nepoužijete systémovou proměnnou QPWDRQDDIF. Následující tabulka uvádí volby systémové hodnoty QPWDRQDDIF.

Tabulka 13. Hodnoty pro systémovou hodnotu QPDRQDDIF

Hodnota	Počet hesel kontrolovaných na duplicitu
0	0 Duplicitní hesla jsou povolena
1	32
2	24
3	18
4	12
5	10
6	8
7	6
8	4

Doporučení

Použijte dobu platnosti hesla a hodnoty pro omezení duplicitních hesel tak, aby heslo bylo jedinečné po dobu jednoho roku. Například jestliže doba platnosti hesla je 60 dní, použijte pro systémovou hodnotu QPWDRQDDIF hodnotu 7.

Poté, co v části 2 formuláře Výběr systémových hodnot zadáte volbu systémové hodnoty QPWDRQDDIF, můžete rozhodnout, jak přizpůsobit systém pomocí systémových hodnot.

Přizpůsobení systému pomocí systémových hodnot

Server iSeries používá systémové hodnoty a atributy sítí k ovládání mnoha faktorů, které se netýkají zabezpečení. Většinu těchto systémových hodnot a atributů využívá systém a aplikační programy. K přizpůsobení vašeho systému by měl správce systému nastavit několik systémových hodnot.

Pojmenování systému

Pro přiřazení jména vašemu systému použijte síťový atribut SYSNAME. Jméno systému se objevuje v pravém horním rohu obrazovky Přihlášení a v systémových zprávách. Používá se také, když systém komunikuje s jinými systémy nebo s osobními počítači pomocí produktu iSeries Access for Windows.

Při komunikaci s jinými systémy nebo osobními počítači identifikuje váš systém systémové jméno a odliší jej tak od ostatních systémů v síti. Počítače si vzájemně předávají systémová jména, kdykoliv komunikují. Jakmile jednou přidělíte systému jméno, neměli byste je měnit, protože změna systémového jména má vliv na jiné systémy v síti.

Doporučení

Zvolte pro systém jednoznačné a smysluplné jméno. I když dnes nekomunikujete s jinými počítači, může tomu tak být v budoucnu. Jestliže je váš systém součástí sítě, zeptá se vás patrně správce sítě, jaké jméno systému chcete používat.

Například Sharon Jonesová z firmy JKL Toy Company se rozhodla pojmenovat systém JKLTOY.

Zobrazení systémového času a data

Můžete nastavit pořadí, v jakém se bude ukazovat rok, měsíc a den, když systém vytiskne nebo zobrazí datum. Můžete také určit, jaké znaky oddělovače mají být použity mezi Y (rok), M (Měsíc) a D (Den).

Systémová hodnota QDATFMT určuje formát data. Následující tabulka uvádí, jak systém vytiskne datum 16. června 2000 při všech možných volbách.

Tabulka 14. QDATFMT (Formáty systémového data)

Volba	Popis	Výsledek
YMD	Rok, měsíc, den	00/06/16
MDY	Měsíc, den, rok	06/16/00
DMY	Den, měsíc, rok	16/06/00
JUL	Juliánské datum	00/168

Poznámka: Tyto příklady používají znak / (lomítko) jako oddělovač data.

Systémová hodnota QDATSEP určuje, jaký znak má systém použít mezi údaji rok, měsíc a den. Následující tabulka uvádí tyto volby. K určení volby použijte číslo:

Tabulka 15. QDATSEP (Oddělovač systémového data)

Oddělovač	Hodnota QDATSEP	Výsledek
/ (lomítko)	1	16/06/00
- (pomlčka)	2	16-06-00
. (tečka)	3	16.06.00
, (čárka)	4	16,06,00
(mezera)	5	16 06 00

Poznámka: Výše uvedené příklady používají formát DMY.

Systémová hodnota QTIMSEP určuje, jaký znak systém použije k oddělení údajů hodina, minuta a vteřina, když zobrazuje čas. K určení volby použijte číslo. Následující tabulka uvádí, v jakém formátu bude čas při použití všech možných voleb.

Tabulka 16. QTIMSEP (Oddělovač systémového času)

Oddělovač	QTIMSEP	Výsledek
: (dvojtečka)	1	10:30:00
. (tečka)	2	10.30.00
, (čárka)	3	10,30,00
(mezera)	4	10 30 00

Jak pojmenovat systémové zařízení

Systém automaticky konfiguruje všechny nové obrazovkové stanice a tiskárny, které k němu připojíte. Systém přidělí jméno každému novému zařízení. Systémová hodnota QDEVNAMING určuje, jakým způsobem se mu přiřadí jméno. Následující tabulka uvádí, jak systém pojmenuje třetí obrazovkovou stanici a druhou tiskárnu, připojenou k systému.

Tabulka 17. Pojmenování systémového zařízení

Volba	Formát jména	Jméno obrazovkové stanice	Jméno tiskárny
1	iSeries	DSP03	PRT02
2	S/36	W3	P2
3	Adresa zařízení	DSP010003	PRT010002

Poznámka: Ve výše uvedeném příkladu byla obě zařízení, obrazovková stanice a tiskárna, připojena k prvnímu kabelu.

Doporučení

Používejte konvence pojmenování iSeries, jestliže nebudete používat software, který vyžaduje pojmenování podle S/36. Jména iSeries pro obrazovkové stanice a tiskárny jsou méně těžkopádná než jména, která používají adresu zařízení. Jméno obrazovkové stanice a tiskárny se objevuje na některých obrazovkách Provozního asistenta. Jméno tiskárny se také používá při řízení tiskového výstupu.

Poté, co systém nakonfiguruje nové zařízení, použijte ke smysluplnému popisu tohoto zařízení příkaz CHGDEVDSP (Změna obrazovky) nebo CHGDEVPRT (Změna tiskárny). Do popisu zařízení zahrňte fyzickou adresu zařízení i jeho umístění, například *Kancelář Johna Smitha, linka 1, adresa 6*.

Volba systémové tiskárny

K přiřazení systémové tiskárny použije systémovou hodnotu QPRTDEV. Tato systémová hodnota, uživatelský profil a popis úlohy určují, kterou tiskárnu úloha použije. Není-li v uživatelském profilu nebo v popisu úlohy uvedena jiná tiskárna, použije úloha systémovou tiskárnu.

Doporučení

Obvykle by měla být systémová tiskárna nejrychlejší tiskárnou v systému. Systémovou tiskárnu použijte pro tisk dlouhých sestav a jako systémový výstup.

Poznámka: Dokud nenainstalujete a nenakonfigurujete systém, nebudete znát jména tiskáren. Poznamenejte si umístění vaší systémové tiskárny. Později tento údaj použijete v názvu tiskárny.

Povolte zobrazení zprávy o ukončení tiskového výstupu.

Systém umožňuje uživatelům vyhledat jejich tiskové výstupy. Práce s obrazovkou Tiskový výstup zobrazí všechny výstupy, které se právě tisknou nebo čekají na vytištění. Můžete také umožnit uživatelům, aby si mohli prohlédnout seznam zpracovaných tiskových výstupů. Na této obrazovce také uvidíte, kdy byla úloha vytištěna a na které tiskárně. To může být užitečné při hledání ztracených sestav.

Funkce evidence úloh a systémová hodnota QACGLVL umožní zobrazit informace o zpracovaných tiskových výstupech. Volba *PRINT systémové hodnoty QACGLVL umožňuje uložit informace o zpracovaných tiskových výstupech.

Doporučení

Uložené informace o zpracovaných tiskových výstupech zabírají místo v systému. Jestliže uživatelé nebudou podle vašeho mínění tisknout mnoho sestav, nebude patrně nutné umožnit tuto funkci. Zadejte NO ve formuláři Výběr systémových hodnot. Tato hodnota nastaví úroveň evidence úloh na *NONE.

- Ujistěte se, že jste vypracovali firemní strategii zabezpečení pro váš podnik, podobně jako ji v příkladu pro firmu JKL Toy Company připravili Sharon Jonesová a John Smith.
- Dále se ujistěte, že jste zadali volby systémových hodnot ve formuláři Výběr systémových hodnot.
- Poznamenejte si, co byste chtěli zařadit do sdělení týkajícího se zabezpečení.

Poté, co jste zadali všechny volby ve formuláři Výběr systémových hodnot a vypracovali strategii zabezpečení, můžete přejít k plánování skupin uživatelů.

Příklad: Strategie zabezpečení společnosti JKL Toy Company: Níže uvedené poznámky popisují strategii zabezpečení, kterou John Smith, prezident společnosti JKL Toy Company, zaslal svým zaměstnancům. Při vytváření tohoto návrhu zabezpečení spolupracoval John s Sharon.

Tabulka 18. Příklad: Návrh strategie zabezpečení společnosti JKL Toy Company

Připravil: John Smith, prezident

Tabulka 18. Příklad: Návrh strategie zabezpečení společnosti JKL Toy Company (pokračování)

JKL Toy Company

Pro: Všechny zaměstnance společnosti JKL Toy Company

Věc: Zabezpečení nového systému

Všichni jste se zúčastnili informační schůzky o našem novém systému. Ti, kteří budou systém používat, se začali školit a příští týden začnou zpracovávat zákaznické objednávky. Očekáváme, že se tento systém brzy stane rozhodujícím prvkem na cestě k úspěchu našeho podnikání.

Rád bych nyní zhodnotil naše rozhodnutí a strategii týkající se zabezpečení a zdůraznil jejich význam. Tyto strategie byly navrženy k ochraně informací, jež mají rozhodující význam pro naše podnikatelské aktivity.

- Sharon Jonesová je odpovědná za zabezpečení nového systému. Ken Harrison bude jejím asistentem. Pokud budete mít nějaké otázky nebo problémy se zabezpečením, obracejte se přímo na ně.
- Naše rozhodnutí o tom, kdo můžete provádět operace v systému, vycházejí ze současných strategií týkajících se informací. Například:
  - Informace o smlouvách a zvláštních cenících jsou pokládány za důvěrné. Nikdy by neměly být prozrazeny nikomu mimo naši společnost.
  - Pouze účtárna může změnit kreditní limity našich zákazníků.
- Každý, kdo potřebuje použít systém, obdrží ID uživatele a heslo. Po prvním přihlášení do systému budete vyzváni, abyste si změnili heslo, a tato výzva se potom bude opakovat každých 60 dní. Vyberte si takové heslo, které si budete dobře pamatovat, ale které není současně zřejmé. Formulář, který obdržíte společně s ID uživatele, obsahuje několik návrhů pro vytváření hesel.
- *Své heslo nikomu nesdělujte*. Hodláme vám umožnit provádět v systému veškeré operace, které jsou nezbytné pro vaši práci. Pokud budete potřebovat přístup k informacím, kontaktujte Sharon nebo Kena. Zapomenete-li své heslo, Sharon nebo Ken vám mohou okamžitě nastavit nové heslo. Nikdo by neměl mít žádný důvod přihlašovat se do systému s ID uživatele a heslem někoho jiného.
- Možná jste se naučili, jak na pracovní stanici používat funkce pro záznam a přehrávání k tomu, abyste se vyhnuli psaní. *Nepoužívejte* tyto funkce pro uložení svého hesla.
- Neopouštějte svou pracovní stanici bez odhlášení. Během školení jste se naučili, jak se okamžitě odhlásit z pracovní stanice. Použijte tuto funkci v případě, že potřebujete na krátkou chvíli odejít od pracovního stolu. Pokud budete pryč delší dobu, dokončete práci a řádně se odhlaste.

  Odhlášení při opouštění pracovní stanice je zvlášť důležité v místech, která jsou přístupná veřejnosti, jako je například nákladní prostor, zákaznická střediska a detašované prodejní kanceláře.
- Přestože je systémová jednotka velmi odolná, chraňte ji prosím před nárazy a nepokládejte na ni žádné předměty. Ovládací panely na jednotce jsou obvykle deaktivovány, ale raději se jich prosím nedotýkejte. Zaměstnanci účtárny jsou odpovědní za to, že se systémovou jednotkou nebude nikdo bez dovolení manipulovat.

Pamatujte si, že náš nový systém nám má usnadnit práci a zlepšit náš výkon. Naše zásady zabezpečení by vám měly pomoci, nikoli vám překážet. Pokud máte nějaké otázky nebo připomínky, obraťte se kdykoliv na Sharon, Kena nebo na mě.

Jakmile vytvoříte návrh strategie zabezpečení, můžete začít plánovat skupiny uživatelů.

Plánování skupin uživatelů

První krok v procesu plánování, rozhodnutí o strategii zabezpečení, se podobá volbě strategie firmy. Nyní jste připraveni k plánování skupin uživatelů, což připomíná strategii oddělení.

Co je skupina uživatelů?

Skupina uživatelů je přesně to, co vyplývá z jejího názvu: skupina osob, které potřebují pracovat stejným způsobem se stejnými aplikacemi. Skupina uživatelů je obvykle tvořena osobami, které pracují ve stejném oddělení a mají podobné pracovní odpovědnosti. Skupinu uživatelů definujete tak, že vytvoříte skupinový profil.

K čemu slouží skupinový profil?

Skupinový profil slouží v systému k dvěma účelům:

- **Nástroj zabezpečení**: Skupinový profil umožňuje jednoduše organizovat, kteří uživatelé mohou používat určité objekty v systému (oprávnění k objektům). Místo abyste definovali oprávnění k objektům pro jednotlivé členy skupiny, můžete je definovat pro celou skupinu.
- **Nástroj přizpůsobení**: Skupinový profil lze používat jako vzor k vytváření profilů individuálních uživatelů. Většina uživatelů patřících do stejné skupiny má stejné vlastní potřeby z hlediska přizpůsobení, například počáteční menu nebo předvolenou tiskárnu. Tato nastavení lze definovat ve skupinovém profilu a kopírovat je do profilů individuálních uživatelů.

Profily uživatelů usnadňují dodržování jednoduchého a konzistentního schématu zabezpečení a přizpůsobení.

Jaké formuláře použít?

K plánování skupin uživatelů potřebujete tyto formuláře:

- formulář Identifikace skupiny uživatelů
- formulář Popis skupiny uživatelů

Poznámka: Pro každou skupinu uživatelů, která bude v systému, potřebujete jeden formulář Popis skupiny uživatelů.

Informace potřebné k vyplnění těchto formulářů najdete v těchto tématech:

- Identifikace skupin uživatelů.
- Plánování skupinových profilů.
- Výběr hodnot ovlivňujících přihlášení do systému.
- Výběr hodnot omezujících možné činnosti uživatele.
- Výběr hodnot nastavujících prostředí uživatele.

Identifikace skupin uživatelů

Při plánování skupin uživatelů je třeba nejdříve identifikovat skupiny uživatelů v systému. To vám umožní naplánovat přístupová práva k prostředkům, které tyto skupiny potřebují. Pokuste se identifikovat skupiny uživatelů jednoduchým způsobem. Vezměte v úvahu oddělení nebo pracovní skupiny, které budou chtít systém používat. Podívejte se na diagram aplikací, který jste již nakreslili pro používané aplikace. Zjistěte, zda mezi pracovními skupinami a aplikacemi existují přirozené souvislosti:

- Můžete ke každé pracovní skupině určit primární aplikaci?
- Víte, které aplikace každá skupina potřebuje? Které aplikace určité skupiny nepotřebují?
- Víte, které skupiny by měly vlastnit informace v jednotlivých knihovnách aplikací?

Pokud na tyto otázky můžete odpovědět Ano, můžete začít plánovat skupiny uživatelů. Pokud jste však odpověděli Někdy nebo Možná, pravděpodobně bude užitečné použít k identifikaci skupin uživatelů systematický přístup.

Měli byste se podívat na příklad použití tohoto přístupu k identifikaci skupin uživatelů.

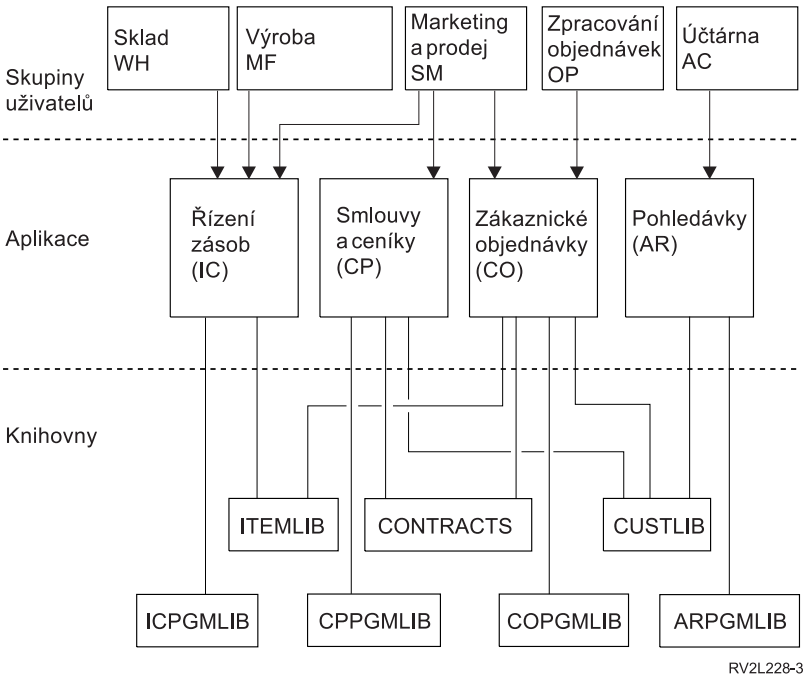
Poznámka: Budou-li uživatelé členy pouze jednoho skupinového profilu, zjednoduší se tím správa zabezpečení. V některých situacích však může být výhodné, aby uživatelé patřili do více než jednoho skupinového profilu.

Správa uživatelů patřících do více než jednoho skupinového profilu je obvykle snazší než udělování mnoha soukromých oprávnění profilům individuálních uživatelů.

Příklad: Identifikace skupin uživatelů: Pokud je vztah mezi pracovními skupinami a aplikacemi složitý nebo nejasný, je možné vše vyjasnit pomocí tabulky použité například ve formuláři Identifikace skupiny uživatelů. Vyplníte-li v tabulce uživatele systému a aplikace, které budou potřebovat, měli byste rozpoznat podobnosti

požadavků. Sharon Jonesová nejen vyplnila formulář Identifikace skupiny uživatelů, ale také pomocí diagramu aplikací identifikovala skupiny uživatelů, kteří potřebují mít k těmto aplikacím přístup.

Na následujícím obrázku je znázorněn diagram aplikací firmy JKL Toy Company.



Pokud je váš přístup k zabezpečení uvolněný, vyznačte písmenem X, že uživatel danou aplikaci potřebuje. Je-li váš přístup k zabezpečení restriktivní, musíte uvážit, jak budou pracovníci používat aplikace. V takovém případě nepište do tabulky písmeno X, ale písmeno V (view - zobrazit) - tím vyznačíte, že uživatel bude informace aplikací pouze prohlížet. Pokud někdo potřebuje provádět změny informací, použijte písmeno C (change - měnit). Má-li někdo primární zodpovědnost za informace, použijte písmeno O (owner - vlastník).

Například ve firmě JKL Toy Company potřebují různé skupiny aplikaci Smlouvy a ceníky:

- Oddělení prodeje a marketingu stanoví ceny a uzavírá smlouvy se zákazníky. Toto oddělení vlastní (*O*wns) informace o cenách a smlouvách.
- Oddělení zákaznických objednávek mění informace o smlouvách nepřímo. Když toto oddělení zpracovává objednávky, mění se množství obsažená ve smlouvě. Pracovníci tohoto oddělení potřebují měnit (*C*hange) informace o cenách a smlouvách.
- Pracovníci oddělení pro zpracování objednávek potřebují při plánování práce prohlížet informace o kreditních limitech, avšak nesmějí tyto informace měnit. Potřebují zobrazit (*V*iew) soubor kreditních limitů.

Tabulka 19. Příklad: Formulář společnosti JKL Toy Company: Identifikace skupiny uživatelů

Formulář Identifikace skupiny uživatelů					
Zhotovila: Sharon Jonesová		Datum: 2. 9. 2003			
		Požadovaný přístup k aplikacím			
Jméno uživatele	Oddělení	APL: CO	APL: IC	APL: PC	APL: AR
Ken H.	Zpracování objednávek	O	C	C	C
Karen R.	Zpracování objednávek	O	C	C	C
Kris T.	Účtárna	V		V	O
Sandy J.	Účtárna	V	C	V	O

Tabulka 19. Příklad: Formulář společnosti JKL Toy Company: Identifikace skupiny uživatelů (pokračování)

Peter D.	Účtárna	C		V	O
Ray W.	Sklad	V	O	V	
Rose Q.	Sklad	V	O	V	
Roger T.	Prodej a marketing	C	C	O	C
Sharon J.	Vedoucí	C	C	C	C

Poznámka:

- Pokud je vaše prostředí zabezpečení *uvolněné*, vyznačte písmenem X, které aplikace uživatelé potřebují.
- Pokud je vaše prostředí zabezpečení *průměrné*, vyznačte písmenem A, kteří uživatelé a k jakým aplikacím budou mít oprávnění.
- Pokud je vaše prostředí zabezpečení *přísné*, vyznačte *způsob* použití aplikací pomocí písmen C (change - změny), V (view - prohlížení) a O (owner - vlastník).

Sharon Jonesová si při přípravě tabulky udělala pár poznámek o svých rozhodnutích:

- Pracovníci oddělení pro zpracování objednávek a pracovníci účtárny se mohou vzájemně zastupovat. V současnosti potřebují podobné aplikace. Musí však být v samostatných skupinách, protože časem přijmou více zaměstnanců a budou se více specializovat.
- Přestože není dovoleno, aby pracovníci oddělení pro zpracování objednávek měnili stav zásob nebo smlouvy přímo, vyrovnávání položek a smluv probíhá automaticky při vytváření a vyplňování objednávek. Stane se z toho v budoucnosti bezpečnostní problém?
- Pracovníci oddělení prodeje a marketingu se účastní všech obchodních činností a potřebují všechny aplikace. Stanovují ceny a popisy položek. Definují nové zákazníky, i když kreditní limity určuje účtárna. Odpovídají za stanovení všech smluvních podmínek a cen.

Rozhodněte, jak rozdělit uživatele do skupin. Pokud vám to pomůže, vyplňte formulář Identifikace skupiny uživatelů.

Po přidání uživatelů do formuláře Identifikace skupiny uživatelů můžete začít plánovat skupinové profily.

Plánování skupinových profilů

Po identifikaci skupin uživatelů jste připraveni naplánovat pro každou skupinu profil. Mnohá rozhodnutí, která učiníte, budou mít vliv na zabezpečení i přizpůsobení. Pokud například zadáte počáteční menu, můžete uživatele omezit pouze na toto menu. Zároveň tím zajistíte, aby se uživateli po přihlášení zobrazilo správné menu.

Připravte pro jednu skupinu uživatelů ukázkový formulář Popis skupiny uživatelů. Po dokončení prvního formuláře se vraťte a vytvořte formuláře pro další skupiny, které potřebujete.

Zabezpečení a přizpůsobení je v systému iSeries navrženo tak, aby bylo velmi flexibilní. Metoda plánování uvedená v tomto tématu je vhodným způsobem návrhu skupinových profilů a popisů úloh, ale programátor nebo dodavatel aplikací může doporučit jinou metodu.

Pojmenování skupinových profilů

Protože se skupinový profil chová jako zvláštní typ uživatelského profilu, můžete skupinové profily snadno identifikovat v seznamech a obrazovkách. Musíte jim přiřadit speciální jména. Pokud se mají skupinové profily zobrazit v seznamech pohromadě, musí jejich jména začínat stejnými písmeny, například GRP (pro skupinu) nebo DPT (pro oddělení). Při pojmenování skupin uživatelů dodržujte tyto pokyny:

- Jména skupin uživatelů mohou být dlouhá maximálně 10 znaků.
- Jméno může obsahovat písmena, číslice a tyto speciální znaky: # (znak libry), $ (znak dolaru), _ (znak podtržení) a @ (znak ″zavináč″).
- Jméno nesmí začínat číslicí.

Poznámka: Systém přiřadí každému skupinovému profilu identifikační číslo skupiny (*gid*). Obvykle přenecháte systému, aby generoval číslo *gid*. Pokud používáte systém v síti, můžete potřebovat přiřadit skupinovým profilům specifická čísla gid. Obraťte se na správce sítě a ověřte, zda potřebujete přiřadit čísla gid.

Svůj systém pojmenování skupinových profilů zadejte do příslušného pole formuláře Konvence pojmenování. Sharon Jonesová například zvolila jako konvenci pojmenování skupinových profilů použití počátečních písmen DPT. Vyplnila odpovídající část formuláře Konvence pojmenování.

Tabulka 20. Příklad: Formulář společnosti JKL Toy Company: Konvence pojmenování - skupinový profil

Typ objektu	Konvence pojmenování
Skupinové profily	Používejte znaky DPT následované zkratkou oddělení. Textovým popisem skupinového profilu by mělo být jméno oddělení.

Určení aplikací a knihoven, které skupina uživatelů potřebuje

Pokud jste tak dosud neučinili, přidejte skupiny uživatelů do diagramu aplikací a knihoven, který jste nakreslili dříve. Toto grafické znázornění vám pomůže při rozhodování, které prostředky a aplikace jednotlivé skupiny potřebují.

V části 1 formuláře Popis skupiny uživatelů zadejte primární aplikaci skupiny. Je to aplikace, kterou bude skupina používat nejčastěji. Uveďte další aplikace, které bude skupina potřebovat.

Podívejte se na formuláře Popis aplikace a na diagram aplikací. Tak poznáte, které knihovny každá skupina potřebuje. Obraťte se na programátora nebo dodavatele aplikací a zjistěte nejlepší způsob, jak poskytnout přístup k těmto knihovnám. Většina aplikací používá některou z těchto metod:

- Aplikace zahrne knihovny do počátečního seznamu knihoven.
- Aplikace spustí instalační program, který umístí knihovny do seznamu knihoven uživatele.
- Knihovny nemusí být v seznamu knihoven. Aplikační programy knihovnu vždy specifikují.

Systém používá seznam knihoven k tomu, aby nalezl soubory a programy, které potřebujete při spouštění aplikací. **Seznam knihoven** je seznam knihoven, ve kterém systém hledá objekty, jež potřebuje uživatel. Tento seznam má dvě části:

1. **Systémová část**: Tato část je zadána pomocí systémové hodnoty QSYSLIBL. Používá se pro knihovny systému OS/400. Předvolbu této systémové hodnoty není třeba měnit.
2. **Uživatelská část**: Tuto část seznamu knihoven určuje systémová proměnná QUSRLIBL. Popis úlohy uživatele specifikuje počáteční seznam knihoven a příkazy prováděné po přihlášení uživatele. Použijete-li počáteční seznam knihoven, potlačí systémovou hodnotu QUSRLIBL. Knihovny aplikací by měly být obsaženy v uživatelské části seznamu knihoven.

Použití popisu úlohy

Když se uživatel přihlásí do systému, popis úlohy uživatele definuje mnoho charakteristik úlohy, včetně toho, jak úloha tiskne, jak jsou prováděny dávkové úlohy, a také počáteční seznam knihoven. Systém obsahuje popis úlohy nazvaný QDFTJOBD, který můžete využít při vytváření skupinových profilů. QDFTJOBD však jako počáteční seznam knihoven určuje systémovou hodnotu QUSRLIBL. Pokud chcete, aby po přihlášení měly různé skupiny uživatelů přístup k různým knihovnám, musíte pro každou skupinu vytvořit jedinečné popisy úloh.

Knihovny, které bude skupina potřebovat, uveďte ve formuláři Popis skupiny uživatelů. Pokud má být knihovna obsažena na počátečním seznamu knihoven v popisu úlohy skupiny, označte jméno takové knihovny ve formuláři.

Dříve než budete volit hodnoty ovlivňující přihlášení, měli byste se seznámit s příkladem, jak Sharon Jonesová popsala skupiny uživatelů ve firmě JKL Toy Company.

Příklad: Formulář společnosti JKL Toy Company: Popis skupiny uživatelů: První tabulka zobrazuje část 1 formuláře Popis skupiny uživatelů, kterou Sharon Jonesová připravila pro prodejní a marketingové oddělení. Všimněte

si, že do počátečního seznamu knihoven skupiny nezahrnula knihovny CONTRACTS a CPPGMLIB. Aplikace je namísto do počátečního seznamu knihoven DPTSM automaticky přidává do seznamu knihoven. Když uživatel ukončí aplikaci, systém odstraní knihovny ze seznamu knihoven. To poskytuje těmto knihovnám další zabezpečení, protože ke knihovnám je přístup pouze přes aplikační programy.

Tabulka 21. Příklad: Formulář společnosti JKL Toy Company: Popis skupiny uživatelů

Formulář Popis skupiny uživatelů	část 1 ze 2
Zhotovila: Sharon Jonesová	Datum: 9/5/99
Jméno skupinového profilu: DPTSM Popis skupiny: Prodejní a marketingové oddělení	
Primární aplikace pro skupinu: Smlouvy a ceníky Zapište do seznamu ostatní aplikace požadované skupinou: Zásoby (zadání cen a popisů položek), zákaznické objednávky	
Zapište do seznamu všechny knihovny, které skupina potřebuje. Označte (✓) každou skupinu, která by měla být na počátečním seznamu knihoven pro skupinu: • ✓CUSTLIB • ✓ITEMLIB • ✓COPGMLIB • ✓ICPGMLIB • CPPGMLIB • CONTRACTS	

Sharon také začala pracovat na formuláři Popis skupiny uživatelů pro sklad.

Tabulka 22. Formulář Popis skupiny uživatelů: Popisné informace

Formulář Popis skupiny uživatelů	část 1 ze 2
Zhotovila: Sharon Jonesová	Datum: 9/5/99
Jméno skupinového profilu: DPTWH Popis skupiny: Sklad	
Primární aplikace pro skupinu: Řízení zásob Zapište do seznamu ostatní aplikace požadované skupinou: Žádné	
Zapište do seznamu všechny knihovny, které skupina potřebuje. Zaškrtněte (✓) každou knihovnu, která by měla být na počátečním seznamu knihoven pro skupinu: • ✓ITEMLIB • ✓ICPGMLIB	

Jakmile dokončíte část 1 formuláře Popis skupiny uživatelů, můžete začít s výběrem hodnot, které ovlivňují přihlašování do systému.

Výběr hodnot ovlivňujících přihlášení do systému

Po naplánování skupinových profilů v systému je třeba zvolit systémové hodnoty ovlivňující přihlášení do systému. Své volby zadejte do části 2 formuláře Popis skupiny uživatelů. Pamatujte na to, že vyberete hodnoty, které budou použity při vytvoření individuálních profilů členů skupiny. Začněte zadáním jména skupinového profilu, které jste vybrali, a stručným textovým popisem skupiny.

Pokud systém správně uživatelsky přizpůsobíte, budou uživatelé moci na obrazovce Přihlášení zadávat pouze své ID uživatele a hesla. Další hodnoty přihlášení poskytnou uživatelské profily.

Heslo

Nastavte heslo skupinového profilu na *NONE. Tím zabráníte, aby se kdokoliv mohl přihlásit pomocí skupinového profilu. Až později kopírováním skupinového profilu vytvoříte profily individuálních uživatelů, nastavíte heslo pro každého uživatele.

Počáteční program a počáteční procedura

Počáteční program uživatele, nazývaný také často jako **přihlašovací program**, se spustí předtím, než systém zobrazí první menu. Vložte jméno programu a jeho knihovnu do skupinového profilu, i když je knihovna součástí počátečního seznamu knihoven. Zadáním obou údajů zajistíte, aby systém spustil správný program, a nemusíte starat o změny v seznamu knihoven.

Počáteční program nebo procedura se používá z některého z těchto důvodů:

- Některé aplikace používají počáteční program k nastavení aplikačního prostředí.
- Chcete, aby uživatel spouštěl pouze jeden program a nikdy se mu nezobrazilo menu. Například pracovníci ve firmě JKL Toy Company, kteří používají pracovní stanici v nákladovém prostoru, mohou spustit pouze program pro příjem zásob. Zabraňuje se tak bezpečnostním rizikům na pracovních stanicích na veřejném místě.

Nastavením pole **Omezené schopnosti** pro uživatele na hodnotu *YES nebo *PARTIAL lze zabránit uživateli, aby na obrazovce Přihlášení změnil počáteční program.

Zjistěte od programátora, zda vaše aplikace vyžadují počáteční program nebo proceduru.

Počáteční menu a knihovna počátečního menu

Počáteční menu, nazývané také **init menu**, je první menu, které se uživateli zobrazí po přihlášení. Před zobrazením počátečního menu se spustí počáteční program. Pokud počáteční program zobrazuje nějaké obrazovky, uživatel uvidí tyto obrazovky předtím, než systém ukáže počáteční menu.

Počáteční menu skupiny by obvykle mělo být primárním menu hlavní aplikace skupiny. Zadejte jméno menu a jeho knihovnu.

Nastavením pole **Omezené schopnosti** pro uživatele na hodnotu *YES lze zabránit uživateli, aby na obrazovce Přihlášení změnil počáteční menu. Nastavíte-li pole *Omezené schopnosti* na hodnotu *PARTIAL, dovolíte uživateli změnit na obrazovce Přihlášení počáteční menu.

Aktuální knihovna

Aktuální knihovna se také nazývá **předvolená knihovna**. Určíte-li pro uživatele aktuální knihovnu, stane se několik věcí:

- Jestliže uživatel vytvoří nějaké objekty, například dotazovací programy, systém umístí tyto objekty do aktuální knihovny (pokud uživatel neurčí jinou knihovnu).
- Systém automaticky přidá aktuální knihovnu do uživatelské části seznamu knihoven. Aktuální knihovna může být zahrnuta na počátečním seznamu knihoven v popisu úlohy, ale nemusí.
- Aktuální knihovna se stane první knihovnou v uživatelské části seznamu knihoven. Systém hledá soubory a programy nejdříve v aktuální knihovně a až potom v knihovnách uvedených na seznamu uživatelských knihoven.
- Pokud uživateli nepřiřadíte aktuální knihovnu, systém mu přiřadí knihovnu QGPL (univerzální).

Doporučení

Aktuální knihovna je důležitá, zejména pokud plánujete použití licencovaného programu IBM Query for iSeries, nebo jiného podobného programu. Použijte některý z těchto přístupů:

- Vytvořte knihovnu, kterou budou sdílet všichni členové skupiny. Umístěte do této knihovny všechny dotazovací programy a soubory skupiny. Dejte jí stejné jméno jako skupinovému profilu a učiňte z ní aktuální knihovnu skupiny.
- Poskytněte každému uživateli, který plánuje používání licencovaného programu Query, osobní knihovnu. Pojmenujte knihovnu stejně jako uživatelský profil. Určete tuto knihovnu jako aktuální knihovnu v profilech individuálních členů skupiny, ne však ve skupinovém profilu.

V části 2 formuláře Popis uživatele vyplňte své volby do polí, která ovlivňují přihlášení.

Po výběru hodnot ovlivňujících přihlášení můžete vybrat hodnoty omezující možné činnosti uživatele.

Výběr hodnot omezujících možné činnosti uživatele

Po výběru hodnot ovlivňujících přihlášení v části 2 formuláře Popis skupiny uživatelů byste měli zvážit, jak omezit možné činnosti uživatelů v systému. K omezení činností uživatelů můžete mít několik důvodů:

- Chcete zabránit uživatelům používat CL příkazy. Mohlo by je to lákat k experimentování, při kterém by mohli neúmyslně způsobit různé škody.
- Chcete omezit přístup uživatelů k určitým aplikacím a funkcím.
- Chcete poskytovat jednoduché prostředí, ve kterém nebudou uživatelé mateni nadbytečnými volbami.

Rozsah možných činností uživatelů určuje mnoho faktorů:

- návrh aplikace
- systémové hodnoty
- zabezpečení prostředků
- skupinové profily
- uživatelské profily
- popisy úloh

Dvě pole ve skupinovém nebo uživatelském profilu, **Omezení schopností** a **Třída uživatele**, určují, nakolik budou uživatelé moci předefinovat rozhodnutí, která provedete.

Pole Omezení schopností

Pole **Omezení schopností** se nazývá **Omezené použití příkazového řádku**. Omezit můžete, zda uživatelé mohou měnit hodnoty na obrazovce Přihlášení, zadávat příkazy a měnit svůj program pro zpracování klávesy Attention. Můžete zvolit přísná omezení (*YES), průměrná omezení (*PARTIAL) nebo žádná omezení (*NO). V následující tabulce je ukázáno, co každá z těchto hodnot dovoluje:

Tabulka 23. Činnosti povolené hodnotami polí Omezené schopnosti.

Hodnota pole Omezené schopnosti	Změna počátečního programu	Změna počátečního menu	Změna aktuální knihovny	Změna programu pro zpracování klávesy Attention	Zadávání příkazů
*YES	Ne	Ne	Ne	Ne	Pouze několik [1]
*PARTIAL	Ne	Ano	Ne	Ne	Ano
*NO	Ano	Ano	Ano	Ano	Ano

1 Povoleny jsou tyto příkazy: SIGNOFF, SNDMSG, DSPMSG, DSPJOB, DSPJOBLOG a STRPCO. Uživatel nemůže z žádného menu nebo obrazovky Provozního asistenta (Operational Assistant) použít klávesu F9 k zobrazení příkazového řádku.

Pole Třída uživatele

Třída uživatele, často také nazývaná jako **typ uživatele**, určuje, které volby uživatel uvidí v Provozním asistentovi a v systémových menu. Určuje také, které funkce systému smí uživatel provádět, neuvedete-li oprávnění v poli **Zvláštní oprávnění**.

Doporučení pro omezené schopnosti a třídu uživatele

Většina uživatelů nepotřebuje nebo nechce mít přístup k CL příkazům nebo systémovým funkcím. Obrazovky Provozního asistenta (Operational Assistant) poskytují uživatelům dostatek informací a dostatečnou kontrolu nad vlastní prací. Tato doporučení umožňují, aby uživatelé měli přístup pouze k systémovým prostředkům, které potřebují k provádění svých úkolů:

- V každém skupinovém profilu nastavte pole **Omezené schopnosti** na hodnotu *YES. Nastavte pole *Třída uživatele* na hodnotu *USER.
- Předefinujte tyto specifikace u individuálních uživatelů, kteří potřebují systémové funkce.
- Zajistěte, aby vaše menu poskytovala prostředky k přechodům mezi aplikacemi, pokud to uživatelé potřebují.

Po zadání vybraných hodnot třídy uživatele a možností omezení v části 2 formuláře Popis skupiny uživatelů můžete vybrat hodnoty nastavující prostředí uživatele.

Výběr hodnot nastavujících prostředí uživatele

Po výběru voleb omezujících činnost uživatelů v systému v části 2 formuláře Popis skupiny uživatelů můžete vybrat hodnoty, které určují provozní prostředí uživatele. Uživatelský profil obsahuje mnoho polí, která určují provozní prostředí uživatele: kterou tiskárnu používat, kam posílat zprávy, s jakou prioritou spouštět úlohy. U mnoha polí se doporučuje použít předvolené nastavení. Několik polí je popsáno v následujících odstavcích.

- **Popis úlohy a knihovna popisu úlohy**: Tato pole profilu sdělují systému, který popis úlohy má použít při přihlášení uživatele do systému. Popisy úloh obsahují počáteční seznam knihoven. Každá skupina uživatelů má mít popis úlohy se stejným jménem jako skupinový profil. Popisy úloh se obvykle ukládají do knihovny QGPL.
- **Tiskové zařízení a výstupní fronta**: Jakýkoliv tiskový výstup vytvořený uživatelem směřuje do tiskového zařízení uvedeného v profilu (pokud jej konkrétní tisková úloha neodešle na jinou tiskárnu). Členové skupiny uživatelů jsou obvykle umístěni společně a sdílejí stejnou tiskárnu. Tuto tiskárnu lze zadat ve skupinovém profilu a zkopírovat její jméno do všech profilů individuálních uživatelů. Tiskové zařízení uživatele se také nazývá **předvolená tiskárna**.

  Výstupní fronta obsahuje tiskový výstup před jeho vytištěním. Každé tiskové zařízení má obvykle vlastní výstupní frontu téhož jména. Chcete-li sdělit systému, aby používal výstupní frontu tiskového zařízení, můžete jako výstupní frontu zadat *DEV.

  Vyplňte ve formuláři Popis skupiny uživatelů pole jména popisu úlohy a jeho knihovny a pole předvolené tiskárny a výstupní fronty.
- **Nastavení rozhraní Provozního asistenta**: V dodaném systému je menu Provozního asistenta vyvoláváno u každého uživatele programem pro zpracování klávesy Attention. Jestliže uživatelé stisknou klávesu Attention, zobrazí se menu Provozního asistenta (ASSIST). Pokud vaše aplikační programy již používají jiný program pro zpracování klávesy Attention, musíte uživatelům poskytnout jiný způsob, jak zobrazit menu Provozního asistenta:
  - Přidejte menu Provozního asistenta jako volbu do hlavních menu aplikací - buď pomocí příkazu GO ASSIST, nebo pomocí příkazu CALL QEZAST.
  - Instruujte uživatele, aby zadávali na příkazovém řádku příkaz GO ASSIST.

Pokud je pole **Omezené schopnosti** v uživatelském profilu nastaveno na hodnotu *YES, nemůže uživatel zobrazit menu pomocí příkazu GO. Uživatelům Provozního asistenta musíte nabídnout jinou metodu, jak otevřít menu ASSIST.

Měli byste se podívat na příklad hodnot, které Sharon Jonesová zadala ve formuláři Popis skupiny uživatelů pro firmu JKL Toy Company.

K provedení těchto plánovacích kroků je třeba:

- Vyplnit pro každou skupinu uživatelů ve firmě formulář Popis skupiny uživatelů.
- Popsat pravidla pojmenování skupin uživatelů ve formuláři Konvence pojmenování.
- Přidat skupiny uživatelů do diagramu aplikací a knihoven.

Po dokončení těchto úkolů můžete začít plánovat profily individuálních uživatelů.

Příklad: Formulář společnosti JKL Toy Company: Popis skupiny uživatelů — část 2: Sharon Jonesová vytvořila během přípravy formuláře Popis skupiny uživatelů pro zaměstnance prodejního a marketingového oddělení také několik poznámek o prodejním a marketingovém oddělení a skladu.

- Zaměstnanci prodejního a marketingového oddělení budou častými uživateli produktu IBM Query for iSeries. Každý uživatel by měl mít vlastní knihovnu. Sklad může mít jednu skupinovou knihovnu.
- Lidé ze skladu, kteří pracují na příjmu, budou potřebovat namísto počátečního menu počáteční program.

Sharon připravila pro obě oddělení část 2 formuláře Popis skupiny uživatelů.

Tabulka 24. Příklad: Formulář společnosti JKL Toy Company: Popis skupiny uživatelů - prodejní a marketingové oddělení

Jméno pole	**Doporučená hodnota**	**Vaše volba**
Jméno skupinového profilu (uživatel)		DSTSM
Heslo	*NONE	*NONE
Třída uživatele (typ uživatele)	*USER	*USER
Aktuální knihovna (předvolená knihovna)	*stejné jako jméno skupinového profilu*	(pro skupinu nechte prázdné; vyplňte pro individuální profily)
Počáteční program, který má být volán (program pro přihlášení se do systému)		
Knihovna počátečního programu		
Počáteční menu (první menu)		CPMAIN
Knihovna počátečního menu		CPMAINLIB
Omezení schopností (omezené použití příkazového řádku)	*YES	*PARTIAL
Text (popis uživatele)		Prodej a marketing
Popis úlohy	*stejné jako jméno skupinového profilu*	DPTSM
Knihovna popisu úlohy		QGPL
Jméno skupinového profilu (skupina uživatelů)	*NONE[1]	*NONE
Tiskové zařízení (předvolená tiskárna)		PRT03
Výstupní fronta	*DEV	*DEV

Tabulka 25. Příklad: Formulář společnosti JKL Toy Company: Popis skupiny uživatelů - sklad

Jméno pole	**Doporučená hodnota**	**Vaše volba**
Jméno skupinového profilu (uživatel)		DPTWH
Heslo	*NONE	*NONE
Třída uživatele (typ uživatele)	*USER	*USER
Zvláštní prostředí		
Aktuální knihovna (předvolená knihovna)	*stejné jako jméno skupinového profilu*	DPTWH
Počáteční program, který má být volán (program pro přihlášení se do systému)		
Knihovna počátečního programu		
Počáteční menu (první menu)		ICMAIN
Knihovna počátečního menu		ICPGMLIB

Tabulka 25. Příklad: Formulář společnosti JKL Toy Company: Popis skupiny uživatelů - sklad (pokračování)

Jméno pole	Doporučená hodnota	Vaše volba
Omezení schopností (omezené použití příkazového řádku)	*YES	*YES
Text (popis uživatele)		Sklad
Popis úlohy	*stejné jako jméno skupinového profilu*	DPTWH
Knihovna popisu úlohy		QGPL
Jméno skupinového profilu (skupina uživatelů)	*NONE[1]	*NONE
Tiskové zařízení (předvolená tiskárna)		PRT04
Výstupní fronta	*DEV	*DEV
1 Pro skupinový profil musí být jméno skupinového profilu *NONE. Skupinový profil nemůže být členem jiné skupiny.		

Nyní můžete začít plánovat profily individuálních uživatelů.

Plánování profilů individuálních uživatelů

Nyní, když jste zvolili celkovou strategii zabezpečení a naplánovali skupiny uživatelů, jste připraveni k plánování profilů individuálních uživatelů.

Jaké formuláře použít?

K plánování profilů individuálních uživatelů použijte tyto formuláře:

- formulář Profil individuálního uživatele
- formulář Odpovědnost za systém

Také budete potřebovat použít informace z těchto vyplněných formulářů:

- formulář Definice skupiny uživatelů
- formulář Konvence pojmenování
- diagram aplikací

Pojmenování uživatelských profilů

Jméno uživatelského profilu slouží k identifikaci uživatele v systému. Uživatel zadává jméno uživatelského profilu do pole **ID uživatele** na obrazovce Přihlášení. Cokoliv uživatel udělá a jakýkoliv tiskový výstup vytvoří, vše je asociováno se jménem jeho uživatelského profilu.

Při volbě jmen uživatelských profilů pamatujte na tyto skutečnosti:

- Jméno uživatelského profilu může být dlouhé maximálně 10 znaků. Některé komunikační metody omezují délku ID uživatele na 8 znaků.
- Jméno uživatelského profilu může obsahovat písmena, číslice a tyto speciální znaky: # (znak libry), $ (znak dolaru), _ (znak podtržení) a @ (znak ″zavináč″). Nesmí začínat číslicí nebo podtržítkem (_).
- Systém nerozlišuje ve jménu uživatelského profilu velká a malá písmena. Zadáte-li písmena malé abecedy, systém je převede na velká písmena.
- Na obrazovkách a v seznamech používaných ke správě uživatelských profilů se uživatelské profily zobrazují v abecedním pořadí podle jmen uživatelských profilů.
- Všechny profily dodané IBM začínají písmenem Q. Nedávejte uživatelským profilům jména začínající písmenem Q, aby nebyly při zobrazení zařazeny mezi profily dodané IBM.

Doporučení

Jedna z možných metod přiřazování jmen uživatelských profilů je, že použijete prvních 7 znaků příjmení a za ně připojíte první znak křestního jména. Zde je příklad konvencí pojmenování, které pro uživatelské profily použila Sharon ve firmě JKL Toy Company:

Tabulka 26. Příklad: Formulář společnosti JKL Toy Company: Konvence pojmenování

Jméno uživatele	**Jméno uživatelského profilu**
Anderson, George	ANDERSOG
Anderson, Roger	ANDERSOR
Jonesová, Sharon	JONESS

Tato metoda umožňuje snadné zapamatování jmen uživatelských profilů. Kromě toho jsou seznamy a obrazovky seřazeny abecedně podle příjmení.

Například Sharon Jonesová z firmy JKL Toy Company má v úmyslu tuto metodu pojmenování používat. Vyplnila odpovídající část formuláře Konvence pojmenování.

Tabulka 27. Příklad: Formulář společnosti JKL Toy Company: Konvence pojmenování - profil uživatele

Typ objektu	**Konvence pojmenování**
Uživatelské profily	Používejte prvních 7 znaků příjmení uživatele a za ně připojte první znak křestního jména uživatele. Popisem uživatelského profilu bude příjmení, křestní jméno.

Popište ve formuláři Konvence pojmenování plánované pojmenování uživatelských profilů. Pak můžete určit, kdo má být zodpovědný za systémové funkce, a zvolit hodnoty pro každého uživatele.

Určení, kdo má být zodpovědný za systémové funkce

Při plánování profilů individuálních uživatelů musíte nejdříve určit odpovědnost individuálních uživatelů systému. Má-li být provoz systému efektivní, musí uživatelé pravidelně provádět různé činnosti v oblasti správy a údržby. Uživatelé provádějící tyto úkoly potřebují patřičná oprávnění, aby mohli spouštět příkazy a provádět systémové funkce.

V části Výběr hodnot omezujících možné činnosti uživatele bylo popsáno, jak pole **Třída uživatele** a pole **Omezení schopností** určují, ke kterým systémovým funkcím bude mít uživatel přístup. Uživatelé by běžně neměli mít povoleno provádět systémové funkce (pole Třída uživatele by mělo být nastaveno na hodnotu *USER a pole Omezení schopností na hodnotu *PARTIAL nebo *YES). K efektivnímu fungování systému je však nutné, aby někteří uživatelé měli další oprávnění.

V následující tabulce jsou uvedeny některé důležité úkoly správy systému. Jsou v ní také vyznačeny třídy uživatele a zvláštní oprávnění, které je třeba přidělit uživatelům s příslušnými odpovědnostmi. Tento seznam vám pomůže určit, kteří uživatelé systému potřebují zvláštní oprávnění. Nemá to však být úplný plánovací nástroj pro provoz a údržbu systému. V této tabulce jsou uvedeny třídy uživatele a zvláštní oprávnění, které fungují ve většině systémů. V závislosti na použitém systému však může být zapotřebí přiřadit jiná oprávnění.

Pokud v profilu přiřadíte jinou třídu uživatele než *USER, uživatel automaticky získá určitou sadu zvláštních oprávnění k provádění systémových funkcí. Uživateli můžete přiřadit zvláštní oprávnění, která se liší od oprávnění, která jste zadali v poli Třída uživatele, ale nemusí to být nezbytné.

Tabulka 28. Odpovědnost za systém, třída uživatele a zvláštní oprávnění

Systémová funkce[1]	**Popis**	**Požadovaná třída uživatele** [2]	**Požadované zvláštní oprávnění** [3]
Systémové operace	Správa tiskových výstupů, odpovědi na zprávy systému, monitorování opakovaných operací, IPL.	*SYSOPR	*JOBCTL

Tabulka 28. Odpovědnost za systém, třída uživatele a zvláštní oprávnění (pokračování)

Systémová funkce[1]	Popis	Požadovaná třída uživatele [2]	Požadované zvláštní oprávnění [3]
Údržba systému	Provádění činností údržby systému, například vytváření plánu automatického čištění nebo monitorování využití disku.	*SYSOPR	*JOBCTL
Zálohování systému	Pravidelné ukládání knihoven aplikací, systémových knihoven a informací o zabezpečení. Podrobné informace o těchto funkcích najdete v aplikaci Information Center v tématu Zálohování a obnova.	*SYSOPR	*SAVSYS
Administrace profilů	Přidávání nových uživatelských profilů, údržba stávajících profilů.	*SECADM	*SECADM
Administrace zabezpečení prostředků	Správa oprávnění k objektům v systému.	*SECOFR	*ALLOBJ
Údržba programů	Pravidelné aplikování PTF na knihovny dodané IBM. Provádění změn v knihovnách aplikací.	*SECOFR	*ALLOBJ
Prověřování zabezpečení	Nastavení funkce prověřování zabezpečení. Určení událostí, uživatelů a objektů, které je třeba prověřovat.		*AUDIT [4]
Konfigurace systému	Přidávání zařízení do systému, změny zařízení v systému a odebírání zařízení ze systému.		*IOSYSCFG[5]

1 U uživatelů s těmito odpovědnostmi nastavte pole Omezení schopností na hodnotu *NO.

2 Toto je minimální potřebná třída uživatele. Třída uživatele poskytuje oprávnění k používání příkazů a voleb menu, které jsou nezbytné k provádění funkce. V závislosti na používaném zabezpečení prostředků mohou být zapotřebí další oprávnění k objektům.

3 Toto konkrétní zvláštní oprávnění je nezbytné k odpovědnostem týkajícím se úloh. Další zvláštní oprávnění může poskytnout třída uživatele.

4 K zvláštnímu oprávnění *AUDIT neexistuje odpovídající třída uživatele. Zvláštní oprávnění *AUDIT je obsaženo v třídě uživatele *SECOFR. Prověřující osoba (auditor) však pravděpodobně nebude potřebovat ostatní schopnosti třídy uživatele *SECOFR. Proto byste měli každému individuálnímu uživateli, který bude potřebovat řídit prověřování systému, měli udělit zvláštní oprávnění *AUDIT.

5 K zvláštnímu oprávnění *IOSYSCFG neexistuje odpovídající třída uživatele. Zvláštní oprávnění *IOSYSCFG je obsaženo v třídě uživatele *SECOFR. Zvláštní oprávnění *IOSYSCFG byste měli udělit pouze uživatelům, kteří potřebují konfigurovat systém. Tito uživatelé mohou vytvářet linky, řadiče a zařízení nebo konfigurovat TCP/IP. Uživatel, který konfiguruje systém, však pravděpodobně nebude potřebovat ostatní schopnosti třídy uživatele *SECOFR.

Doporučení

Předchozí tabulku použijte k plánování uživatelů, kteří budou provádět systémové funkce. Přinejmenším byste měli přiřadit dva uživatele pro správu zabezpečení systému a další dva pro správu provozních operací a zálohování.

Jako nástroj pro správu a prověřování systému používejte formulář Odpovědnost za systém. Sledujte každého uživatele systému, který má zvláštní oprávnění, a důvody, proč tato oprávnění má.

Dříve než zvolíte hodnoty pro každého uživatele, byste se měli seznámit s příkladem, jak stanovila odpovědnosti Sharon Jonesová.

Příklad: Formulář společnosti JKL Toy Company: Odpovědnost za systém: Níže najdete příklad formuláře Odpovědnost za systém, který vytvořila Sharon Jonesová:

Tabulka 29. Příklad: Formulář společnosti JKL Toy Company: Odpovědnost za systém

Kdo je vaším hlavním správcem systému? Sharon Jonesová Kdo je zástupcem správce systému?Ken Harrison			
Jméno profilu	Jméno uživatele	Třída	Poznámky
JONESS	Sharon Jonesová	*SECOFR	Sharon je hlavním správcem systému.
HARRISOK	Ken Harrison	*SECOFR	Ken je Sharonin zástupce jako správce celého systému.
JOHNSONS	Sandy Johnsonová	*SYSOPR	Sandy má hlavní odpovědnost za provoz a zálohování systému.
ROGERSK	Karen Rogersová	*SYSOPR	Karen bude pomáhat Sandy s provozem a zálohováním systému.
WILLISR	Rose Willisová	*SYSOPR	Rose bude obsluhovat systém během druhé směny.

Jakmile dokončíte formulář Odpovědnost za systém, můžete začít s výběrem hodnot pro každého uživatele.

Výběr hodnot pro každého uživatele

Po určení odpovědností uživatelů v systému můžete začít s výběrem hodnot pro každého uživatele. Většinu práce jste vykonali tím, že jste naplánovali skupinové profily jako vzory pro profily individuálních uživatelů. Pomocí formuláře Profil individuálního uživatele přiřaďte každému uživateli správnou skupinu a definujte odlišnosti uživatele od ostatních členů skupiny. Formulář Profil individuálního uživatele byste měli vyplnit jako vzorový pro jednu skupinu uživatelů a pak se vrátit a připravit formuláře Profil individuálního uživatele pro všechny další skupiny uživatelů.

V horní části formuláře Profil individuálního uživatele vyplňte jméno skupinového profilu a další popisné informace.

Příklad: Formulář společnosti JKL Toy Company: Profil individuálního uživatele - popisné informace

Zde je ukázka, jak Sharon Jonesová vyplnila horní část formuláře Profil individuálního uživatele

Tabulka 30. Formulář společnosti JKL Toy Company: Profil individuálního uživatele - popisné informace

Formulář Profil individuálního uživatele		
Zhotovila: Sharon Jonesová		Datum: 5. 9. 2003
Jména skupinových profilů: DPTOP		
Vlastník vytvořených objektů:	Skupinové oprávnění k vytvořeným objektům:	
Typ skupinového oprávnění:		

Určení hodnot pro členy skupiny

Vyplňte ve formuláři Profil individuálního uživatele pro každého člena skupiny jméno profilu a popis (jméno uživatele). V následujících odstavcích je popsáno, jak pro každého člena skupiny určit další hodnoty.

Pamatujte, že vzorem pro profily individuálních uživatelů je skupinový profil. Ve formuláři Profil individuálního uživatele zadejte pouze informace, které se liší od dané skupiny.

- **Přiřazení hesel**: Počáteční hesla přiřadíte uživatelům nejsnadněji tak, že určíte stejná hesla, jako jsou jména profilů. Pak můžete vyžadovat, aby si uživatel změnil heslo při prvním přihlášení do systému (nastavením dočasné platnosti hesla). V tématu Nastavení dočasné platnosti hesla se dozvíte, jak to udělat automaticky při kopírování skupinového profilu. Máte-li v úmyslu to takto provést, nemusíte psát hesla do formuláře Profil individuálního uživatele.

- **Třída uživatele a omezení schopností**: Podívejte se do formuláře Odpovědnost za systém, kteří členové každé skupiny potřebují odlišné hodnoty polí **Třída uživatele** a **Omezení schopností**. Pro všechny, kteří potřebují jiné hodnoty, než jsou ve skupinovém profilu, vyplňte odpovídající informace ve formuláři Profil individuálního uživatele.
- **Zadání jiných hodnot**: Zkontrolujte, zda konkrétní uživatelé nepotřebují hodnoty, které se liší od hodnot zadaných pro skupinu ve formuláři Popis skupiny uživatelů. Ve formuláři Popis skupiny uživatelů jsou pole **Třída uživatele** a **Omezení schopností** uvedena nahoře, protože se jejich hodnoty u některých členů skupiny mohou lišit. Uveďte všechna další pole, která se budou u členů skupiny, se kterou pracujete, lišit.

Chcete-li dokončit tento krok plánování, musíte provést tyto akce:

- Vyplňte formulář Výběr systémových hodnot.
- Popište ve formuláři Konvence pojmenování plánovaný způsob pojmenování uživatelských profilů.
- Pro každou skupinu uživatelů ve firmě připravte formulář Profil individuálního uživatele.

Dříve než budete plánovat zabezpečení prostředků, měli byste se seznámit s příkladem, jaké informace použila pro individuální uživatele Sharon.

Příklad: Formulář společnosti JKL Toy Company: Profil individuálního uživatele: Ve společnosti JKL Toy Company mohou lidé, kteří pracují v nakládacím prostoru, spouštět pouze jeden program. Sharon omezila možnosti těchto uživatelů pouze na několik funkcí, neboť tito uživatelé pracují v místě, kde má veřejnost snadný přístup k jejich pracovním stanicím. Tito zaměstnanci skladu mají počáteční program, ale nikoli počáteční menu. Oddělení pro zpracování objednávek má dvě lokální tiskárny a jednu tiskárnu ve vzdálené prodejní kanceláři. Sharon proto přiřadila některým uživatelům odlišné tiskárny než skupině.

Níže najdete formulář Profil individuálního uživatele, který Sharon Jonesová připravila pro sklad a oddělení pro zpracování objednávek ve společnosti JKL Toy Company. Všimněte si, že Sharon vyplnila pouze ta pole, která se lišila od hodnot nastavených ve skupinovém profilu.

Tabulka 31. Příklad: Formulář společnosti JKL Toy Company: Profil individuálního uživatele - sklad

Jména skupinových profilů: DPTWH					
Pořiďte záznam pro každého člena skupiny:					
Uživatelský profil	**Text (popis)**	**Třída uživatele**	**Omezení schopností**	**Počáteční program / knihovna**	**Počáteční menu / knihovna**
WILLISR	Willisová, Rose	*SYSOPR	*NO		
WAGNERR	Wagner, Ray			ICRCPT/ICPGMLIB	none
AMESJ	Amesová, Janice			ICRCPT/ICPGMLIB	none
FOSSJ	Fossová, Julie				
WOODBURC	Woodburtová, Carol				

Tabulka 32. Příklad: Formulář Profil individuálního uživatele - oddělení pro zpracování objednávek

Jména skupinových profilů: DPTOP				
Pořiďte záznam pro každého člena skupiny:				
Uživatelský profil	**Text (popis)**	**Třída uživatele**	**Omezení schopností**	**Tiskové zařízení**
HARRISOK	Harrison, Ken	*SECOFR	*NO	PRT05
RICHARDK	Richardsová, Karen			
UNGERJ	Unger, Jeff			PRT04
BELLB	Bell, Brad			PRT04

Jako další krok můžete zahájit plánování zabezpečení prostředků.

Plánování zabezpečení prostředků

Po dokončení procesu plánování uživatelů v systému můžete začít s plánováním zabezpečení prostředků, které chrání objekty v systému. V tématu Nastavení zabezpečení prostředků se seznámíte s tím, jak lze zabezpečení prostředků v systému nastavit.

Systémové hodnoty a uživatelské profily řídí přístup k systému a zabraňují neoprávněným uživatelům v přihlášení. Zabezpečení prostředků řídí akce, které mohou oprávnění uživatelé provádět po úspěšném přihlášení. Zabezpečení prostředků podporuje hlavní úkoly zabezpečení v systému, mezi které patří:

- chránit důvěrnost informací
- chránit přesnost informací a zabraňovat tak neoprávněným změnám
- chránit dostupnost informací a zabraňovat tak náhodným nebo úmyslným škodám

Zabezpečení prostředků můžete plánovat různým způsobem v závislosti na tom, zda vaše společnost aplikace vyvíjí, nebo zda je kupuje. U vyvíjených aplikací byste měli požadavky na zabezpečení informací sdělit programátorům během procesu návrhu aplikace. Když aplikace kupujete, musíte své požadavky na zabezpečení nejprve stanovit, a potom je sladit s návrhem výrobce aplikací. Zde uvedené techniky by měly pomoci v obou případech.

Toto téma uvádí základní pojetí plánování zabezpečení prostředků. Představuje hlavní techniky a ukazuje, jak je můžete používat. Níže popsané zásady nemusí fungovat pro každou společnost a každou aplikaci. O plánování zabezpečení prostředků diskutujte s programátorem nebo s dodavatelem aplikací.

Následující témata vám pomohou plánovat zabezpečení prostředků:

- Stanovení cílů v oblasti zabezpečení prostředků.
- Seznámení s typy oprávnění.
- Plánování zabezpečení knihoven aplikací.
- Určení vlastnictví knihoven a objektů.
- Seskupování objektů.
- Zabezpečení tiskových výstupů.
- Zabezpečení pracovních stanic.
- Souhrn doporučení k zabezpečení prostředků.
- Plánování instalace aplikací.

Jaké formuláře použít?

Zkopírujte si následující formuláře a vyplňte je při čtení tohoto tématu. Proveďte celý proces pro jednu aplikaci a potom ho opakujte pro každou další aplikaci.

Tabulka 33. Plánovací formuláře potřebné pro plánování zabezpečení prostředků

Jméno formuláře	**Potřebný počet kopií**
Formulář Seznam oprávnění	Několik
Formulář Zabezpečení pracovní stanice a tiskového výstupu	1

Doplňte údaje do následujících formulářů, se kterými jste již pracovali:

Tabulka 34. Plánovací formuláře, které budou změněny:

Jméno formuláře	**Připravený v tématu**
Formulář Popis knihovny	Popis informací o knihovnách

Tabulka 34. Plánovací formuláře, které budou změněny: (pokračování)

Jméno formuláře	Připravený v tématu
Formulář Popis skupiny uživatelů	Plánování skupinových profilů

Podívejte se do těchto formulářů, které jste již dříve připravili:

Tabulka 35. Plánovací formuláře potřebné pro dokončení zabezpečení prostředků

Jméno formuláře	Připravený v tématu:
Formulář Popis knihovny	Nakreslení diagramu aplikací a Identifikace skupin uživatelů
Formulář Popis aplikace	Popis aplikací
Formulář Profil individuálního uživatele	Výběr hodnot pro každého uživatele
Formulář Identifikace skupiny uživatelů	Identifikace skupin uživatelů
Formulář Odpovědnost za systém	Určení, kdo má být zodpovědný za systémové funkce
Formulář Plánování fyzického zabezpečení systému	Plánování fyzického zabezpečení

Stanovení cílů v oblasti zabezpečení prostředků

Chcete-li začít plánovat zabezpečení prostředků, musíte nejprve porozumět tomu, čeho potřebujete dosáhnout. Server iSeries poskytuje flexibilní implementaci zabezpečení prostředků. Umožňuje vám chránit kritické prostředky přesně podle vašeho přání. Zabezpečení prostředků však aplikacím přináší také zvýšenou režii. Příklad: Kdykoli aplikace potřebuje objekt, musí systém ověřit oprávnění uživatele k tomuto objektu. Vaše potřeba důvěrnosti a provozní náklady musí být v rovnováze. Při rozhodování o zabezpečení prostředků zvažte hodnotu zabezpečení oproti nákladům vynaloženým na zabezpečení.

Chcete-li zabránit tomu, aby zabezpečení prostředků snižovalo výkon aplikací, dodržujte následující pokyny:

- Schéma zabezpečení prostředků musí být jednoduché.
- Zabezpečte pouze ty objekty, které potřebujete zabezpečit.
- Zabezpečení prostředků používejte, chcete-li doplnit, ne nahradit, jiné nástroje na ochranu informací, jako jsou například:
  - omezení uživatelů na určitá menu a aplikace,
  - zabránění uživatelům v zadávání příkazů (omezené schopnosti v uživatelských profilech).

Plánování zabezpečení prostředků zahajte stanovením cílů. Cíle v oblasti zabezpečení můžete definovat buď ve formuláři Popis aplikace, nebo ve formuláři Popis knihovny.

Použití formuláře závisí na tom, jak jsou v knihovnách informace uspořádány.

Prostudujte si příklad cílů v oblasti zabezpečení společnosti JKL Toy Company dříve, než se seznámíte s typy oprávnění, které můžete pro zabezpečení prostředků používat.

Příklad: Cíle v oblasti zabezpečení společnosti JKL Toy Company

Sharon Jonesová použila ve společnosti JKL Toy Company formulář Popis knihovny, aby popsala požadavky na zabezpečení pro knihovnu CUSTLIB (Záznamy o zákaznících):

Tabulka 36. Příklad: Formulář společnosti JKL Toy Company: Popis knihovny - cíle v oblasti zabezpečení

Formulář Popis knihovny	část 1 ze 2
Definujte pro knihovnu cíle v oblasti zabezpečení, jako například to, zda jsou některé informace důvěrné:	Dnes má každý zaměstnanec společnosti povoleno prohlížet si zákaznické objednávky a informace o zákaznících. K tomu, abychom mohli chránit přesnost informací, měli bychom stanovit, kdo je oprávněn je měnit.

Sharon použila formulář Popis aplikace pro aplikací Smlouvy a ceníky, aby popsala cíle v oblasti zabezpečení pro celou aplikaci.

Tabulka 37. Příklad: Formulář společnosti JKL Toy Company: Popis aplikace - cíle v oblasti zabezpečení

Formulář Popis aplikace	část 1 ze 2
Definujte pro knihovnu cíle v oblasti zabezpečení, jako například to, zda jsou některé informace důvěrné:	Informace o smlouvách a zvláštních cenících jsou důvěrné. Prohlížet si je a měnit je může jen několik lidí: • Zaměstnanci prodejního a marketingového oddělení a všichni vedoucí pracovníci potřebují vytvářet, měnit a analyzovat smlouvy. Musí používat soubory a programy. • Zaměstnanci oddělení pro zpracování objednávek mění smlouvy a prohlížejí si ceníky nepřímo, když zadávají a odesílají objednávky. Není jim ale umožněno prohlížet si smlouvy a ceníky v jiných případech, než když zadávají nebo mění objednávku.

Napište cíle v oblasti zabezpečení pro aplikace buď na formulář Popis aplikace, nebo na formulář Popis knihovny. Můžete potom přezkoumat typy oprávnění, které můžete použít pro plánování zabezpečení prostředků.

Seznámení s typy oprávnění

Až dokončíte stanovení cílů v oblasti zabezpečení prostředků a zaznamenáte svá rozhodnutí do formuláře Popis knihovny, můžete začít s plánováním typů oprávnění. Zabezpečení prostředků určuje, jak uživatelé přistupují k objektům v systému.

Oprávnění znamená způsob, jakým je uživatel autorizován k použití objektu. Můžete mít například oprávnění prohlížet informace v systému nebo oprávnění tyto informace měnit. Systém poskytuje několik různých typů oprávnění. IBM seskupuje tato oprávnění do kategorií zvaných **oprávnění definovaná systémem**, která vyhovují potřebám většiny lidí. Následující tabulka uvádí seznam kategorií a popis jejich použití pro zabezpečení souborů a programů.

Poznámka: Při plánování oprávnění použijte níže uvedené tabulky.

Tabulka 38. Oprávnění definovaná systémem

Jméno oprávnění	Povolené operace pro soubory	Nepovolené operace pro soubory	Povolené operace pro programy	Nepovolené operace pro programy
*USE	Prohlížet informace v souboru.	Měnit libovolné informace v souboru a mazat je ze souboru, vymazat soubor.	Spouštět program.	Změnit a vymazat program.
*CHANGE	Prohlížet záznamy v souboru, měnit je a mazat je ze souboru.	Vymazat celý soubor a jeho obsah.	Změnit popis programu.	Změnit a vymazat program.
*ALL	Vytvořit soubor a vymazat ho; přidat záznamy do souboru, měnit je a mazat je ze souboru; poskytovat ostatním oprávnění k použití souboru.	Žádné.	Vytvořit, změnit a vymazat program; poskytovat ostatním oprávnění k použití programu.	Měnit vlastníka programu, pokud program převzal oprávnění.
*EXCLUDE[1]	Žádné.	Každý přístup k souboru.	Žádné.	Každý přístup k programu.

Tabulka 38. Oprávnění definovaná systémem (pokračování)

Jméno oprávnění	Povolené operace pro soubory	Nepovolené operace pro soubory	Povolené operace pro programy	Nepovolené operace pro programy
1	Oprávnění *EXCLUDE potlačuje všechna oprávnění, která jste udělili veřejným uživatelům nebo prostřednictvím skupinového profilu.			

Jak oprávnění k objektu a oprávnění ke knihovně spolupracují

Pokuste se navrhnout jednoduché zabezpečení prostředků na příkladu plánování zabezpečení pro celé knihovny. Musíte nejprve porozumět tomu, jak jsou oprávnění definovaná systémem aplikována na knihovny. Ukazuje to následující tabulka:

Tabulka 39. Oprávnění definovaná systémem pro knihovny

Jméno oprávnění	Povolené operace	Nepovolené operace
*USE	• Pro objekty v této knihovně jsou povoleny všechny operace, které jsou povoleny oprávněním k určitému objektu. • Pro knihovnu je povoleno prohlížet popisné informace.	• Přidávat nové objekty do knihovny. • Změnit popis knihovny. • Vymazat knihovnu.
*CHANGE	• Pro objekty v této knihovně jsou povoleny všechny operace, které jsou povoleny oprávněním k určitému objektu. • Přidávat nové objekty do knihovny. • Změnit popis knihovny.	• Vymazat knihovnu.
*ALL	• Všechny operace povolené oprávněním *CHANGE. • Vymazat knihovnu. • Poskytovat ostatním oprávnění k knihovně.	• Žádné.

Musíte také porozumět tomu, jak oprávnění ke knihovně a oprávnění k objektu spolupracují. Následující tabulka uvádí příklady oprávnění, která jsou vyžadována jak pro objekt, tak pro knihovnu:

Tabulka 40. Jak oprávnění ke knihovně a oprávnění k objektu spolupracují

Typ objektu	Operace	Potřebné oprávnění k objektu	Potřebné oprávnění ke knihovně
Soubor	Měnit data	*CHANGE	*USE
Soubor	Vymazat soubor	*ALL	*USE
Soubor	Vytvořit soubor	*ALL	*CHANGE
Program	Spustit program	*USE	*USE
Program	Měnit (znovu kompilovat) program	*ALL	*CHANGE
Program	Vymazat program	*ALL	*USE

Oprávnění k adresáři je podobné jako oprávnění ke knihovně. Pro přístup k objektu potřebujete oprávnění ke všem adresářům v cestě k objektu.

Nyní můžete začít s plánováním zabezpečení knihoven aplikací.

Plánování zabezpečení knihoven aplikací

Poté, co jste provedli určení hlavních cílů při zabezpečení objektů, můžete začít s plánováním zabezpečení knihoven aplikací. Zvolte si aplikaci, se kterou budete pracovat při provádění zde popsaných pokynů. Jestliže váš systém ukládá soubory a programy do samostatných knihoven, zvolte knihovnu, ve které uloženy soubory. Když skončíte, zopakujte tento postup pro všechny zbývající knihovny.

Prostudujte informace aplikacích a knihovnách, které jste shromáždili.

- Formulář Popis aplikace.
- Formulář Popis knihovny.
- Formulář Popis uživatelské skupiny - pro každou uživatelskou skupinu, která potřebuje používat knihovnu.
- Tabulku aplikací, knihoven a uživatelských skupin.

Přemýšlejte o tom, které skupiny potřebují informace z knihovny, proč je potřebují a co s nimi potřebují dělat.

Stanovení obsahu knihovny

Knihovny aplikací obsahují důležité soubory aplikací. Ty mohou obsahovat další objekty, mnohé z nich jsou programovací nástroje, které se starají o správný běh aplikací. Jsou to například:

- pracovní soubory
- datové oblasti a fronty zpráv
- programy
- soubory zpráv
- příkazy
- výstupní fronty

Většina těchto objektů, mimo knihoven a výstupních front, nepředstavuje velké bezpečnostní riziko. Obvykle obsahují malé množství aplikačních dat, často v podobě těžko srozumitelné mimo prostředí programu. Můžete procházet seznamem jmen a popisů všech objektů v knihovně, nebo tento seznam vytisknout pomocí příkazu DSPLIB (Zobrazení knihovny). Příklad zobrazení obsahu knihovny SMLOUVY: DSPLIB LIB(SMLOUVY) OUTPUT(*PRINT)

Dále rozhodněte, jaká veřejná oprávnění budete potřebovat pro knihovny aplikací a knihovny programů.

Rozhodnutí o veřejném oprávnění ke knihovnám aplikací

Pro účely ochrany objektů se výrazem **veřejnost** rozumí kdokoliv, kdo má oprávnění přihlásit se do systému. **Veřejné oprávnění** umožňuje přístup uživatelů k objektu, jestliže nemají nějaký jiný, blíže specifikovaný přístup. Kromě rozhodnutí o veřejném oprávnění pro objekty, které již jsou v knihovně, můžete specifikovat veřejné oprávnění pro každý nový objekt, přidaný do knihovny později. To lze udělat použitím parametru **CRTAUT (Vytvoření oprávnění)**. Obvykle se shoduje oprávnění uživatelů pro přístup k objektům v knihovně s oprávněním vytvořit nový objekt v knihovně.

Systémová hodnota QCRTAUT (Vytvoření oprávnění) definuje oprávnění k vytvoření nového objektu v rámci celého systému. IBM dodává systémovou hodnotu QCRTAUT nastavenou na *CHANGE. Vyvarujte se změny QCRTAUT, protože ji využívá mnoho systémových funkcí. Jestliže pro nějakou knihovnu zadáte pro systémovou hodnotu CRTAUT (Vytvoření oprávnění) hodnotu *SYSVAL, pak systém použije pro QCRTAUT hodnotu (*CHANGE).

Používejte veřejné oprávnění co nejvíce - jak kvůli jednoduchosti, tak z důvodu výkonu systému. Při rozhodování, jaké veřejné oprávnění byste přidělili dané knihovně si položte tyto otázky.

- Měl by mít kdokoliv z podniku přístup k většině informací v této knihovně?
- Jaký druh přístupu by lidé měli mít při přístupu k většině informací v této knihovně?

Soustřeďte se na rozhodování o většině lidí a o většině informací. Později se naučíte, jak zacházet s výjimkami. Plánování zabezpečení objektů je často cyklický proces. Můžete zjistit, že potřebujete provést změny v veřejných oprávněních poté, co jste zvážili doporučení pro konkrétní objekty. Ještě než zvolíte konkrétní oprávnění, která vyhoví potřebám zabezpečení systému i jeho výkonu, vyzkoušejte několik kombinací veřejných a soukromých k objektům a knihovnám.

Zajištění odpovídajících nastavení

Oprávnění *CHANGE pro objekty a *USE pro knihovny je odpovídající pro většinu funkcí v aplikacích. Ovšem je třeba se dotázat programátora nebo dodavatele dané aplikace, zda některé její funkce nepotřebují další oprávnění.

- Dochází během zpracování k vymazání některých souborů? Dochází k vyčištění některých souborů? Dochází k přidání členů k některým souborům? Smazání objektu, vyčištění souboru nebo přidání členu souboru vyžaduje oprávnění k objektu typu *ALL.
- Vytvářejí se v průběhu zpracování soubory nebo jiné objekty? Vytvoření objektu vyžaduje oprávnění ke knihovně typu *CHANGE.

Můžete si prostudovat příklad o oprávněních k objektům, která zvolila Sharon, ještě než zvážila, jak rozhodnout o veřejných oprávněních pro knihovny programů.

Příklad: Formulář společnosti JKL Toy Company: Popis knihovny:

Sharon Jonesová zkoumala cíle v oblasti zabezpečení pro knihovnu ″Záznamy o zákaznících a informace o aplikacích″ a rovněž si prostudujte informace o odděleních, která tyto informace o zákaznících využívají. Udělala si o svých závěrech poznámky:

- Každé oddělení, kromě skladu a výrobního oddělení, potřebuje měnit informace o zákaznících.
- Všichni uživatelé ve skladu a výrobním oddělení mají uživatelské profily s omezenými schopnostmi (hodnota pole Omezení schopností nastavená na "YES") a jsou jim vyhrazena jen určitá menu a programy. Jejich menu jim umožňují prohlížet si informace o zákaznících, ale nemohou tyto informace měnit.
- Veřejné oprávnění pro objekty v knihovně Záznamy o zákaznících může být nastaveno na *CHANGE. Omezení menu zabrání neoprávněným osobám měnit informace o zákaznících. Tato situace by však měla být znovu zhodnocena v případě, kdy do systému někdy později přidáte další oddělení.

Toto je příklad volného přístupu k informacím. V tomto případě jsou výjimky zpracovány pomocí uživatelských profilů namísto omezování oprávnění. Sharon vyplnila část veřejné oprávnění u formuláře Popis knihovny pro knihovnu CUSTLIB (Záznamy o zákaznících).

Tabulka 41. Příklad: Formulář společnosti JKL Toy Company: Popis knihovny — část 1 (Záznamy o zákaznících)

Jméno knihovny: CUSTLIB	Popisné jméno (text): Záznamy o zákaznících
Veřejné oprávnění ke knihovně:	*USE
Veřejné oprávnění k objektům v knihovně:	*CHANGE
Veřejné oprávnění pro nové objekty (CRTAUT):	*CHANGE

Sharon Jonesová zjistila, že obsah některých dočasných souborů v knihovně Záznamy o zákaznících je mazán během zpracování aplikace Pohledávky na konci každého měsíce. Rozhodla se zpracovat oprávnění pro tyto soubory individuálně namísto toho, aby riskovala, že by mohly být náhodně vymazány další objekty v knihovně. Pro všechny další činnosti zpracování je dostatečné oprávnění *CHANGE.

Ačkoli zpracování na konci měsíce provádí několik lidí, Sharon se nedomnívala, že dočasné soubory představují bezpečnostní riziko. Rozhodla se udělit těmto souborům veřejné oprávnění *ALL namísto udělení oprávnění pouze těm lidem, kteří provádějí zpracování na konci měsíce. Níže uvedená tabulka zobrazuje druhou část formuláře Popis knihovny pro knihovnu Záznamy o zákaznících:

Tabulka 42. Příklad: Formulář společnosti JKL Toy Company: Popis knihovny — část 2 (Záznamy o zákaznících)

Vytvořte seznam specifických oprávnění pro objekty knihovny				
Skupinový nebo uživatelský profil	Jméno objektu	Typ objektu	Potřebné oprávnění	Seznam oprávnění
PUBLIC	ARFILE01	*FILE	*ALL	
PUBLIC	ARFILE02	*FILE	*ALL	
PUBLIC	ARFILE03	*FILE	*ALL	

Nyní můžete určit veřejná oprávnění pro knihovny programů.

Přidělení veřejného oprávnění knihovnám programů

Aplikační programy bývají často uloženy v samostatných knihovnách, odděleně od souborů a ostatních objektů. Není nutné, abyste používali pro programy oddělené knihovny, ale mnoho programátorů tento způsob používá při návrhu aplikace. Jestliže má aplikace oddělené knihovny programů, uvažujte o přidělení veřejných oprávnění těmto knihovnám. Můžete použít oprávnění *USE pro knihovnu i programy v této knihovně, což postačuje pro běh programů, avšak v knihovně programů mohou být další objekty, které budou vyžadovat dodatečná oprávnění. Položte programátorovi několik otázek:

- Využívá aplikace datové oblasti nebo fronty zpráv ke komunikaci mezi programy? Jsou tyto v knihovně programů? K používání datových oblastí a front zpráv je zapotřebí oprávnění *CHANGE.
- Dochází v průběhu zpracování k vymazání některých objektů, například datových oblastí? K vymazání objektu je vyžadováno oprávnění *ALL.
- Jsou některé objekty v knihovně programů, například datové oblasti, vytvářeny v průběhu zpracování? K vytvoření nových objektů v knihovně je zapotřebí oprávnění *CHANGE pro tuto knihovnu.

Vyplňte formulář Popis knihovny, kam do obou částí zapíšete veškeré informace o zabezpečení, s výjimkou vlastníka knihovny a sloupce se seznamem oprávnění. Pak můžete stanovit vlastnictví knihoven a objektů.

Můžete prostudovat následující dva příklady, kde se dozvíte, jak Sharon Jonesová stanovila oprávnění ke knihovnám programů. V prvním příkladu se Sharon Jonesová rozhodla, že pro knihovnu programů Zákaznické objednávky bude vhodný uvolněný přístup. Druhý příklad uvádí přísnější, který Sharon zvolila pro knihovnu programů Pohledávky.

Příklad: Formulář společnosti JKL Toy Company: Popis knihovny — přístup bez omezení: Sharon Jonesová zkoumala knihovnu programů Zákaznické objednávky a poznamenala si následující:

- Ke komunikaci mezi programy se používá jedna fronta zpráv - COMSGQ01.
- Obsah této fronty zpráv se maže, ale fronta samotná se nevymaže nikdy. Oprávnění *CHANGE pro tuto frontu zpráv je dostačující.

Sharon se rozhodla udělit oprávnění *USE všem objektům v knihovně programů a definovat frontu zpráv COMSGQ01 samostatně. Dvě níže uvedené tabulky zobrazují její formulář Popis knihovny pro knihovnu COPGMLIB:

Tabulka 43. Příklad: Formulář společnosti JKL Toy Company: Popis knihovny - knihovna programů

Formulář Popis knihovny	**část 1 ze 2**
Jméno knihovny: COPGMLIB	Popisné jméno (text): Knihovna programů Zákaznické objednávky
Veřejné oprávnění ke knihovně: *USE Veřejné oprávnění k objektům v knihovně: *USE Veřejné oprávnění pro nové objekty (CRTAUT): *USE Vlastník knihovny:	

Tabulka 44. Příklad: Formulář společnosti JKL Toy Company: Popis knihovny - knihovna programů

Formulář Popis knihovny				**část 2 ze 2**
Vytvořte seznam oprávnění k jednotlivým objektům v knihovně				
Skupinový nebo uživatelský profil	Jméno objektu	Typ objektu	Potřebné oprávnění	Seznamy oprávnění
PUBLIC	COMSGQ01	*MSGQ	*CHANGE	

Použití oprávnění k programu pro řízení přístupu

Ačkoli má většina zaměstnanců společnosti JKL Toy Company povoleno měnit informace o zákaznících, pouze několik lidí má povoleno nastavovat zákazníkům kreditní limity. Kreditní limity jsou uloženy v kmenovém souboru zákazníků (CUSTMAS), ale jejich hodnoty se mění v knihovně ARPGMLIB samostatným programem nazvaným ARPGM12. Sharon může omezit použití tohoto programu tak, aby program zabránil neoprávněným osobám měnit kreditní limity. Níže uvedená tabulka zobrazuje formulář Popis knihovny pro knihovnu ARPGMLIB:

Tabulka 45. Příklad: Formulář společnosti JKL Toy Company: Popis knihovny - individuální oprávnění

Formulář Popis knihovny	**část 1 ze 2**
Jméno knihovny: ARPGMLIB	Popisné jméno (text): Knihovna programů Pohledávky
Veřejné oprávnění ke knihovně: *USE Veřejné oprávnění k objektům v knihovně: *USE Veřejné oprávnění pro nové objekty (CRTAUT): *USE Vlastník knihovny:	

Tabulka 46. Příklad: Formulář společnosti JKL Toy Company: Popis knihovny - individuální oprávnění

Formulář Popis knihovny				**část 2 ze 2**
Vytvořte seznam oprávnění k jednotlivým objektům v knihovně				
Skupinový nebo uživatelský profil	Jméno objektu	Typ objektu	Potřebné oprávnění	Seznamy oprávnění
PUBLIC	ARPGM12	*PGM	*EXCLUDE	
JACOBS	ARPGM12	*PGM	*USE	
DAVISP	ARPGM12	*PGM	*USE	
SMITHJ	ARPGM12	*PGM	*USE	

Dříve než začnete určovat vlastnictví knihoven a objektů, si možná budete chtít prostudovat příklad s omezením, který používá adoptované oprávnění.

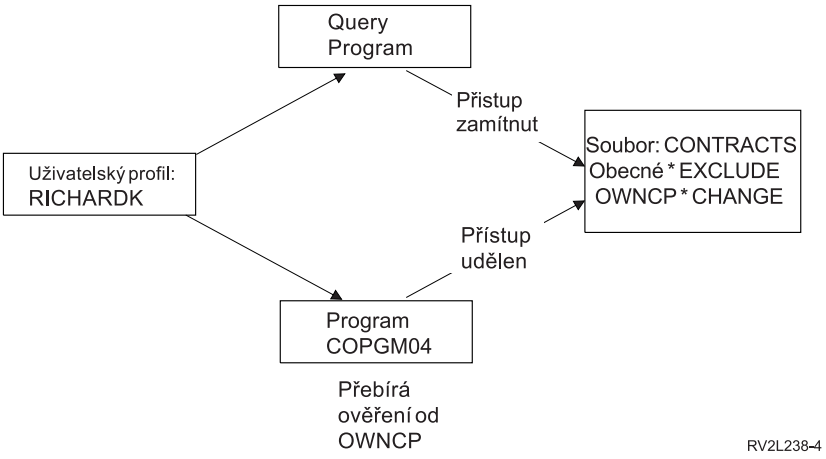
Příklad: Formulář společnosti JKL Toy Company: Popis knihovny — omezený přístup: Všechny dosavadní příklady popisovaly uvolněný přístup k zabezpečení, kdy má většina zaměstnanců přístup k informacím v knihovně. Informace o smlouvách a cenících jsou ve společnosti JKL Toy Company pokládány za důvěrné a vyžadují omezený přístup. Naštěstí jsou všechny tyto informace uloženy v samostatné knihovně. Programy pro aktualizaci smluv a ceníků jsou také ve zvláštní knihovně.

Sharon zkoumala cíle v oblasti zabezpečení pro aplikaci Smlouvy a ceníky (viz Stanovení cílů v oblasti zabezpečení prostředků). Přezkoumala také formuláře Popis aplikace a Popis knihovny. Sharon došla k závěru, že bude obtížné splnit cíle v oblasti zabezpečení pro tuto aplikaci. Udělala si několik poznámek a posoudila tento problém s dodavatelem aplikací:

- Zaměstnanci prodejního a marketingového oddělení potřebují vytvářet a měnit smlouvy. Musí používat soubory a programy.
- Zaměstnanci oddělení pro zpracování objednávek mění smlouvy a prohlížejí si ceníky nepřímo, když zadávají a odesílají objednávky, není jim však umožněno prohlížet si smlouvy a ceníky jakýmkoliv jiným způsobem. Pro vytváření svých vlastních sestav o zákaznících a objednávkách však budou používat program Query. Dostanou-li oprávnění k souborům Smlouvy a ceníky, mohli by vytvářet programy Query, aby si mohli prohlížet a tisknout smlouvy a ceník.

Dodavatel aplikací pro společnost JKL Toy Company navrhl jako řešení použít zabezpečovací funkci adoptovaného oprávnění. Funkce **adoptované oprávnění** umožňuje uživateli adoptovat během provádění programu oprávnění vlastníka programu. Uživatel nepotřebuje oprávnění k objektu.

Níže uvedený diagram zobrazuje příklad toho, jak adoptované oprávnění funguje. Karen Richardsová (RICHARDK) z oddělení pro zpracování objednávek nemá obvykle oprávnění pro použití souboru Smlouvy. Když však zadává objednávky, potřebuje zkontrolovat a aktualizovat saldo účtu. Vstupní program pro zadávání objednávek, který pracuje se smluvními saldy (COPGM04), převezme oprávnění profilu OWNCP. Když bude Karen provádět program COPGM04, bude mít oprávnění pro použití souboru se smlouvami:



V tématu ″Určení vlastnictví knihoven a objektů″ najdete podrobnosti o vlastnictví objektů. Dodavatel aplikací nebo programátor mohou při vytváření (kompilování) programu určit, aby program převzal oprávnění vlastníka. Programátor může také specifikovat adoptované oprávnění pro program, který používá příkaz CHGPGM (Změna programu). Před použitím tohoto postupu se ujistěte se, že rozumíte všem funkcím programu.

Sharon se rozhodla použít funkci adoptovaného oprávnění, aby umožnila osobám mimo prodejní a marketingové oddělení přístup k souborů Smlouvy a ceníky. Určila také, že přístup *CHANGE je dostatečný pro všechny objekty používané aplikací Smlouvy a ceníky. Níže uvedená tabulka zobrazuje formulář Popis knihovny pro knihovnu CONTRACTS:

Tabulka 47. Příklad: Formulář společnosti JKL Toy Company: Popis knihovny - omezené oprávnění

Formulář Popis knihovny	**část 1 ze 2**
Jméno knihovny: CONTRACTS	Popisné jméno (text): Knihovna Smlouvy a ceníky
Veřejné oprávnění ke knihovně: *EXCLUDE Veřejné oprávnění k objektům v knihovně: *CHANGE Veřejné oprávnění pro nové objekty (CRTAUT): *CHANGE Vlastník knihovny:	

Tabulka 48. Příklad: Formulář společnosti JKL Toy Company: Popis knihovny - omezené oprávnění

Formulář Popis knihovny				**část 2 ze 2**
Vytvořte seznam oprávnění k jednotlivým objektům v knihovně				
Skupinový nebo uživatelský profil	Jméno objektu	Typ objektu	Potřebné oprávnění	Seznamy oprávnění
DPTSM	CONTRACTS	*LIB	*USE	
DPTMG	CONTRACTS	*LIB	*USE	

Nemusíte omezovat oprávnění k objektům v knihovně, protože jste omezili přístup ke knihovně samotné. Sharon udělila oprávnění také vedoucím pracovníkům a zaměstnancům prodejního a marketingového oddělení. Namísto udělování oprávnění každému zaměstnanci oddělení použila skupinové oprávnění.

Poznámka: Zkušený programátor, který má přístup ke knihovně, možná bude schopen ponechat si přístup k objektům v knihovně i poté, co jste odvolali oprávnění ke knihovně. Obsahuje-li knihovna objekty s vysokými požadavky na zabezpečení, omezte přístup k objektům a knihovně na úplnou ochranu.

Dříve, než začnete s určováním vlastnictví knihoven a objektů, si možná budete chtít prostudovat příklad neomezeného přístupu.

Určení vlastnictví knihoven a objektů

Po naplánování zabezpečení knihoven aplikací můžete rozhodnout o vlastnictví knihoven a objektů. Každému objektu je při vytvoření přiřazen vlastník. Vlastník objektu má k objektu automaticky všechna oprávnění; patří k nim právo k poskytování oprávnění ostatním k používání objektu, právo ke změnám objektu a k vymazání objektu. Správce systému může tyto činnosti provádět pro libovolný objekt v systému.

Systém používá ke sledování toho, kdo má k objektu oprávnění, profil vlastníka objektu. Tuto činnost provádí systém interně. Nemusí to mít vliv přímo na uživatelský profil. Pokud však správně nenaplánujete vlastnictví objektů, mohou být některé uživatelské profily velmi velké.

Systém při uložení objektu uloží zároveň jméno profilu vlastníka. Systém využívá tyto informace při obnovování objektu. Pokud profil vlastníka obnovovaného objektu není v systému, přenese systém vlastnictví na profil dodaný IBM nazvaný QDFTOWN.

Doporučení

Následující doporučení platí v mnoha situacích, ne však vždy. Postupujte nejprve podle těchto doporučení a pak projednejte své názory na vlastnictví objektů s programátorem nebo dodavatelem aplikací. Koupíte-li aplikace, pravděpodobně nebudete moci ovlivnit, který profil bude vlastníkem knihoven a objektů. Aplikace bývají navrženy tak, aby bránily změnám vlastnictví.

- Nepoužívejte jako vlastníka aplikace profil dodaný IBM, například QSECOFR nebo QPGMR. Tyto profily vlastní mnoho objektů v knihovnách dodaných IBM a jsou samy o sobě velmi velké.
- Skupinový profil by normálně neměl být vlastníkem aplikace. Každý člen skupiny má stejná oprávnění jako skupinový profil, pokud mu výslovně nepřidělíte menší oprávnění. Takto byste tedy každému členu skupiny udělili úplná oprávnění k aplikaci.
- Plánujete-li přenést odpovědnost za řízení aplikací na vedoucí různých oddělení, mohou být tito vedoucí vlastníky všech aplikačních objektů. Odpovědnost vedoucích (správců aplikací) se však mohou měnit. Dojde-li k tomu, měli byste přenést vlastnictví všech aplikačních objektů na nového vedoucího.
- Často se používá metoda, při které se pro každou aplikaci vytvoří speciální profil vlastníka s heslem nastaveným na *NONE. Systém používá profil vlastníka ke správě oprávnění k aplikaci. Samotnou správu aplikace provádí správce systému (nebo uživatel s oprávněními správce systému) nebo pověří touto činností vedoucí pracovníky, kteří mají ke konkrétním aplikacím oprávnění *ALL.

Rozhodněte, které profily budou vlastníky aplikací. Zadejte informace o profilu vlastníka na každý formulář Popis knihovny.

Dříve než budete rozhodovat o vlastnictví uživatelských knihoven a přístupu k nim, měli byste se seznámit s příkladem, jak určili vlastnictví aplikací ve společnosti JKL Toy Company.

Příklad: Vlastnictví aplikací ve společnosti JKL Toy Company

Sharon Jonesová se rozhodla vytvořit zvláštní uživatelský profil pro každou aplikaci. Společně s Kenem Harrisonem, zástupcem správce systému, budou odpovědní za správu zabezpečení aplikací. Když se později stanou požadavky společnosti na zabezpečení složitější, může Sharon převést určitou odpovědnost za správu oprávnění na vedoucí pracovníky oddělení.

Sharon přidala nový záznam do formuláře Konvence pojmenování:

Tabulka 49. Formulář společnosti JKL Toy Company Konvence pojmenování: Profil vlastníka

Typ objektu	Konvence pojmenování
Profil vlastníka	Profil vlastníka je třeba vytvořit pro každou aplikaci. Bude obsahovat všechny knihovny aplikací a objekty v knihovnách. Profil vlastníka bude mít jméno OWN plus zkratku aplikace. Profil vlastníka Řízení zásob bude mít zkratku OWNIC.

Sharon se rozhodla začít jméno profilu vlastníka písmeny OWN, aby se všechny profily vlastníků zobrazily společně na obrazovkách a seznamech.

Sharon přiřadila vlastníky ke všem knihovnám aplikací a zadala tyto informace do formulářů Konvence pojmenování. Jedinou knihovnou, která má více než jednoho možného vlastníka aplikace, je knihovna Záznamy o zákaznících. Jelikož je aplikace Pohledávky používána pro vytváření nových zákazníků a nastavování kreditních limitů, Sharon se rozhodla, že by by tato aplikace měla vlastnit zákaznické soubor. Toto jsou vlastníci, které Sharon přiřadila:

Jméno knihovny	Jméno vlastníka
ICPGMLIB	OWNIC
ITEMLIB	OWNIC
CONTRACTS	OWNCP
CPPGMLIB	OWNCP
COPGMLIB	OWNCO
CUSTLIB	OWNAR
ARPGMLIB	OWNAR

Nyní můžete určit vlastnictví a přístup pro uživatelské knihovny.

Rozhodnutí o vlastnictví a přístupu k uživatelským knihovnám

Pokud je ve vašem systému licencovaný program IBM Query for iSeries, nebo jiný program pro podporu rozhodování, potřebují uživatelé knihovnu, do které budou ukládat programy Query, které vytvoří. Normálně je touto knihovnou **aktuální knihovna** v uživatelském profilu. Další informace o vytvoření aktuální knihovny pro každého uživatele najdete v tématu Výběr hodnot ovlivňujících přihlášení do systému. Sharon Jonesová plánuje, že aktuální knihovny bude používat oddělení prodeje a marketingu a ostatní oddělení budou používat skupinové knihovny.

- Pracovníci oddělení prodeje a marketingu budou častými uživateli produktu Query. Každý uživatel by měl mít vlastní (soukromou) knihovnu. Jinak by měli starosti, jak své dotazy pojmenovat, a mohli by neúmyslně vymazat programy Query jiných uživatelů.
- Ostatní oddělení budou mít pro začátek skupinové knihovny. Pokud vytvoří mnoho programů Query, je možné uvažovat o individuálních knihovnách.

Patří-li uživatel do určité skupiny, je možné pomocí pole v uživatelském profilu definovat, zda uživatel nebo skupina vlastní nějaké objekty vytvořené uživatelem. Pokud je uživatel vlastníkem objektů, lze nastavit, jaká oprávnění mají

členové skupiny k používání těchto objektů. Také lze zadat, zda oprávnění skupiny je primární skupinové oprávnění nebo soukromé oprávnění. Primární skupinové oprávnění může vést k lepší výkonnosti systému. Sharon si k uživatelským knihovnám udělala pár poznámek:

- Pracovníci oddělení prodeje a marketingu by měli vlastnit objekty, které vytvoří, místo aby byly tyto objekty ve skupinovém vlastnictví. Nemusí mít možnost vzájemně měnit dotazovací programy vytvořené jinými uživateli.
- Každý člen skupiny by měl mít možnost spouštět programy Query vytvořené ostatními členy, což znamená, že skupina získá oprávnění *USE ke všem objektům vytvořeným libovolným členem skupiny.
- Oprávnění skupiny by mělo být primárním skupinovým oprávněním.
- Veřejnost by neměla mít k těmto knihovnám přístup. Pracovníci oddělení prodeje a marketingu mohou vytvářet výstupní soubory svých dotazů. Tyto soubory mohou obsahovat důvěrná data.
- U ostatních oddělení bude vlastníkem skupinové knihovny a všech objektů vytvořených v knihovně celá skupina. Znamená to, že každý člen skupiny může v knihovně cokoli měnit a mazat. Bude-li to přinášet problémy, je možné zvolit jinou metodu.

Následující tabulka obsahuje Profil individuálního uživatele pro oddělení prodeje a marketingu, které používá objekty ve vlastnictví uživatele:

Tabulka 50. Příklad: Formulář společnosti JKL Toy Company: Profil individuálního uživatele - objekty vlastněné uživatelem

Jména skupinových profilů: DPTSM	
Vlastník vytvořených objektů: *USRPRF	Skupinové oprávnění k vytvořeným objektům: *USE
Typ skupinového oprávnění: *PGP	

Následující tabulka obsahuje formulář Profil individuálního uživatele pro oddělení, které má objekty ve vlastnictví skupiny:

Tabulka 51. Příklad: Formulář společnosti JKL Toy Company: Profil individuálního uživatele - objekty vlastněné skupinou

Jména skupinových profilů: DPTxx	
Vlastník vytvořených objektů: *GRPPRF	Skupinové oprávnění k vytvořeným objektům:

Pokud je vlastníkem vytvořených objektů skupina, pole **Skupinové oprávnění k vytvořeným objektům** se nepoužije. Členové skupiny mají ke všem vytvořeným objektům automaticky oprávnění *ALL.

Rozhodněte, kdo má být vlastníkem uživatelských knihoven a kdo k nim má mít přístup. Zadejte své volby do polí **Vlastník vytvořených objektů** a **Skupinové oprávnění k objektům** ve formuláři Profil individuálního uživatele. Nyní jste připraveni začít seskupovat objekty.

Seskupování objektů

Po určení vlastnictví knihoven a objektů můžete začít v systému seskupovat objekty. Správu oprávnění můžete zjednodušit používáním seznamů oprávnění, do kterých seskupíte objekty se stejnými požadavky. Místo abyste udělovali oprávnění jednotlivým objektům ze seznamu, můžete celému seznamu udělit veřejná oprávnění, oprávnění skupinových profilů a uživatelských profilů. Systém zachází se všemi objekty, které zabezpečíte pomocí seznamu oprávnění, stejným způsobem. K celému seznamu však můžete dát různým uživatelům různá oprávnění.

Seznamy oprávnění usnadňují opětovné nastavení oprávnění při obnovování objektů. Zabezpečíte-li objekty pomocí seznamu oprávnění, budou během procesu obnovení objekty automaticky propojeny se seznamem.

Skupině nebo uživateli lze udělit oprávnění ke správě seznamu oprávnění (*AUTLMGT). Správa seznamu oprávnění umožňuje uživateli přidávat do seznamu další uživatele, měnit oprávnění jiných uživatelů v seznamu a odstraňovat uživatele ze seznamu.

Doporučení

- Seznamy oprávnění používejte pro objekty, které vyžadují bezpečnostní ochranu a které mají podobné požadavky na zabezpečení. Používání seznamů oprávnění podporuje plánování na úrovni kategorií oprávnění místo na úrovni individuálních oprávnění. Seznamy oprávnění také usnadňují obnovování objektů a monitorování oprávnění v systému.
- Vyvarujte se složitých schémat, která kombinují seznamy oprávnění, skupinová oprávnění a individuální oprávnění. Zvolte metodu, která nejlépe vyhovuje požadavkům, místo abyste současně používali všechny metody.

Rovněž bude třeba, abyste přidali konvence pojmenování seznamů oprávnění do formuláře Konvence pojmenování.

Až připravíte formulář Seznam oprávnění, vraťte se a přidejte tyto informace do formuláře Popis knihovny. Seznamy oprávnění možná již vytvořil programátor nebo dodavatel aplikací. Obraťte se na ně.

Dříve než budete plánovat zabezpečení tiskáren a tiskových výstupů, byste se měli seznámit s příkladem, jak seznamy oprávnění naplánovala Sharon Jonesová z firmy JKL Toy Company.

Příklad: Formulář společnosti JKL Toy Company: Seznam oprávnění

Sharon přezkoumala formulář Popis knihovny pro knihovnu Záznamy o zákaznících a rozhodla se vytvořit seznam oprávnění pro soubory, jejichž obsah je mazán na konci každého měsíce. Přestože se maže obsah pouze tří souborů, Sharon se rozhodla použít seznam oprávnění, aby zjednodušila správu oprávnění. Pokud budou do zpracování na konci měsíce později zahrnuty další soubory, může jednoduše zabezpečit tyto soubory pomocí seznamu oprávnění. Sharon se rozhodla omezit veřejnosti přístup k souborům, aby zabránila nepředvídaným problémům během zpracování na konci měsíce. Udělila oprávnění*ALL pouze těm uživatelům, kteří provádějí zpracování. Rose Willisová, systémová operátorka druhé směny, bude možná potřebovat prohlížet si informace o souborech, aby mohla kontrolovat zpracování na konci měsíce. K tomu potřebuje oprávnění *USE.

Níže uvedená tabulka zobrazuje konvence pojmenování, které Sharon použila pro seznamy oprávnění:

Tabulka 52. Příklad: Formulář společnosti JKL Toy Company: Konvence pojmenování - seznam oprávnění

Formulář Konvence pojmenování	
Zhotovila: Sharon Jonesová	Datum: 9/5/99
Typ objektu	**Konvence pojmenování**
Seznamy oprávnění	Pro seznamy, které zabezpečují objekty z jedné knihovny, použijte část jména knihovny plus písmena LST a číslo. Jméno seznamu pro objekty v knihovně CUSTLIB by bylo CUSTLST1. Pro seznam zabezpečující objekty z více než jedné knihovny použijte v případě možnosti zkratku aplikace: ARLST1. Používá-li se seznam pro několik aplikací, vyberte nějaké smysluplné jméno. Popis seznamu by měl vyjadřovat hlavní účel.

Níže uvedená tabulka zobrazuje formulář Seznam oprávnění pro knihovnu CUSTLIB. Sharon připravila tento formulář s použitím informací z formuláře Popis knihovny:

Tabulka 53. Příklad: Formulář společnosti JKL Toy Company: Seznam oprávnění

Formulář Seznam oprávnění					
Jméno seznamu oprávnění: CUSTLST1					
Popis: Soubory, jejichž obsah se maže během zpracování na konci měsíce.					
Vytvořte seznam objektů, které jsou zabezpečovány seznamem oprávnění.					
Jméno objektu	Typ objektu	Knihovna objektu	Jméno objektu	Typ objektu	Knihovna objektu
ARFILE01	*FILE	CUSTLIB	ARFFILE02	*FILE	CUSTLIB
ARFILE03	*FILE	CUSTLIB			
Vytvořte seznam skupin a uživatelů, kteří mají přístup k seznamu oprávnění.					

Tabulka 53. Příklad: Formulář společnosti JKL Toy Company: Seznam oprávnění (pokračování)

Skupina nebo uživatel	Typ povoleného přístupu	Správa seznamu?	Skupina nebo uživatel	Typ povoleného přístupu	Správa seznamu?
PUBLIC	*EXCLUDE	ne	ROSSG	*ALL	ne
SMITHJ	*ALL	ne	JONESS	*ALL	ano
WILLISR	*USE	ne			

Sharon přidala informace o seznamu oprávnění také do formuláře Popis knihovny pro knihovnu CUSTLIB:

Formulář Popis knihovny				část 2 ze 2
Zhotovila: Sharon Jonesová			Datum: 9/9/99	
Jméno knihovny: CUSTLIB				
Vytvořte seznam specifických oprávnění pro objekty knihovny				
Skupinový nebo uživatelský profil	Jméno objektu	Typ objektu	Potřebné oprávnění	Seznam oprávnění
PUBLIC	ARFILE01	*FILE	*AUTL	CUSTLST1
PUBLIC	ARFILE02	*FILE	*AUTL	CUSTLST1
PUBLIC	ARFILE03	*FILE	*AUTL	CUSTLST1

Všimněte si, že k tomu, aby mohl systém učit veřejné oprávnění, musí být veřejné oprávnění pro každý soubor změněno na *AUTL.

Prohlédněte si skupinová a individuální oprávnění ve formulářích Popis knihovny. Rozhodněte, zda je vhodné použít seznamy oprávnění. Pokud ano, připravte si formuláře Seznam oprávnění a doplňte formuláře Popis knihovny o informace ze seznamů oprávnění. Potom můžete začít plánovat zabezpečení tiskáren a tiskového výstupu.

Plánování zabezpečení tiskáren a tiskových výstupů

Po seskupení objektů je třeba naplánovat ochranu tiskového výstupu. Vytvořili jste plán ochrany informací uložených v systému. Potřebujete také plán, jak chránit důvěrné informace při tisku nebo čekání na tisk. Podívejte se na formulář Plánování fyzického zabezpečení, který vaše firma používá pro důvěrné výstupy.

Spustíte-li program, který tiskne nějakou sestavu, nejde tato sestava obvykle přímo do tiskárny. Program vytvoří kopii sestavy, nazývanou **soubor pro souběžný tisk** neboli **tiskový výstup**. Systém uloží soubor pro souběžný tisk v objektu nazvaném **výstupní fronta**, kde tento soubor čeká, až bude tiskárna k dispozici. Jestliže výstupní fronta obsahuje tiskový výstup, můžete si sestavu prohlédnout v pracovní stanici. Tisk sestavy můžete pozastavit nebo jej přesměrovat na určitou tiskárnu.

Souběžný tisk usnadňuje plánování tiskových úloh a sdílení tiskáren. Souběžný tisk také pomáhá chránit důvěrné výstupy. Můžete vytvořit jednu nebo více zvláštních výstupních front, které budou určeny k uchování důvěrných výstupů a k omezení uživatelů, kteří budou moci prohlížet a spravovat tyto výstupní fronty. Také můžete řídit, kdy bude důvěrný výstup odeslán z fronty do tiskárny.

Jak budete postupovat tímto tématem, vyplňujte formulář Zabezpečení výstupních front a pracovních stanic.

Vytvoříte-li zvláštní výstupní frontu, můžete zadat několik parametrů, které se týkají zabezpečení:

- **Parametr DSPDTA (Display Data)**: Parametr DSPDTA výstupní fronty určuje, zda nějaký uživatel může zobrazit, odeslat nebo kopírovat soubor pro souběžný tisk, jehož vlastníkem je jiný uživatel.
- **Parametr AUTCHK (Authority to Check)**: Parametr AUTCHK výstupní fronty určuje, zda nějaký uživatel může změnit nebo vymazat soubor pro souběžný tisk, jehož vlastníkem je jiný uživatel.

- **Parametr OPRCTL (Operator Control)**: Parametr OPRCTL výstupní fronty určuje, zda je uživatelům se zvláštním oprávněním *JOBCTL (nebo s třídou uživatele *SYSOPR) dovoleno řídit výstupní frontu.

Parametry výstupní fronty, oprávnění uživatele k výstupní frontě a zvláštní oprávnění uživatele společně určují činnosti, které může uživatel provádět se soubory pro souběžný tisk ve výstupní frontě. Následující tabulka ukazuje, jaké kombinace dovolují uživatelům provádět různé operace:

Tiskové operace	Parametry výstupní fronty			Oprávnění k výstupní frontě	Zvláštní oprávnění
	DSPDTA	AUTCHK	OPRCTL		
Přidání souboru pro souběžný tisk do fronty [1]	Libovolný	Libovolný	Libovolný	*READ	Žádné
	Libovolný	Libovolný	*Yes	Libovolné	*JOBCTL
Zobrazení seznamu souborů pro souběžný tisk (příkazem WRKOUTQ)[2]	Libovolný	Libovolný	Libovolný	*READ	Žádné
	Libovolný	Libovolný	*Yes	Libovolné	*JOBCTL
Zobrazení, kopírování nebo odeslání souborů pro souběžný tisk (DSPSPLF, CPYSPFL, SNDNETSPLF, SNTCPSPLF)[2]	*YES	Libovolný	Libovolný	*READ	Žádné
	*NO	*DTAAUT	Libovolný	*CHANGE	Žádné
	*NO	*OWNER	Libovolný	Vlastník[3]	Žádné
	*YES	Libovolný	*Yes	Libovolné	*JOBCTL
	*NO	Libovolný	*Yes	Libovolné	*JOBCTL
	*OWNER[5]	Libovolný	Libovolný	Libovolné	Libovolné
Změny, vymazání, pozastavení, uvolnění souboru pro souběžný tisk (CHGSPLFA, DLTSPLF, HLDSPLF, RLSSPLF)[2]	Libovolný	*DTAAUT	Libovolný	*CHANGE	Žádné
	Libovolný	*OWNER	Libovolný	Vlastník[3]	Žádné
Změny, vyčištění, pozastavení a uvolnění výstupní fronty (CHGOUTQ, CLROUTO, HLDOUTQ, RLSOUT)[2]	Libovolný	*DTAAUT	Libovolný	*CHANGE	Žádné
	Libovolný	*OWNER	Libovolný	Vlastník[3]	Žádné
	Libovolný	Libovolný	*YES	Libovolné	*JOBCTL
Spuštění zapisovacího programu fronty (STRPRTWTR, STRRMTWTR)[2]	Libovolný	*DTAAUT	*Libovolný	*CHANGE[4]	Žádné
	Libovolný	Libovolný	*YES	Libovolné[4]	*JOBCTL

1 Toto oprávnění je nutné ke směrování výstupu do výstupní fronty.

2 Pomocí těchto příkazů nebo ekvivalentních voleb obrazovky.

3 Musíte být vlastníkem výstupní fronty.

4 Vyžaduje také oprávnění *USE k popisu tiskového zařízení.

5 Chcete-li použít tento příkaz, musíte být vlastníkem souboru pro souběžný tisk nebo mít zvláštní oprávnění *SPLCTL.

Přezkoumejte ve formuláři Plánování fyzického zabezpečení část věnovanou tiskárnám. Jak budete postupovat tímto tématem, vyplňujte část formuláře Zabezpečení výstupních front a pracovních stanic zaměřenou na výstupní fronty.

Dříve než začnete plánovat zabezpečení prostředků pracovních stanic, byste se měli seznámit s příkladem, jak hodnoty těchto parametrů výstupní fronty stanovila Sharon Jonesová z firmy JKL Toy Company.

Příklad: Formulář společnosti JKL Toy Company: Zabezpečení výstupních front a pracovních stanic — výstupní fronta

Prodejní a marketingové oddělení společnosti JKL Toy Company má dva požadavky na důvěrný tisk:

- Když se plánují změny cen, tisknou se předběžné ceníky. Tyto informace nemůže vidět nikdo mimo oddělení prodeje a marketingu, s výjimkou vedoucích pracovníků společnosti.
- Během vyjednávání jsou důvěrné také smlouvy. Z oddělení prodeje a marketingu může stručný návrh smlouvy vidět pouze osoba, která o smlouvě jedná.

Sharon se rozhodla, že vytvoří dvě zvláštní výstupní fronty:

PRICEQ

Použije se pro předběžné ceníky. Kdokoliv z oddělení prodeje a marketingu může provádět jakékoliv funkce v této výstupní frontě. Výstupní frontu nemůže použít nikdo mimo toto oddělení, včetně systémových operátorů. Výstupní fronta PRICEQ se nachází v knihovně CONTRACTS.

NEWCP

Používá se pro tisk smluv, o kterých se právě jedná. Výstupní frontu sdílí zaměstnanci oddělení prodeje a marketingu, ale tento soubor může spravovat pouze osoba, která vytváří soubor pro souběžný tisk na výstupní frontě. Výstupní fronta NEWCP je umístěna v knihovně CONTRACTS.

Níže uvedená tabulka zobrazuje formulář Zabezpečení výstupních front a pracovních stanic, který Sharon připravila pro tyto výstupní fronty:

Tabulka 54. Formulář společnosti JKL Toy Company: Zabezpečení výstupních front a pracovních stanic - výstupní fronta

Vytvořte seznam parametrů pro vyhrazené výstupní fronty:				
Jméno výstupní fronty	Knihovna výstupní fronty	Zobrazit libovolný soubor (DSPDTA)	Oprávnění, které má být zkontrolováno (AUTCHK)	Řízení operátorem (OPRCTL)
PRICEQ	CONTRACTS	*YES	*DTAAUT	*NO
NEWCP	CONTRACTS	*NO	*OWNER	*NO

Téma Určení veřejného oprávnění ke knihovnám programů obsahuje příklad, který popisuje oprávnění pro knihovnu CONTRACTS ve společnosti JKL Toy Company. K této knihovně mají přístup pouze vedoucí pracovníci a zaměstnanci oddělení prodeje a marketingu. Veřejné oprávnění pro objekty v knihovně (včetně těchto výstupních front) je *CHANGE.

Jelikož parametr AUTCHK má na výstupní frontě NEWCP hodnotu *OWNER, může s tímto souborem pracovat pouze vlastník souboru pro souběžný tisk (viz výše uvedená tabulka Požadované oprávnění pro provádění tiskových funkcí). Tím se zabrání zaměstnancům oddělení prodeje a marketingu tisknout cizí smlouvy nebo si je prohlížet ve výstupní frontě.

Jakmile naplánujete zabezpečení výstupní fronty, můžete začít plánovat zabezpečení pracovní stanice..

Plánování zabezpečení pracovních stanic

Po naplánování zabezpečení prostředků můžete začít plánovat zabezpečení pracovních stanic. Ve formuláři Plánování fyzického zabezpečení jste uvedli pracovní stanice, které představují bezpečnostní riziko z důvodu jejich umístění. Pomocí těchto informací určete, které pracovní stanice je třeba omezit.

Uživatele, kteří tyto pracovní stanice budou používat, byste měli nabádat, aby byli pozorní, pokud jde o bezpečnost. Měli by se odhlásit ze systému, kdykoliv pracovní stanici opustí. Své rozhodnutí o postupech odhlašování u zranitelných pracovních stanic byste měli zaznamenat do své strategie zabezpečení. Chcete-li minimalizovat rizika, můžete omezit funkce, které lze na těchto pracovních stanicích provádět.

Nejjednodušší metodou, jak na pracovní stanici omezit funkce, je vyhradit ji pouze pro uživatelské profily s omezenou funkcí. Tuto techniku použila Sharon Jonesová v oddělení skladu firmy JKL Toy Company. Sharon povolila uživatelkám Ray Wagnerové a Janice Amesové, které pracují v nakládacím prostoru, aby mohly spouštět pouze program pro příjem zboží. Sharon také nastavila, aby obě byly jedinými uživateli, kterým je povoleno přihlásit se na pracovní stanici v nakládacím prostoru.

Máte-li oprávnění správce systému nebo servisní oprávnění, můžete zabránit přihlašování uživatelů u libovolné pracovní stanice. Pokud k tomuto účelu použijete systémovou hodnotu QLMTSECOFR, budou se uživatelé s oprávněním správce systému moci přihlašovat pouze na určitých autorizovaných pracovních stanicích.

Vyplňte část formuláře Zabezpečení výstupních front a pracovních stanic, která je zaměřena na pracovní stanice.

Při vyplňování části formuláře Zabezpečení výstupních front a pracovních stanic, která je zaměřena na pracovní stanice, byste se měli seznámit s příkladem, jak zabezpečení pracovních stanic naplánovala Sharon. Dále byste si měli projít seznam doporučení k zabezpečení prostředků, abyste zajistili, že váš plán zabezpečení prostředků bude jednoduchý a úplný. Po shlédnutí příkladu a doporučení můžete začít plánovat instalaci aplikací.

Příklad: Formulář společnosti JKL Toy Company: Zabezpečení výstupních front a pracovních stanic — pracovní stanice

Sharon Jonesová prozkoumala plán fyzického zabezpečení, aby zjistila, které pracovní stanice představují bezpečnostní riziko. Ve společnosti JKL Toy Company mají například lidé mimo společnost snadný přístup k pracovním stanicím v nakládacím prostoru a ve vzdálených prodejních kancelářích. Sharon došla v plánu fyzického zabezpečení k závěru, že tyto pracovní stanice představují potenciální bezpečnostní rizika.

Nejjednodušší metodou, jak na pracovní stanici omezit funkce, je vyhradit ji pouze pro uživatelské profily s omezenou funkcí. Tuto techniku použila Sharon Jonesová v oddělení skladu firmy JKL Toy Company. Sharon povolila uživatelkám Ray Wagnerové a Janice Amesové, které pracují v nakládacím prostoru, aby mohly spouštět pouze program pro příjem zboží. Sharon také nastavila, aby obě byly jedinými uživateli, kterým je povoleno přihlásit se na pracovní stanici v nakládacím prostoru.

Sharon přehodnotila svůj výběr pro systémovou hodnotu QLMTSECOFR. Rozhodla se ji nastavit na 1 (YES) jako dodatečnou ochranu pro odposlechnutelné pracovní stanice v nakládacím prostoru.

Níže uvedená tabulka zobrazuje část pro pracovní stanici formuláře Zabezpečení výstupních front a pracovních stanic, kterou Sharon připravila:

Tabulka 55. Formulář společnosti JKL Toy Company Zabezpečení výstupních front a pracovních stanic - pracovní stanice

Pracovní stanice správce systému: Pokud omezíte přístup správce systému pouze na některé pracovní stanice (systémová hodnota QLMTSECOFR je YES), vytvořte seznam pracovních stanic, ke kterým má oprávnění správce systému a jakákoliv jiná osoba s oprávněním *ALLOBJ: Všechny pracovní stanice kromě níže uvedených.	
Vytvořte seznam oprávnění pro vyhrazené pracovní stanice:	
Jméno pracovní stanice	Skupiny nebo uživatelé, kterým bylo poskytnuto oprávnění (oprávnění *CHANGE)
DSP10	AMESJ, WAGNERR
DSP11	AMESJ, WAGNERR
RMT01	UNGERJ, BELLB
RMT02	UNGERJ, BELLB

Měli byste si prostudovat přehled doporučení pro zabezpečení prostředků. Pak můžete začít s plánováním instalace aplikací.

Souhrn doporučení k zabezpečení prostředků

Poté, naplánujete zabezpečení pracovních stanic, si můžete prostudovat následující doporučení týkající se zabezpečení prostředků. Systém iSeries nabízí mnoho možností ochrany zde uložených informací. Díky tomu můžete navrhnout plán zabezpečení prostředků tak, aby co nejlépe vyhovoval vaší firmě. Takové množství možností však také může být matoucí.

V tomto tématu byl na příkladu firmy JKL Toy Company ukázán základní přístup k plánování zabezpečení prostředků, který se řídil níže uvedenými pokyny:

- Postupujte od obecného ke konkrétnímu:
  - Naplánujte zabezpečení knihoven. Jednotlivými objekty se zabývejte, jen je-li to nutné.

– Nejdříve naplánujte veřejná oprávnění, potom skupinová oprávnění a nakonec individuální oprávnění.

- Abyste zlepšili výkonnost a zjednodušili zálohování a obnovu, definujte specifické zabezpečení pouze u objektů, jejichž požadavky na zabezpečení nelze uspokojit pomocí veřejných oprávnění.
- Nastavte stejná veřejná oprávnění pro nové objekty v knihovně (CRTAUT) jako veřejná oprávnění, která jste definovali pro většinu stávajících objektů v knihovně.
- Snažte se neudělovat skupinám a jednotlivcům menší oprávnění, než mají uživatelé s veřejným oprávněním. Snižuje to výkon, může to vést k pozdějším chybám a komplikuje se tím prověřování. Víte-li, že každý uživatel má k objektům alespoň takové oprávnění jako uživatelé s veřejným oprávněním, usnadníte si tím plánování a prověřování zabezpečení.
- Objekty se stejnými požadavky na zabezpečení seskupujte do seznamů oprávnění. Správa seznamů oprávnění je jednodušší než správa individuálních oprávnění; seznamy oprávnění navíc pomáhají při obnově informací o zabezpečení.
- Jako vlastníky aplikací vytvořte zvláštní uživatelské profily. Nastavte heslo vlastníka na *NONE.
- Vyvarujte se toho, aby vlastníkem aplikací byly profily dodané IBM, například QSECOFR nebo QPGMR.
- Pro důvěrné sestavy používejte zvláštní výstupní fronty. Výstupní frontu umístěte do stejné knihovny jako důvěrné informace.
- Omezte počet uživatelů s oprávněními správce systému.
- Při udělování oprávnění *ALL k objektům a knihovnám buďte opatrní. Uživatelé s oprávněním *ALL mohou neúmyslně vymazat důležité objekty.

K úspěšnému naplánování nastavení zabezpečení prostředků jste měli provést tyto operace shromažďování informací:

- Vyplnit pro všechny knihovny aplikací část 1 a část 2 formuláře Popis knihovny.
- Ve formulářích Profil individuálního uživatele vyplnit pole **Vlastník vytvořených objektů** a **Skupinové oprávnění k objektům**.
- Ve formuláři Konvence pojmenování popsat své plány, pokud jde o pojmenování seznamů oprávnění.
- Připravit formuláře Seznam oprávnění.
- Přidat do formulářů Popis knihovny informace o seznamech oprávnění.
- Připravit formulář Zabezpečení výstupních front a pracovních stanic.

Nyní jste připraveni k plánování instalace aplikací.

Plánování instalace aplikací

K tomu, aby bylo možné dokončit plánování zabezpečení prostředků, je třeba připravit se na instalaci aplikací. Následující témata vám pomohou naplánovat vlastnictví a oprávnění k aplikacím po instalaci těchto aplikací. Zde popsané metody nemusí fungovat u všech aplikací. Chcete-li vytvořit kvalitní plán instalace, přizvěte si k tomu programátora nebo dodavatele aplikací.

Máte-li v úmyslu získat aplikaci od dodavatele aplikací, použijte tyto informace k naplánování zabezpečovacích činností, které budete muset provést před zavedením knihoven aplikací a po jejich zavedení.

Zamýšlíte-li nainstalovat aplikaci, kterou programátoři vyvinuli přímo ve vašem systému, použijte tyto informace k plánování zabezpečovacích činností, které budete muset provést kvůli přenesení aplikace z testovacího prostředí do provozního prostředí.

Proveďte jednotlivé kroky pro jednu aplikaci. Pak se vraťte a vyplňte formuláře Instalace aplikace pro všechny další aplikace.

Jaké formuláře použít?

Udělejte si kopie následujících formulářů a při procházení tímto tématem je vyplňte:

Tabulka 56. Formuláře potřebné k plánování instalace aplikací

Jméno formuláře	Potřebný počet kopií
Formulář Instalace aplikace	jedna kopie na aplikaci

Použijte tyto formuláře, na kterých jste pracovali dříve, když jste shromažďovali informace pro plánování instalace aplikací:

Jméno formuláře	Připravený v tématu:
Formulář Popis knihovny	Popis informací o knihovnách
Seznam oprávnění	Seskupování objektů

V tématu o zavádění aplikací se seznámíte s kroky potřebnými k instalaci aplikací.

Kvůli plánování instalace aplikací byste se měli seznámit s těmito tématy:

- Určení uživatelských profilů a instalačních hodnot pro aplikace.
- Provádění změn instalačních hodnot.

Určení uživatelských profilů a instalačních hodnot pro aplikace

Při plánování instalace aplikací musíte nejdříve pro každou aplikaci zvolit uživatelské profily a instalační hodnoty. Dříve než nainstalujete aplikaci, která byla vytvořena v jiném systému, měli byste vytvořit jeden nebo více uživatelských profilů. Předtím, než zavedete ve svém systému knihovny aplikací, by měl v systému existovat uživatelský profil, který bude vlastníkem knihoven aplikací a aplikačních objektů. Profily, které je třeba vytvořit pro každou knihovnu, a parametry těchto profilů zaznamenejte do formuláře Instalace aplikace.

Při určování nezbytných instalačních hodnot položte programátorovi nebo dodavateli aplikací následující otázky a zaznamenejte jejich odpovědi do formuláře Instalace aplikace:

- Který profil je vlastníkem knihovny aplikací?
- Který profil je vlastníkem objektů v knihovně?
- Jaká jsou veřejná oprávnění ke knihovně (AUT)?
- Jaká jsou veřejná oprávnění k novým objektům (CRTAUT)?
- Jaká jsou veřejná oprávnění k objektům v knihovně?
- Které programy (jsou-li takové) přebírají oprávnění vlastníka?

Zjistěte, zda programátoři nebo dodavatel aplikací vytvořili pro aplikaci nějaké seznamy oprávnění. Připravte pro každý vytvořený seznam oprávnění formulář Seznam oprávnění nebo požádejte programátora o informace o tomto seznamu.

Nyní můžete určit, zda je potřeba změnit nějaké instalační hodnoty.

Provádění změn instalačních hodnot pro aplikace

Porovnejte informace ve formuláři Instalace aplikace s plánem zabezpečení prostředků pro knihovnu ve formuláři Popis knihovny. Pokud se liší, musíte se rozhodnout, jaké změny po nainstalování aplikace provést.

Změny vlastnictví aplikací

Pokud váš programátor nebo dodavatel aplikací vytvořil pro účely vlastnictví knihoven aplikací a aplikačních objektů zvláštní profil, zvažte možnost použití tohoto profilu, i když neodpovídá vašim konvencím pojmenování. Přenos vlastnictví objektů může být časově náročný a je třeba se ho vyvarovat.

Pokud je vlastníkem aplikace některý ze skupinových profilů dodaných IBM, například QSECOFR nebo QPGMR, měli byste po instalaci aplikace přenést vlastnictví na jiný profil.

Programátoři někdy navrhují aplikace tak, aby nebylo možné měnit vlastnictví objektů. Snažte se v rámci těchto omezení splnit vlastní požadavky na správu zabezpečení. Pokud je však vlastníkem aplikace profil dodaný IBM, například QSECOFR, musíte spolu s programátorem nebo dodavatelem aplikací vytvořit plán, jak vlastnictví změnit. V ideálním případě byste měli vlastnictví změnit před instalací aplikace.

Změny veřejných oprávnění

Při ukládání objektů se spolu s nimi ukládají jejich veřejná oprávnění. Jestliže v systému obnovíte nějakou knihovnu aplikací, bude mít knihovna a všechny její objekty stejná veřejná oprávnění jako v době, kdy byly uloženy. Platí to i v případě, že jste knihovnu uložili v jiném systému.

Hodnota CRTAUT pro knihovnu (veřejné oprávnění k novým objektům) nemá na obnovované objekty vliv. Objekty se obnoví s uloženými veřejnými oprávněními bez ohledu na hodnotu CRTAUT pro knihovnu.

Veřejná oprávnění ke knihovnám a objektům byste měli změnit tak, aby odpovídala vašemu plánu ve formuláři Popis knihovny.

Při plánování instalace aplikací byste se měli seznámit s příkladem, jak instalaci aplikací naplánovala Sharon Jonesová z firmy JKL Toy Company.

Chcete-li zajistit, aby byl plán instalace aplikací úplný, postupujte takto:

- Dokončete vyplňování počátečního formuláře Instalace aplikace. Pak se vraťte a vyplňte formuláře pro všechny další aplikace.
- Zkontrolujte všechny formuláře a ujistěte se, zda jsou úplné. Udělejte si kopie formulářů a uložte je na bezpečném místě, dokud nenainstalujete systém a licencované programy.

Po dokončení těchto plánovacích úkolů jste připraveni nastavit zabezpečení uživatelů.

Příklad: Formulář společnosti JKL Toy Company: Instalace aplikace: Společnost JKL Toy Company koupila aplikace Zákaznické objednávky a Pohledávky od dodavatele aplikací. Najala programátora, aby vyvinul aplikaci Smlouvy a ceníky a spojil ji s aplikací Zákaznické objednávky.

Sharon Jonesová použila pro přípravu formuláře Instalace aplikace informace z formuláře Popis knihovny. Níže uvedená tabulka zobrazuje kopii Sharonina formuláře Popis knihovny pro knihovnu CUSTLIB: (viz téma ″Informace popisující knihovnu″).

Tabulka 57. Příklad: Formulář společnosti JKL Toy Company: Popis knihovny

Formulář Popis knihovny	**část 1 ze 2**
Zhotovila: Sharon Jonesová	Datum: 9/9/99
Jméno knihovny: CUSTLIB	Popisné jméno (text): Knihovna záznamů o zákaznících
Stručně popište funkce této knihovny: Obsahuje všechny zákaznické soubory, včetně objednávek a účtů.	

Definujte pro knihovnu cíle v oblasti zabezpečení, jako například to, zda jsou některé informace důvěrné:
`Dnes umožníme každému zaměstnanci společnosti, aby si prohlédl zákaznické objednávky.`
`Abychom ochránili přesnost informací, měli bychom omezit, kdo je oprávněn je měnit.`	

Veřejné oprávnění ke knihovně: *USE Veřejné oprávnění k objektům v knihovně: *CHANGE Veřejné oprávnění pro nové objekty (CRTAUT): *CHANGE Vlastník knihovny: OWNAR	

Níže uvedená tabulka zobrazuje formulář Instalace aplikace, který Sharon připravila pro aplikaci Zákaznické objednávky. Všimněte si, že Sharon se rozhodla použít profil vlastníka vytvořený poskytovatelem aplikace. Profil COWNER bude vlastnit soubor i knihovny programů.

Po instalaci aplikace by Sharon měla:

- Změnit ve formulářích Popis knihovny veřejná oprávnění pro knihovny tak, aby odpovídala plánu zabezpečení.
- Změnit třídu uživatele profilu COWNER na *USER a odstranit všechna zvláštní oprávnění.
- Změnit heslo profilu COWNER na *NONE.

Tabulka 58. Příklad: Formulář společnosti JKL Toy Company: Instalace aplikace

Jméno aplikace: Zákaznické objednávky (CO)		Popis: Zadávání, sledování a odesílání objednávek.
Uveďte a vysvětlete všechny profily, které musejí být vytvořeny, aby mohla být instalována aplikace: Knihovna obsahující soubory je vlastněna profilem nazvaným COWNER. Knihovna programů je vlastněna QPGMR.		
Jméno knihovny: CUSTLIB		
	Před instalací	**Po instalaci**
Vlastník knihovny	COWNER	COWNER
Vlastník objektu.	COWNER	COWNER
Veřejné oprávnění ke knihovně	*EXCLUDE	*USE
Veřejné oprávnění k objektu	*ALL	*CHANGE
Veřejné oprávnění pro nové objekty	*CHANGE	*CHANGE
Jméno knihovny: COPGMLIB		
	Před instalací	**Po instalaci**
Vlastník knihovny	QPGMR	COWNER
Vlastník objektu.	QPGMR	COWNER
Veřejné oprávnění ke knihovně	*EXCLUDE	*USE
Veřejné oprávnění k objektu	*ALL	*CHANGE
Veřejné oprávnění pro nové objekty	*CHANGE	*CHANGE

Když jste nyní ukončili úkoly plánování, jste připraveni nastavit zabezpečení uživatelů.

Nastavení zabezpečení uživatelů

Toto téma vás provede úkoly potřebnými k nastavení zabezpečení uživatelů systému pomocí rozhraní příkazového řádku. Pokud nastavujete nový systém, provádějte tyto kroky v uvedeném pořadí. Systém využije informace zadané v jednotlivých krocích procesu. K nastavení základního zabezpečení systému musíte provést dvě sady úkolů. Za prvé musíte definovat zabezpečení uživatelů a za druhé musíte nastavit ochranu prostředků systému. V následujících dvou tabulkách jsou uvedeny jednotlivé kroky konfigurace, které je nutné provést k nastavení zabezpečení uživatelů a prostředků.

Poznámka: Dříve než začnete nastavovat zabezpečení prostředků, **musíte** provést všechny kroky týkající se nastavení zabezpečení uživatelů.

Tabulka 59. Kroky týkající se nastavení zabezpečení uživatelů

Krok	Činnosti prováděné v tomto kroku	Používané formuláře
Nastavení celkového prostředí	Nastavte počáteční systémové hodnoty a atributy sítě. Vytvořte uživatelský profil správce systému.	Výběr systémových hodnot

Tabulka 59. Kroky týkající se nastavení zabezpečení uživatelů (pokračování)

Krok	Činnosti prováděné v tomto kroku	Používané formuláře
Nastavení systémových hodnot pro zabezpečení	Nastavte další systémové hodnoty.	Výběr systémových hodnot
Příprava základních kroků zabezpečení pro zavedení aplikací	Vytvořte profily vlastníků. Zaveďte aplikace. Dříve než provedete zbývající kroky, musí být knihovny aplikací a aplikační objekty umístěny v systému.	Instalace aplikace
Nastavení skupin uživatelů	Vytvořte popisy úloh, skupinové knihovny a skupinové profily.	Popis skupiny uživatelů
Nastavení individuálních uživatelů	Vytvořte individuální knihovny a uživatelské profily.	Formulář Profil individuálního uživatele

Tabulka 60. Kroky nastavení zabezpečení prostředků

Krok	Činnosti prováděné v tomto kroku	Používané formuláře
Nastavení vlastnictví a veřejných oprávnění	Nastavte vlastnictví a veřejná oprávnění ke knihovnám a objektům.	Instalace aplikace
Vytvoření seznamu oprávnění	Vytvořte seznamy oprávnění.	Seznam oprávnění
Nastavení specifických oprávnění	Nastavte přístup ke knihovnám a jednotlivým objektům.	Formulář Popis knihovny
Zabezpečení tiskového výstupu	Nastavení ochrany tiskového výstupu vytvořením výstupních front a přiřazením výstupu.	Zabezpečení výstupních front a pracovních stanic
Zabezpečení pracovních stanic	Nastavení ochrany pracovních stanic.	Zabezpečení výstupních front a pracovních stanic

Kromě témat uvedených v předchozí tabulce se seznamte s těmito tématy o správě zabezpečení systému:

- Testování zabezpečení.
- Provádění změn informací o zabezpečení.
- Uložení informací o zabezpečení.
- Monitorování zabezpečení.

Dříve než začnete

Instalujete-li nový systém, proveďte před zahájením nastavování zabezpečení tyto akce:

- Ujistěte se, zda systémová jednotka a zařízení jsou správně nainstalovány a řádně fungují. Pokud nemáte v úmyslu používat pro zařízení konvencí pojmenování systému iSeries, nepřipojujte pracovní stanice a tiskárny, dokud nezměníte systémovou hodnotu, jež určuje metodu pojmenování zařízení (QDEVNAMING). V části Použití nových systémových hodnot se dozvíte, kdy je třeba zařízení připojit.
- Zaveďte všechny licencované programy, které budete chtít používat.

Nastavení celkového prostředí

Chcete-li začít s nastavením zabezpečení uživatelů, musíte pro uživatele nastavit celkové prostředí. V tomto tématu nastavíte systémové hodnoty pomocí menu SETUP a vytvoříte vlastní uživatelský profil. Změníte rovněž ID uživatele a hesla pro profily DST (Dedicated Service Tools).

V následujících postupech najdete ukázky obrazovek příkazového řádku, které tyto kroky ilustrují. Nejsou však uvedeny celé obrazovky. Jsou znázorněny pouze informace nezbytné k provedení úkolů.

Jaké formuláře použít?

Zadejte informace z formuláře Výběr systémových hodnot, který jste připravili v tématu Plánování celkové strategie zabezpečení.

K nastavení celkového prostředí je třeba provést tyto úkoly:

1. Přihlášení do systému.
2. Výběr správné úrovně asistence.
3. Zabránění přihlášení jiných uživatelů.
4. Zadání systémových hodnot zabezpečení.
5. Použití nových systémových hodnot.
6. Vytvoření profilu správce systému.

Po dokončení těchto kroků musíte změnit hesla SST a zabránit tak jejich neoprávněnému použití. Další podrobnosti najdete v tématu Servisní nástroje.

Přihlášení do systému

Abyste mohli začít s nastavením prostředí systému, musíte se přihlásit do systému.

1. Přihlaste se na konzoli jako správce systému (QSECOFR). Pokud se přihlašujete poprvé, použijte heslo QSECOFR. Protože systém dodává toto heslo s prošlou platností, budete vyzváni ke změně hesla. K úspěšnému přihlášení je nutné toto heslo změnit.
2. Na obrazovce Přihlášení zadejte do pole *Menu* slovo SETUP.

Poznámka: Menu SETUP se nazývá menu Customize Your System, Users, and Devices. V tomto textu používáme označení menu SETUP.

```
                Přihlášení
                            Systém  . . . . .
                            Podsystém . . . .
                            Obrazovka . . . .

Uživatel. . . . . . . . . . . . QSECOFR
Heslo . . . . . . . . . . . . . _________
Program/procedura . . . . . . . _________
Menu  . . . . . . . . . . . . . SETUP
Aktuální knihovna . . . . . . . _________
```

Po přihlášení do systému musíte vybrat správnou úroveň asistence.

Výběr správné úrovně asistence

Po přihlášení do systému můžete pro uživatele zvolit odpovídající úroveň asistence. **Úroveň asistence** určuje, jakou verzi obrazovky uživatel uvidí. Mnohé systémové obrazovky mají dvě různé verze:

- Úroveň asistence ″basic assistance level″ obsahuje méně informací a není v ní použita technická terminologie.
- Úroveň asistence ″intermediate assistance″ zobrazuje více informací a používá technické výrazy.

Některá pole nebo funkce jsou k dispozici pouze v konkrétní verzi obrazovky. V pokynech se dozvíte, kterou verzi máte použít. Chcete-li změnit určitou úroveň asistence na jinou, použijte volbu **F21** (Výběr úrovně asistence). **F21** není k dispozici u všech obrazovek.

Po výběru úrovně asistence musíte zabránit přihlášení jiných uživatelů do systému v době, kdy nastavujete zabezpečení.

Zabránění přihlášení jiných uživatelů

Po výběru správné úrovně asistence musíte zabránit komukoliv jinému, aby se mohl přihlásit do systému. Máte-li obavy, že by jiní uživatelé mohli zasáhnout do systému dříve, než ho zabezpečíte, můžete zabránit, aby se kdokoliv mohl přihlásit z jiné pracovní stanice. Tato akce je nepovinná. Proveďte ji pouze v případě, že se domníváte, že dočasné zabezpečení je nezbytné:

1. V menu SETUP stisknutím klávesy **F9** zobrazte příkazový řádek.
2. Na příkazovém řádku zadejte příkaz GO DEVICESTS.
3. Na obrazovce se ukáže menu Device Status Tasks. Pokud se ukáže menu Work with Configuration Status, použijte volbu **F21** (Výběr úrovně asistence) ke změně na úroveň ″basic assistance level″.
4. Vyberte volbu **1** (Práce s obrazovkami).
5. Na obrazovce Práce s obrazovkami učiňte nedostupnými všechny pracovní stanice, kromě té, na které pracujete. Uděláte to tak, že před jména jednotlivých pracovních stanic vždy napíšete číslo **2** a stisknete klávesu **Enter**.
6. Vraťte se do menu SETUP dvojím stisknutím klávesy **F3** (Konec).
7. Stisknutím klávesy **F12** (Zrušení) odstraňte příkazový řádek.

```
                          Práce s obrazovkami

Zapište volby, stiskněte Enter.
  1=Zpřístupnění    2=Znepřístupnění   5=Zobrazení podrobností
  7=Zobrazení zprávy   8=Práce s řadičem a linkou
  13=Změna popisu

Vol  Zařízení    Typ     Stav
__   DSP01       3196    QSECOFR
2_   DSP02       3196    Available to use
2_   DSP03       3196    Available to use
2_   DSP04       3196    Available to use
```

Učiníte-li zařízení nedostupným, nebude mít obrazovku Přihlášení, a to ani po zapnutí. Pracovní stanice zůstanou nedostupné, dokud nezastavíte a nerestartujete systém. Tento krok tedy může být nutné zopakovat.

Jakmile zabráníte všem ostatním přihlásit se do systému, můžete zadat systémové hodnoty zabezpečení.

Zadání systémových hodnot zabezpečení

Poté, co jste zabránili ostatním přihlásit se do systému, je třeba, abyste do systému vložili systémové hodnoty.

Pomocí následujícího postupu vložte informace z části 1 formuláře Výběr systémových hodnot:

1. V menu SETUP vyberte volbu **1** (Změna systémových voleb).
2. Na obrazovce Změna systémových voleb vložte informace z formuláře Výběr systémových hodnot. Pokud některé volby na obrazovce nechcete měnit, můžete je přeskočit pomocí klávesy Tab.
3. Na této obrazovce zadejte správné datum a čas, pokud tyto hodnoty nebyly nastaveny při spuštění systému.
4. Po zadání informací na této stránce přejděte na další stránku. Nápis *Více...* v dolním pravém rohu obrazovky znamená, že obrazovka má nejméně jednu další stránku.

```
                          Změna systémových voleb
Systém:
Zapište volby, stiskněte Enter.

Jméno systému . . . . . .  JKLTOY     Jméno

Volby datumu a času:
  Systémové datum . . . . . .  09/21/99     MM/DD/RR
  Systémový čas . . . . . .  10:52:57     HH:MM:SS
  Oddělovač datumu . . . . . .  1            1=/
                                             2=-
                                             3=.
                                             4=,
                                             5=mezera
  Formát datumu . . . . . .   MDY           YMD, MDY, DMY, JUL
  Oddělovač času  . . . . . .   1           1=:
                                             2=.
                                             3=,
                                             4=mezera


                                                                  Více...
F1=Nápověda   F3=Konec   F5=Obnova   F12=Zrušení
```

5. Napište své volby na druhé stránce obrazovky a přejděte na další stránku.

```
                          Změna systémových voleb

Zapište volby, stiskněte Enter.

Volby zabezpečení:
  Úroveň zabezpečení  . . . . . .   40
   :
  Povolit správcům systému
    (QSECOFR) přihlášení z
    libovolné stanice . . . . . .   N
```

6. Napište své volby na třetí stránce obrazovky a stiskněte klávesu **Enter**.

```
                          Změna systémových voleb

Zapište volby, stiskněte Enter.

Volby zařízení:
  Formát pojmenování nových
  zařízení . . . . . .   1


  Předpokládaná systémová tiskárna. . .   PRT01

Další volby:
  Umístit uživatele po přihlášení
    do prostředí S/36 . . . . .   N
  Uchovat informace o
    dokončených tiskových
    výstupech pro účtování úloh.  Y
```

7. Nyní byste měli vidět opět menu SETUP. Povšimněte si zprávy v dolní části obrazovky: **Systémové volby byly úspěšně změněny. Je nutný IPL.**

   Poznámka: Systém vyžaduje IPL jen v případě, že jste změnili úroveň zabezpečení.

Na konci většiny témat o systémových úlohách najdete tabulku, která popisuje možné chyby a postup nápravy. Použijte tyto tabulky jako pomůcku pro případ, že jste získali jiné výsledky, než je popsáno. Tyto tabulky nemohou vyřešit všechny problémy. Mají vám pouze poskytnout rady při řešení problémů a usnadnit vám práci se systémem.

Možná chyba	Náprava
Je zobrazeno hlavní menu.	Stiskli jste klávesu **F3** (Konec) nebo **F12** (Zrušení). Napište příkaz GO SETUP a zopakujte akci.
Je zobrazena jiná obrazovka, například obrazovka Change Cleanup Options.	Vybrali jste nesprávnou volbu v menu SETUP. Stisknutím klávesy **F3** (Konec) se vraťte k menu a zopakujte akci.
Po stisknutí klávesy **Enter** se znovu zobrazí obrazovka Změna systémových voleb.	Podívejte se na chybovou zprávu v dolní části obrazovky. Pravděpodobně jste zadali hodnotu, která není povolena. Potřebujete-li další informace, můžete použít klávesu **F1** (Nápověda). Chcete-li, aby systém obnovil všechny hodnoty do stavu, ve kterém byly předtím, než jste začali psát, stiskněte klávesu **F5** (Obnova). Zopakujte akci.
Stiskli jste klávesu **Enter** dříve, než jste napsali všechny své volby na obrazovce.	Tuto obrazovku můžete ke změnám systémových hodnot používat tak často, jak potřebujete. Vyberte volbu **1** v menu SETUP a vložte hodnoty, na které jste poprvé zapomněli. **Upozornění: Jakmile je systém v provozu, neměňte bez porady s programátorem úroveň zabezpečení. Rovněž neměňte jméno systému, jestliže používáte produkt iSeries Access, nebo jestliže komunikujete s jiným počítačem.**
Místo abyste přešli na další stránku, stiskli jste klávesu **Enter**.	Vyberte znovu volbu **1** v menu SETUP a přejděte na druhou stránku. Napište své volby a stiskněte klávesu **Enter**.

Po zadání systémových hodnot musíte použít nové systémové hodnoty.

Použití nových systémových hodnot

Po zadání systémových hodnot musíte některé z těchto hodnot použít. Většina změn systémových hodnot začne platit okamžitě. Pokud však změníte úroveň zabezpečení systému, neprojeví se tato změna do doby, dokud systém nezastavíte a nerestartujete. Po ověření, že jste na obrazovce Změna systémových voleb napsali všechny hodnoty správně, jste připraveni nové hodnoty použít.

Poznámka: Pokud jste tak dosud neučinili, připojte pracovní stanice k systému. Když systém spustíte, budou tato zařízení automaticky nakonfigurována pomocí formátu pojmenování, který jste zvolili na obrazovce Změna systémových voleb.

Zastavte a restartujte systém. Postupujte přitom v souladu s níže uvedenou procedurou. Po spuštění systému začnou platit hodnoty, které jste zadali na obrazovce Změna systémových voleb.

1. Přihlaste se na konzoli a zajistěte, aby nebyl nikdo přihlášen na jiných pracovních stanicích.
2. Přepínač s klíčkem na procesorové jednotce musí být v normální poloze (Normal).
3. V menu SETUP vyberte volbu Úlohy zapínání a vypínání.
4. Vyberte volbu pro okamžité vypnutí a následné zapnutí systému. Stiskněte klávesu **Enter**.
5. Systém ukáže obrazovku, která vyžaduje, abyste potvrdili požadavek vypnutí. Stiskněte klávesu **F16** (Potvrzení).

Systém tak bude zastaven a poté automaticky spuštěn. Obrazovka bude na krátkou dobu prázdná. Pak by se měla znovu zobrazit obrazovka Přihlášení.

Po použití nových systémových hodnotu musíte v systému pro sebe vytvořit profil správce systému.

Vytvoření profilu správce systému

Správce systému (security officer) je libovolný uživatel s třídou uživatele *SECOFR nebo se zvláštními oprávněními *ALLOBJ a *SECADM.

Jakmile použijete systémové hodnoty z obrazovky Změna systémových voleb, vytvořte uživatelský profil pro sebe a pro alternativního správce systému. V budoucnosti používejte při provádění činností správce systému místo profilu QSECOFR svůj profil.

1. Přihlaste se do systému jako QSECOFR a vyžádejte menu SETUP.

   Všimněte si, že jméno systému, které jste zvolili, je zobrazeno v horním pravém rohu obrazovky Přihlášení.

```
                  Přihlášení
                              Systém  . . . . .
                              Podsystém . . . .
                              Obrazovka . . . .

Uživatel. . . . . . . . . . . . . QSECOFR
Heslo . . . . . . . . . . . . .   _________
Program/procedura . . . . . . .   _________
Menu  . . . . . . . . . . . . .   SETUP
Aktuální knihovna . . . . . . .   _________
```

2. V menu SETUP vyberte volbu *Work with user enrollment*. Na obrazovce Work with User Enrollment se zobrazí výpis profilů, které jsou nyní v systému.

   Poznámka: Pokud se zobrazí obrazovka Práce s uživatelskými profily, stiskněte klávesu **F21** (Výběr úrovně asistence) a zvolte basic assistance level.

3. Nový profil vytvoříte tak, že zadáte **1** (Vytvoření) do sloupce *Vol* a napíšete jméno profilu do sloupce *Uživatelský profil*. Stiskněte klávesu **Enter**.

```
                           Work with User Enrollment

Type options below, then press Enter.
  1=Add   2=Change   3=Copy   4=Remove   5=Display

Opt     User             Description
1       JONESS
QDOC                          Document User Profile
QSECOFR                       Security Officer User Profile
```

4. Na obrazovce Přidání uživatele si přiřaďte heslo.
5. Vyplňte pole znázorněná na ukázce obrazovky vlastními správnými údaji.
6. Přejděte na další stránku obrazovky.

```
                           Přidání uživatele

Zapište dole volby, pak stiskněte Enter.

Uživatel  . . . . . .   JONESS
Uživatelský popis . . .   Jonesová, Sharon
Heslo . . . . . . . . .   secret
Typ uživatele . . . . .   *SECOFR
Uživatelská skupina . . .   *NONE

Omezené použití příkazového řádku   _____
Předpokládaná knihovna . . . . .
Předpokládaná tiskárna . . . . .   *WRKSTN
Přihlašovací program . . . . . .   *NONE
Knihovna . . . . . . . . . . . .

První menu . . . . . . . . . . .
Knihovna . . . . . . . . . . . .
```

7. Vyplňte druhou stránku obrazovky a stiskněte klávesu **Enter**.

8. Zkontrolujte potvrzující zprávy v dolní části obrazovky Work with User Enrollment.
9. Stisknutím klávesy **F3** (Konec) se vraťte k menu SETUP.

```
                          Přidání uživatele

Zapište dole volby, pak stiskněte Enter.

Program klávesy Attn  . .   *SYSVAL
  Knihovna. . . . . . . .
```

Možná chyba	Náprava
Stiskli jste klávesu **Enter** dříve, než jste napsali informace do všech polí.	Použijte volbu *Change* na obrazovce Work with User Enrollment a změňte profil, který jste právě vytvořili. Pokud se profil neobjeví v seznamu, stiskněte klávesu **F5** (Obnova) a stránkujte dál, dokud ho nenajdete.

Až pro sebe vytvoříte profil správce systému, změňte ID uživatele a hesla uživatelů SST. Další informace najdete v tématu Servisní nástroje v aplikaci Information Center.

Nastavení systémových hodnot pro zabezpečení

V tomto tématu použijete příkaz WRKSYSVAL (Práce se systémovými hodnotami) ke změnám a zobrazení systémových hodnot.

Jaké formuláře použít?

Zadejte informace z formuláře Výběr systémových hodnot, který jste připravili v tématu Plánování celkové strategie zabezpečení.

K tomu, abyste nastavili systémové hodnoty, musíte provést tyto úkoly:

1. Změnit systémové hodnoty zabezpečení.
2. Změnit individuální systémové hodnoty.

Přihlášení k rozhraní příkazového řádku

K přihlášení do systému použijte tyto informace:

Profil Váš vlastní (vyžaduje se oprávnění *SECADM a *ALLOBJ)

Menu MAIN

Po přihlášení můžete začít měnit systémové hodnoty zabezpečení.

Změny systémových hodnot zabezpečení

Po přihlášení do systému použijte následující postup k zadání systémových hodnot zabezpečení, které jsou uvedeny v části 2 formuláře Výběr systémových hodnot.

1. Na příkazovém řádku napište příkaz WRKSYSVAL *SEC a stiskněte klávesu **Enter**. Parametr *SEC za jménem příkazu znamená, že chcete vidět pouze systémové hodnoty, které se vztahují k zabezpečení.
2. Na obrazovce Práce se systémovými hodnotami napište **2** (Změna) do sloupce *Volba* před systémovou hodnotou, kterou chcete změnit. Pokud systémová hodnota, kterou chcete změnit, není na obrazovce zobrazena, stránkujte dále, dokud ji nenajdete.

```
                        Práce se systémovými hodnotami

Umístění na  . . . . . .                Počáteční znaky systémové hodnoty
Typ hodnoty  . . . . . .   *SEC         F4 seznam

Zapište volby, stiskněte Enter.
  2=Změna   5=Zobrazení

        Systémová
Volba   hodnota     Typ         Popis
        QINACTMSGQ  *SEC        Inactive job message queue
2       QLMTDEVSSN  *SEC        Limit device sessions
        QLMTSECOFR  *SEC        Limit security officer device
        QMAXSGNACN  *SEC        Action to take for failed
  ⋮
```

3. Napište svou volbu pro systémovou hodnotu a stiskněte klávesu **Enter**. Znovu se ukáže obrazovka Práce se systémovými hodnotami.

```
                          Změna systémové hodnoty
Systémová hodnota . . . . . :    QLMTDEVSSN
Popis . . . . . . . . . . . :    Omezení relací zařízení


Zapište volbu a stiskněte Enter.

  Omezení relací zařízení . . . .   0       0=Bez omezení
                                            1=S omezením
```

4. Zkontrolujte, zda se v dolní části obrazovky zobrazí potvrzovací zpráva.

Možná chyba	Náprava
Zobrazily se jiné systémové hodnoty, než ty, které jsou ukázány v příkladu obrazovky Práce se systémovými hodnotami.	Zapomněli jste napsat parametr *SEC. Porovnejte pole *Typ hodnoty* v horní části obrazovky s ukázkovou obrazovkou. Přesuňte kurzor do pole *Typ hodnoty*. Napište *SEC a stiskněte klávesu **Enter**.
Systém nezpracoval příkaz, který jste zadali. Stále je zobrazeno menu.	Zkontrolujte, zda se v dolní části obrazovky nezobrazily nějaké chybové zprávy. Pravděpodobně jste nesprávně napsali jméno příkazu. Zopakujte akci. Pokud zpráva říká, že nemáte oprávnění, odhlaste se a znovu se přihlaste pomocí profilu s oprávněním správce systému.
Po stisknutí klávesy **Enter** se znovu objeví obrazovka Změna systémové hodnoty.	Zkontrolujte, zda se v dolní části obrazovky neobjevily nějaké chybové zprávy. Pravděpodobně jste chybně napsali svou volbu, nebo jste vybrali hodnotu, která leží mimo povolený rozsah. Další informace zobrazíte stisknutím klávesy **F1** (Nápověda).
Místo obrazovky Práce se systémovými hodnotami vidíte menu.	Pravděpodobně jste dvakrát stiskli klávesu **Enter**. Zadejte příkaz WRKSYSVAL *SEC.
Vybrali jste systémovou hodnotu, kterou nechcete změnit.	Stisknutím klávesy **F12** (Zrušení) se vrátíte na obrazovku Práce se systémovými hodnotami.

Co znamená hvězdička (*)?

Pravděpodobně jste si všimli, že některé hodnoty mají na začátku hvězdičku (*). Systém používá hvězdičku k tomu, aby poznal rozdíl mezi zvláštními hodnotami a běžnými slovy. Jestliže například v uživatelském profilu určíte heslo *NONE, znamená to, že systém nedovolí nikomu, aby se pomocí tohoto profilu přihlásil. Pokud zadáte, že heslo je NONE, musí uživatel jako heslo zadat znaky NONE.

Při nastavování zabezpečení systému věnujte pozornost použití hvězdičky v instrukcích a formulářích.

Po změně systémových hodnot zabezpečení můžete změnit individuální systémové hodnoty.

Změny individuálních systémových hodnot

Po změně systémových hodnot zabezpečení můžete změnit individuální systémové hodnoty.

Systémová hodnota QDSCJOBITV (prodleva odpojené úlohy) například nepatří mezi systémové hodnoty zabezpečení. Neobjeví se v podmnožině *SEC na obrazovce Práce se systémovými hodnotami. Ke změně systémové hodnoty QDSCJOBITV a jakékoliv individuální systémové hodnoty použijte tento postup:

1. Napište příkaz WRKSYSVAL QDSCJOBITV a stiskněte klávesu **Enter**.
2. Na obrazovce Práce se systémovými hodnotami napište **2** (Změna) do sloupce *Volba* před hodnotu QDSCJOBITV.
3. Napište svou volbu pro hodnotu QDSCJOBITV.
4. Zkontrolujte, že se zobrazí potvrzovací zpráva.

```
                            Změna systémové hodnoty
Systémová hodnota . . . . . :   QDSCJOBITV
Popis . . . . . . . . . . . :   Interval prodlevy odpojené úlohy


Zapište volbu a stiskněte Enter.

  Interval prodlevy odpojené úlohy ..... 300
```

Výpis hodnot zabezpečení

Po zadání všech informací z formuláře Výběr systémových hodnot můžete vytisknout seznam všech systémových hodnot zabezpečení. Napište příkaz WRKSYSVAL *SEC OUTPUT(*PRINT). Uložte kopii seznamu k formuláři Výběr systémových hodnot. Kdykoliv změníte některou systémovou hodnotu zabezpečení, vytiskněte seznam znovu.

Po zadání všech voleb pro systémové hodnoty z formuláře Výběr systémových hodnot se můžete připravit k zavedení aplikací.

Provedení kroků zabezpečení pro zavedení aplikací

Po nastavení systémových hodnot se můžete připravit k zavedení aplikací. Toto téma popisuje kroky zabezpečení, které jsou nutné k zavedení knihoven aplikací do systému. Až vytvoříte profily a další objekty zabezpečení, v tématech Nastavení vlastnictví a veřejného oprávnění a ″Nastavení zabezpečení prostředků″ se dozvíte, jak pro aplikace nastavit vlastnictví a oprávnění.

Pokud je to možné, měli byste nejdříve zavést do systému knihovny aplikací, a až potom vytvořit skupiny uživatelů a individuální profily. Při vytváření popisů úloh a profilů se budete potřebovat odvolávat na aplikační objekty.

Pokud nezavedete aplikace před vytvářením skupinových a individuálních profilů, můžete obdržet varovné zprávy tohoto typu:

- Při vytváření popisů úloh: Systém nenašel počáteční knihovny.
- Při vytváření profilů: Systém nenašel počáteční program nebo menu.

Dokud nezavedete knihovny aplikací, nemůžete popisy úloh a profily úspěšně otestovat.

Použijte formuláře Instalace aplikace, které jste si připravili v tématu Plánování instalace aplikací.

K tomu, abyste zavedli jednotlivé aplikace, proveďte tyto úkoly:

1. Vytvořte profil vlastníka.
2. Zaveďte aplikaci.

Přihlášení do systému

- Kvůli vytvoření profilů vlastníků:

  Profil Váš vlastní (vyžaduje se oprávnění *SECADM)

  Menu MAIN
- Chcete-li zavést knihovny aplikací:

  Zeptejte se dodavatele aplikace, zda se kvůli zavedení knihoven aplikací máte přihlásit jako správce systému nebo vlastník aplikace.

Po přihlášení do systému můžete pro aplikace vytvořit profil vlastníka.

Vytvoření profilu vlastníka

Po přihlášení do systému zkontrolujte Plán instalace aplikací, zda byste před zavedením aplikace neměli vytvořit nějaké profily. Chcete-li vytvořit profil, postupujte takto:

1. Napište příkaz CRTUSRPRF a stiskněte klávesu **F4** (Náznak).
2. Na obrazovce Vytvoření profilu uživatele vyplňte pole podle pokynů programátora nebo dodavatele aplikací.
3. Pomocí klávesy **F10** přejděte na další stránku obsahující další pole.

```
                      Vytvoření profilu uživatele (CRTUSRPRF)

Zapište volby, stiskněte Enter.

Uživatelský profil . . . . . >
Uživatelské heslo. . . . . .   *USRPRF
Nastavit heslo na ukonč.plat.  .   *NO
Stav . . . . . .   *ENABLED
Třída uživatele. . . . . .   *USER
Úroveň asistence . . . . . .   *SYSVAL
Aktuální knihovna. . . . . .   *CRTDFT
Počáteční program k volání . . .   *NONE
  Knihovna . . . . . .
Počáteční menu . . . . . .   MAIN
  Knihovna . . . . . .     *LIBL
Omezit schopnosti  . . . . . .   *NO
Text . . . . . .   Vlastník xxxxxx
```

4. Zkontrolujte, zda se v dolní části obrazovky neobjevily nějaké zprávy.

Poznámka: Podrobnější informace o vytváření profilů najdete v tématu Vytvoření skupinového profilu.

Po vytvoření vlastníka aplikace můžete začít zavádět aplikaci.

Zavedení aplikace

Postupujte podle pokynů dodavatele aplikací týkajících se zavádění knihoven aplikací. Informace o tom, jak nastavit vlastnictví a veřejná oprávnění k aplikacím, najdete v tématu Nastavení vlastnictví a veřejného oprávnění.

Po zavedení všech aplikací můžete vytvořit skupiny uživatelů.

Nastavení skupin uživatelů

Po provedení kroků nezbytných k zabezpečení při zavádění vašich aplikací můžete nastavit skupinu uživatelů. Vytvoříte knihovny skupin, popisy úloh a skupinové profily. Při práci projděte celé téma u jedné z vašich skupin

uživatelů, potom se vraťte a opakujte kroky pro kteroukoliv další skupinu. Ukázkové obrazovky zobrazují informace z formulářů Popis skupiny uživatelů pro oddělení prodeje a marketingu a pro oddělení skladu společnosti JKL Toy Company.

Použijte formuláře Popis skupiny uživatelů, které jste si připravili v tématu ″Plánování skupin uživatelů″.

Dokončete tyto úlohy nastavení skupin uživatelů:

1. Vytvoření knihovny pro skupinu uživatelů.
2. Vytvoření popisu úlohy.
3. Vytvoření skupinového profilu.

Přihlášení do systému

Profil Váš vlastní (vyžaduje se oprávnění *SECADM)

Menu MAIN

Po přihlášení do systému vytvořte knihovnu pro skupinu uživatelů.

Vytvoření knihovny pro skupinu

Po přihlášení do systému budete potřebovat vytvořit knihovnu pro skupinu uživatelů. Pokud plánujete, že skupina bude sdílet knihovnu u objektů, které vytvořila, jako jsou například programy Query, vytvořte knihovnu ještě předtím, než vytvoříte skupinový profil:

1. Napište příkaz CRTLIB (Vytvoření knihovny) a stiskněte klávesu **F4** (Náznak).
2. Vyplňte obrazovku. Jméno knihovny musí být jménem skupinového profilu.
3. Stiskněte klávesu **F10** (Přídavné parametry).
4. Vyplňte veřejné oprávnění ke knihovně a k novým objektům, které jsou vytvořeny v knihovně.
5. Stiskněte klávesu **Enter**. Zkontrolujte potvrzující zprávu.

```
                          Vytvoření knihovny

Zapište volby, stiskněte Enter.

Knihovna . . . . . .   DPTWH
Typ knihovny . . . . . .   *PROD
Text . . . . . .   Knihovna skladu

                          Přídavné parametry

Oprávnění  . . . . . .   *USE
ID ASP . . . . . .   1
Vytvořit oprávnění . . . . . .   *CHANGE
Create object auditing . . . . . .   *SYSVAL
```

Možná chyba	Náprava
Stiskli jste klávesu **Enter** ještě před napsáním popisu knihovny.	Napište příkaz **CHGLIB** a stiskněte klávesu **F4** (Náznak). Napište jméno knihovny na náznakovou obrazovku a stiskněte klávesu **Enter**. Zadejte popis na obrazovce Změna knihovny.
Dali jste knihovně nesprávné jméno.	Použijte příkaz RNMOBJ (Přejmenování objektu).

Po vytvoření knihovny pro skupinu můžete vytvořit popis úlohy.

Vytvoření popisu úlohy

Po vytvoření knihovny pro skupinu můžete vytvořit popis úlohy pro každou skupinu.

Pokud knihovny, které jsou nutné pro počáteční seznam knihoven, nejsou dosud v systému, dostanete při vytvoření popisu úlohy varování.

1. Napište příkaz **CRTJOBD** (Vytvoření popisu úlohy) a stiskněte klávesu **F4** (Náznak).
2. Vyplňte tato pole:

   Job description:
   Popis úlohy bude stejný jako jméno skupinového profilu.

   Library name:
   QGPL

   Text: Popis skupiny
3. Stiskněte klávesu **F10** (Přídavné parametry).
4. Stiskem klávesy Page Down se přesuňte do pole *Počáteční seznam knihoven*.

```
                  Vytvoření popisu úlohy

Zapište volby, stiskněte Enter.

Popis úlohy  . . . . . . . . . . .   DPTSM
  Knihovna . . . . . . . . . . . .   QGPL
Fronta úloh. . . . . . . . . . . .   QBATCH
  Knihovna . . . . . . . . . . . .     *LIBL
Priorita úlohy (v JOBQ)  . . . . .   5
Priorita na výstupu (v OUTQ) . . .   5
Tiskové zařízení . . . . . . . . .   *USRPRF
Výstupní fronta. . . . . . . . . .   *USRPRF
  Knihovna . . . . . . . . . . . .
Text . . . . . . . . . . . . . . .   Prodej a marketing
```

5. Napište **+** (plus) u hodnoty *SYSVAL v poli *Počáteční seznam knihoven*. Tím specifikujete, že chcete zadat seznam hodnot. Stiskněte klávesu **Enter**.

```
Účtovací kód . . . . . . . . . .   *USRPRF
   ⋮
Kontrola syntaxe CL . . . . . . .   *NOCHK
Počáteční seznam knihoven . . . . .   +
              + další hodnoty
```

6. Do pole *Počáteční seznam knihoven* napište jména knihoven označených symbolem zaškrtnutí (✓) z vašeho formuláře Popis skupiny uživatelů:
   - Do jednoho řádku uveďte jedno jméno knihovny.
   - Zařaďte QGPL a QTEMP. Každá úloha užívá k ukládání dočasných objektů knihovnu nazvanou QTEMP. **Všechny počáteční seznamy knihoven musí mít knihovnu QTEMP**. U většiny aplikací musí být na počátečním seznamu knihoven uvedena také knihovna QGPL.
   - Běžnou (předvolenou) knihovnu nemusíte zařazovat do seznamu knihoven. Systém tuto knihovnu přidá automaticky při přihlášení do systému.
7. Stiskněte klávesu **Enter**. Zkontrolujte zprávy. (Pomocí klávesy Page Down si můžete prohlížet všechny zprávy.)

```
Zadat více hodnot pro

Zapište volby, stiskněte Enter.

Počáteční seznam knihoven . . . .    CUSTLIB
                                     ITEMLIB
                                     COPGMLIB
                                     ICPGMLIB
                                     QGPL
                                     QTEMP
```

Možná chyba	Náprava
Stiskli jste klávesu **Enter** namísto klávesy **F10**.	Chcete-li do počátečního seznamu knihoven zařadit správné knihovny, napište příkaz **CHGJOBD** (Změna popisu úlohy) a stiskněte klávesu **F4**.
Při pokusu o vytvoření popisu úlohy dostanete chybovou zprávu.	Nejčastěji se chybová zpráva vyskytne v případě, že se pokusíte zahrnout knihovnu, která není v systému. Je to výstražná zpráva. Popis úlohy je již vytvořen pomocí knihovny na počátečním seznamu knihoven. Nemůžete se přihlásit do systému s profilem, který specifikuje popis úlohy, dokud není knihovna v systému. Pokud je knihovna v systému, je možné, že jméno knihovny je napsáno nesprávně. Ověřte jméno knihovny a akci opakujte.

Po vytvoření popisu úlohy můžete vytvořit skupinový profil.

Vytvoření skupinového profilu

Po vytvoření popisu úlohy můžete vytvořit skupinový profil. Pro jeho vytvoření využijte informace uvedené v části 2 formuláře Popis skupiny uživatelů.

1. Použijte příkaz WRKUSRPRF (Práce s uživatelskými profily). Napište WRKUSRPRF *ALL. Nejprve se na obrazovce objeví seznam dodaný IBM.

   Poznámka: Pokud se objeví obrazovka Work with User Enrollment, stiskněte klávesu **F21**, pomocí níž změníte úroveň asistence na úroveň ″intermediate assistance″.

2. Za účelem vytvoření nového profilu napište **1** do sloupce *Opt* a jméno profilu do sloupce *User Profile*. Stiskněte klávesu **Enter**.

```
                        Práce s uživatelskými profily

Zapište volby, stiskněte Enter.
  1=Vytvoření   2=Změna   3=Kopie   4=Výmaz   5=Zobrazení
  12=Práce s objekty dle vlastníka

     Uživatelský
Vol  profil      Text
1    DPTSM
     QDOC        Dokumentace uživatelského profilu
     QSECOFR     Uživatelský profil správce systému
```

3. Zapište informace z vašeho formuláře Popis skupiny uživatelů do odpovídajících polí.
4. Použijte klávesu **Tab** pro vynechání všech polí, v nichž chcete využívat předvolené hodnoty.
5. Stiskněte klávesu **F10** (Přídavné parametry).
6. Odstránkujte dolů.

```
                     CRTUSRPRF (Vytvoření profilu uživatele)

Zapište volby, stiskněte Enter.

Uživatelský profil . . . . . > DPTSM
Uživatelské heslo  . . . . . .   *none
Nastavit heslo na ukonč.plat.  .   *NO
Stav . . . . . .   *ENABLED
Třída uživatele. . . . . .   *USER
Úroveň asistence . . . . . .   *SYSVAL
Aktuální knihovna. . . . . .   *CRTDFT
Počáteční program k volání . . .   cpsetup
  Knihovna . . . . . .   cppgmlib
Počáteční menu . . . . . .   cpmain
  Knihovna . . . . . .   cppgmlib
Omezit schopnosti  . . . . . .   *yes
Text . . . . . .   Prodej a marketing
```

7. Zadejte hodnoty pro zbývající pole z formuláře Popis skupiny uživatelů na dalších stránkách obrazovky a stiskněte klávesu **Enter**.

```
                       Vytvoření profilu uživatele

                         Přídavné parametry

Zvláštní oprávnění . . . . . .   *USRCLS

   ⋮
Popis úlohy  . . . . . .   DPTSM
  Knihovna . . . . . .   QGPL
```

```
                      Vytvoření profilu uživatele

Skupinové oprávnění. . . . . .   *NONE

   ⋮
Tiskové zařízení . . . . . .   PRT03
```

8. Zkontrolujte zprávy.

Nezapomeňte

Skupinový profil představuje zvláštní typ uživatelského profilu. Mnoho zpráv a obrazovek se odvolává na skupinové profily jako profily uživatelů nebo uživatele. Systém ví pouze to, že jste vytvořili skupinový profil, pokud do něj přidáte členy nebo mu přiřadíte identifikační číslo skupiny (group identification number - gid).

Možná chyba	Náprava
Stiskli jste klávesu **Enter** ještě před zapsáním všech hodnot do skupinového profilu.	Stiskněte**F5** (Obnova) pro přidání profilu, který jste vytvořili, na obrazovku Práce s uživatelskými profily. Pro opravu profilu vyberte volbu **2** (Změna).
Vytvořili jste profil s nesprávným jménem.	Nemůžete měnit jméno profilu. Pro vytvoření nového profilu se správným jménem použijte volbu pro kopírování (**3**). Potom vymažte (volba **4**) profil s nesprávným jménem.

Možná chyba	Náprava
Některá z polí z formuláře Popis skupiny uživatelů se neobjeví na obrazovce.	Ujistěte se, že používáte úroveň ″intermediate assistance″. Úroveň ″basic assistance level″ u obrazovky Vytvoření profilu uživatele se nazývá obrazovka Přidání uživatele. Chcete-li změnit úroveň asistence, stiskněte klávesu **F12** (Zrušení), kterou se vrátíte na obrazovku Work with User Enrollment. Ke změně úrovní asistence použijte klávesu **F21**. Informace najdete v tématu ″Výběr správné úrovně asistence″.
Neúmyslně jste vymazali některou z předvolených informací z obrazovky Vytvoření uživatele.	Pokud ponecháte pole prázdné, systém použije při tvorbě uživatelského profilu předvolenou hodnotu. Pokud chcete vidět předvolené hodnoty, stiskněte klávesu **F5** (Obnova), kterou se obnoví celá obrazovka. Znovu napište vaši informaci.

Výpis vašich výsledků

Seznam jmen a popisů všech profilů v systému procházejte pomocí příkazu DSPAUTUSR (Zobrazení oprávněných uživatelů). Napište příkaz DSPAUTUSR OUTPUT(*PRINT). Zkontrolujte, zda mají všechny skupinové profily heslo *NONE.

Následující úkony proveďte před nastavením individuálních uživatelů :

- Pro každou skupinu uživatelů vytvořte popis úlohy.
- Volitelně vytvořte pro každou skupinu knihovnu.
- Pro každou skupinu uživatelů vytvořte skupinový profil.

Nastavení individuálních uživatelů

Jakmile jste vytvořili skupiny uživatelů, dokončili jste kroky potřebné pro vytvoření skupinových profilů. Nyní vytvoříte profily individuálních uživatelů pro členy skupin.

Proveďte všechny kroky v rámci celého tématu u členů jedné skupiny uživatelů, potom se vraťte zpět a zopakujte kroky pro zbývající skupiny. Vzorové obrazovky zobrazují uživatele z formuláře Profil individuálního uživatele, které Sharon Jonesová připravila pro oddělení prodeje a marketingu a skladové oddělení firmy JKL Toy Company. Kopie těchto formulářů můžete najít v tématu ″Plánování profilů individuálních uživatelů″.

Použijte formuláře Profil individuálního uživatele, které jste připravili během práce s částí″ Plánování profilů individuálních uživatelů″.

Pro vytvoření individuálních profilů pro členy skupin musíte dokončit tyto úlohy:

1. Vytvořte osobní knihovnu (volitelné).
2. Zkopírujte skupinový profil.
3. Nastavte dočasnou platnost hesla.
4. Vytvořte další uživatele (volitelné).

   Poznámka: Opakujte postup pro vytvoření osobní knihovny a vytvoření dalšího uživatele, dokud každý člen skupiny nebude mít uživatelský profil.
5. Změňte informace o uživateli, pokud to je zapotřebí.
6. Zobrazte své výsledky.

Přihlášení do systému

Profil Váš vlastní (vyžaduje se oprávnění *SECADM)

Menu SETUP

Vytvoření osobní knihovny

Abyste mohli začít s nastavováním individuálních uživatelů, bude možná zapotřebí vytvořit osobní knihovnu každého člena pro objekty, jako jsou například programy Query. Před vytvořením profilů individuálních uživatelů vytvořte osobní knihovny.

1. Napište příkaz **CRTLIB** a stiskněte **F4** (Náznak).
2. Knihovně dejte stejné jméno, jaké má uživatelský profil.
3. Stiskněte klávesu **F10** (Přídavné parametry).
4. Vyplňte veřejné oprávnění ke knihovně a k novým objektům, které jsou vytvořeny v knihovně.
5. Stiskněte klávesu **Enter**. Zkontrolujte potvrzující zprávu.

```
                          Vytvoření knihovny

Zapište volby, stiskněte Enter.

Knihovna . . . . . .   DPTSM
Typ knihovny . . . . . .   *PROD
Text . . . . . .   Knihovna skladu

                          Přídavné parametry

Oprávnění  . . . . . .   *EXCLUDE
ID ASP . . . . . .   1
Vytvořit oprávnění . . . . . .   *CHANGE
Create object auditing . . . . .   *SYSVAL
```

Po vytvoření osobní knihovny můžete vytvořit profil individuálního uživatele zkopírováním skupinového profilu.

Kopírování skupinového profilu

Skupinový profil má dvě úlohy:

1. Systém jej používá k určení, zda je člen skupiny oprávněn k užívání objektu.
2. Můžete jej využít jako vzor pro vytvoření uživatelských profilů pro jednotlivé členy skupiny.

Jakmile jste vytvořili skupiny uživatelů, vytvořili jste skupinové profily. Nyní můžete zkopírovat skupinový profil, abyste vytvořili profil individuálního uživatele, a ten pak zkopírovat za účelem vytvoření jiných profilů ve skupině.

1. Vyberte volbu Work with User Enrollment z menu SETUP.

   Poznámka: Pokud se objeví obrazovka Práce s uživatelskými profily, použijte klávesu **F21** (Výběr úrovně asistence) za účelem změny úrovně na ″basic assistance level″.

2. Napište volbu **3** (Kopie) do sloupce *Vol* před skupinu uživatelů. Zobrazí se obrazovka Kopie uživatele. (Pokud skupina uživatelů, kterou chcete kopírovat, není na obrazovce, procházejte pomocí klávesy Page Down obrazovku, dokud danou skupinu nenajdete.) Systém ponechává pole se jménem uživatele prázdné a vyplňuje zbývající pole ze skupinového profilu, který jste zkopírovali.

```
                        Work with User Enrollment

Type options below, then press Enter.
  1=Add   2=Change   3=Copy   4=Remove   5=Display

Opt     User           Description

        DPTSM          Sales and Marketing Department
3       DPTWH          Warehouse Department
```

3. Napište jméno a popis uživatelského profilu, který vytváříte.
4. Heslo nevyplňujte. Systém automaticky vytvoří heslo, které je stejné jako nové jméno uživatelského profilu.

5. Jméno skupinového profilu umístěte do pole *User group*.
6. Zkontrolujte formulář Profil individuálního uživatele a zjistěte, zda má tento uživatel nějaké hodnoty, které se liší od skupiny. Zadejte tyto hodnoty.
7. Odstránkujte dolů.

```
                              Kopie uživatele

Kopírování z uživatele . . . :   DPTWH

Zapište dole volby, pak stiskněte Enter.

Uživatel. . . . . . . . . .   WILLISR
Uživatelský popis . . . .   Willis, Rose
Heslo . . . . . . . . . . .
Typ uživatele . . . . . .   *SYSOPR
Uživatelská skupina   . .   DPTWH

Omezené použití
  příkazového řádku . . .   N

Předvolená knihovna . . .   DPTWH
Předvolená tiskárna . . .   PRT04
Přihlašovací program  . .   *NONE
  Knihovna  . . . . . . . .

První menu  . . . . . . . .   ICMAIN
  Knihovna. . . . . . . . .   ICPGMLIB
```

8. Na další stránce obrazovky proveďte všechny nezbytné změny a stiskněte klávesu **Enter**.
9. Zkontrolujte potvrzující zprávy v dolní části obrazovky Work with User Enrollment.

```
                                Kopie uživatele

Kopírování z uživatele . . . :   DPTWH

Zapište dole volby, pak stiskněte Enter.

Program klávesy Attention . .   *SYSVAL
  Knihovna  . . . . . . . . .
```

Možná chyba	Náprava
Vidíte obrazovku Vytvoření profilu uživatele místo obrazovky Kopie uživatele.	Použitím klávesy **F12** (Zrušení) se vrátíte na obrazovku Práce s uživatelskými profily. Použijte klávesu **F21** pro změnu úrovně asistence na ″basic assistance level″. Spusťte znovu operaci kopírování.
Jméno uživatelského profilu, který jste vybrali, neodpovídá uživatelskému náznaku.	Ačkoliv mohou mít jména uživatelského profilu až 10 znaků, obrazovky Kopie uživatele a Přidání uživatele podporují jména tvořená maximálně 8 znaky. Zvolte buď kratší uživatelské jméno, nebo k vytvoření profilů individuálních uživatelů použijte úroveň asistence ″intermediate assistance″.

Testování uživatelského profilu

Při vytváření prvního profilu individuálního uživatele ve skupině byste jej měli otestovat formou přihlášení s tímto profilem. Zkontrolujte, zda vidíte správné počáteční menu a zda probíhá přihlášení do systému.

Pokud se nemůžete úspěšně přihlásit do systému s tímto profilem, systém pravděpodobně nemohl v tomto profilu něco specifického najít. Mohlo by se jednat o program přihlášení do systému, o popis úlohy nebo o jednu z knihoven uvedených na počátečním seznamu knihoven. Pro nalezení protokolu úlohy, která byla zapsána při vašem pokusu o přihlášení se do systému, použijte obrazovku Work with Printer Output. Protokol úlohy vás informuje o tom, k jaké chybě došlo.

Informace o testování a diagnostice problémů během provádění změn v zabezpečení najdete v tématu ″Testování zabezpečení″.

Po otestování uživatelského profilu můžete nastavit dočasnou platnost hesla.

Nastavení dočasné platnosti hesla

Nastavte individuální profily na požadavek, aby uživatelé měnili svá hesla při prvním přihlášení do systému. Pole *Nastavit heslo na ukončení platnosti* se neobjevuje na úrovni ″basic assistance level″ obrazovky Kopie uživatele. Musíte provést změnu samostatně, po vytvoření uživatelského profilu, a to pomocí funkce kopírování. Chcete-li změnit pole *Nastavit heslo na ukončení platnosti*, napište příkaz CHGUSRPRF *jméno-profilu* PWDEXP(*YES).

Poznámka: Chcete-li vyzkoušet uživatelský profil přihlášením se do systému s tímto profilem, proveďte test *předtím*, než nastavíte dočasnou platnost hesla.

Možná chyba	Náprava
Testovali jste profil a byli jste nuceni provést změnu hesla.	Napište příkaz **CHGUSRPRF** *jméno-profilu* a stiskněte klávesu **F4** (Náznak). Nastavte heslo zpátky na jméno uživatelského profilu. Do pole pro heslo napište název uživatelského profilu. Napište ***YES** do pole *Nastavit heslo na ukončení platnosti*. K provedení tohoto kroku potřebujete úroveň ″intermediate assistance″.

Po vytvoření prvního profilu individuálního uživatele můžete vytvořit další uživatele.

Vytvoření dalších uživatelů

Po zkopírování skupinového profilu za účelem vytvoření prvního profilu individuálního uživatele můžete vytvořit další uživatele. Zkopírujte první profil individuálního uživatele a vytvořte další členy skupiny. Při vytváření individuálních profilů pomocí kopírování každý individuální profil pečlivě zkontrolujte. Zkontrolujte si formulář Profil individuálního uživatele a ověřte, zda jste provedli změnu u všech polí, která jsou jedinečná z hlediska profilu nového uživatele.

1. .a obrazovku Work with User Enrollment napište před uživatelský profil, který chcete kopírovat, volbu **3** (Kopie).
2. Na obrazovce Kopie uživatele zadejte jméno a popis profilu.
3. Zadejte informace do všech polí, která jsou jedinečná z hlediska nového uživatele.

```
                        Work with User Enrollment

Type options below, then press Enter.
  1=Add   2=Change   3=Copy   4=Remove   5=Display

Opt     User           Description

        DPTSM          Sales and Marketing Department
        DPTWH          Warehouse Department
3       WILLISR        Willis, Rose
```

Možná chyba	Náprava
Profil, který chcete kopírovat, se neobjeví na obrazovce Work with User Enrollment.	Stiskněte klávesu **F5** (Obnova). Prohledávejte pomocí kláves Page up a Page down. Seznam je uspořádán podle abecedního pořadí jmen profilu.

Pokud byste chtěli pozměnit informace o uživateli, prostudujte si téma Změna informací o uživateli.

Změna informací o uživateli

U některých uživatelů bude možná zapotřebí nastavit hodnoty, které se neobjevují na obrazovce Kopie uživatele. Někteří uživatelé mohou například patřit do více než jednoho skupinového profilu. Po vytvoření uživatelského profilu metodou kopírování jej můžete změnit.

1. Na obrazovce Work with User Enrollment stiskněte **F21**, čímž změníte intermediate assistance.
2. Na obrazovce Práce s uživatelskými profily napište **2** (Změna) ve sloupci *Vol* vedle profilu, který chcete změnit. Stiskněte klávesu **Enter**.

```
                          Práce s uživatelskými profily

Zapište volby, stiskněte Enter.
  1=Vytvoření   2=Změna   3=Kopie   4=Výmaz   5=Zobrazení
  12=Práce s objekty dle vlastníka

     Uživatelský
Vol    profil     Text
2    AMESJ       Ames, Janice
     DPTSM       Oddělení prodeje a marketingu
     QDOC        Dokumentace uživatelského profilu
     QSECOFR     Uživatelský profil správce systému
     WAGNERR     Wagner, Ray
     WILLISR     Willis, Rose
```

3. Na obrazovce Změna profilu uživatele stiskněte **F10** (Přídavné parametry).
4. Klávesou Page down vyhledejte pole, které chcete změnit. Chcete-li například definovat jako uživatele člena dalších skupinových profilů, pomocí Page down vyhledejte pole *Doplňkové skupiny*.
5. Napište hodnotu, kterou požadujete, a stiskněte klávesu **Enter**. Obdržíte potvrzující zprávu a uvidíte opět obrazovku Práce s uživatelskými profily.

```
                          CHGUSRPRF (Změna profilu uživatele)

Zapište volby, stiskněte Enter.

Maximum povolené paměti  . . . .   *NOMAX
Nejvyšší plánovaná priorita. . .   3
Popis úlohy  . . . . . . . . . .   DPTWH
  Knihovna . . . . . . . . . . .     QGPL
Skupinový profil . . . . . . . .   DPTWH
Vlastník . . . . . . . . . . . .   *GRPPRF
Skupinové oprávnění. . . . . . .   *USEE
Typ skup. oprávnění  . . . . . .   *PGP
Doplňkové skupiny  . . . . . . .   DPTIC
               + další hodnoty
```

Po provedené změně uživatelských informací můžete pro kontrolu svých profilů zobrazit výsledky.

Zobrazení uživatelských profilů

Chcete-li zobrazit profily, které jste vytvořili, nabízí se několik metod.

Zobrazení jednoho profilu

Použijte volbu **5** (Zobrazení) buď z obrazovky Work with User Enrollment, nebo z obrazovky Práce s uživatelskými profily.

Výpis jednoho profilu

Použijte příkaz Zobrazení uživatelského profilu: DSPUSRPRF *jméno-profilu* DETAIL(*BASIC) OUTPUT(*PRINT).

Zobrazení členů skupiny

Napište příkaz DSPUSRPRF *jméno-skupinového-profilu* *GRPMBR. K vytisknutí seznamu můžete použít příkaz OUTPUT(*PRINT).

Výpis všech profilů

Chcete-li získat jména a popisy všech profilů roztříděných podle skupin, použijte příkaz Zobrazení oprávněných uživatelů: DSPAUTUSR SEQ(*GRPPRF) OUTPUT(*PRINT).

Před nastavením vlastnictví a veřejného oprávnění se ujistěte, zda jste dokončili následující úkoly:

- Dokončit vytvoření všech profilů individuálních uživatelů.
- Nastavit dočasnou platnost hesla pro každý profil.
- Vytisknout seznam všech profilů setříděných podle skupin a uložit jej u formulářů Popis skupiny uživatelů. Po přidání nových uživatelů seznam znovu vytiskněte.

Nastavení zabezpečení prostředků

V rámci tohoto tématu vytvoříte vlastnictví a veřejné oprávnění k objektům a také specifické oprávnění k vašim aplikacím. Zároveň nastavíte zabezpečení prostředků pro pracovní stanice a tiskárny. Nejprve projděte celé téma u jedné knihovny, potom se vraťte a opakujte postup pro všechny další knihovny, které aplikace používá. Až dokončíte nastavení zabezpečení prostředků pro jednu aplikaci, opakujte kroky u dalších aplikací.

Tento postup používejte vždy, když instalujete novou aplikaci do systému, nebo tehdy, když nastavujete zabezpečení prostředků pro existující aplikaci.

Vzorové obrazovky v tomto tématu zobrazují formuláře Seznam oprávnění, Popis knihovny a Zabezpečení výstupních front a pracovních stanic pro společnost JKL Toy Company. Příklady těchto formulářů můžete nalézt v tématu ″Nastavení vlastnictví a veřejného oprávnění″.

Jaké formuláře použít?

- Formuláře Instalace aplikace, které jste si připravili v tématu ″ Plánování instalace aplikací″.
- Formuláře Seznam oprávnění, které jste si připravili v tématu ″Seskupování objektů″.
- Formuláře Popis knihovny, které jste si připravili v tématu ″Určení vlastnictví knihoven a objektů″.
- Formulář Zabezpečení výstupních front a pracovních stanic, který jste si připravili v tématu ″Ochrana tiskového výstupu″ a ″Ochrana pracovních stanic″.
- Formulář Odpovědnost za systém, který jste si připravili v tématu ″Plánování celkové strategie zabezpečení″.

Zabezpečení prostředků můžete nastavit několika způsoby. Posloupnost kroků v tomto tématu odpovídá pořadí informací na formulářích Instalace aplikace, Seznam oprávnění a Popis knihovny:

1. Nastavení vlastnictví a veřejného oprávnění.
2. Vytvoření seznamů oprávnění.
3. Zabezpečení objektů pomocí seznamu oprávnění.
4. Přidání uživatelů do seznamů oprávnění.
5. Nastavení všech specifických oprávnění.
6. Zabezpečení tiskového výstupu.
7. Zabezpečení pracovních stanic.
8. Omezení přístupu k frontě zpráv operátora systému.

Nastavení vlastnictví a veřejného oprávnění

Obsahem tohoto tématu je nastavení vlastnictví a veřejného oprávnění ke knihovnám aplikací, skupinovým knihovnám a osobním knihovnám. Celé téma projděte u jedné aplikace, potom se vraťte a opakujte kroky pro všechny další aplikace. Vzorové obrazovky ukazují formuláře Instalace aplikace, které Sharon Jonesová připravila pro aplikaci Zákaznické objednávky v tématu ″Plánování instalace aplikací″.

Procedury uvedené v tomto tématu použijte vždy v případech, kdy do systému instalujete novou aplikaci nebo když nastavujete zabezpečení pro stávající aplikaci.

Použijte formuláře Instalace aplikace, které jste si připravili v tématu Plánování instalace aplikací.

Pro nastavení vlastnictví a veřejného oprávnění je třeba dokončit tyto úkoly:

1. Vytvořte profil vlastníka.
2. Změňte vlastnictví knihovny.
3. Nastavte vlastnictví objektů aplikace.
4. Nastavte veřejný přístup ke knihovně.
5. Nastavte veřejné oprávnění ke všem objektům v knihovně.
6. Nastavte veřejné oprávnění k novým objektům.
7. Proveďte práci se skupinovými a osobními knihovnami.

Přihlášení do systému

Profil Váš vlastní (vyžaduje se oprávnění *ALLOBJ)

Menu MAIN

Vytvoření profilu vlastníka

V případě, že neexistuje profil vlastníka, postupujte následujícím způsobem:

- Vytvořte jej pomocí příkazu CRTUSRPRF (Vytvoření uživatelského profilu). Heslo nastavte na *NONE.

Pokud profil vlastníka již existuje, postupujte takto:

- Pomocí příkazu CHGUSRPRF (Změna uživatelského profilu) nastavte heslo na *NONE.

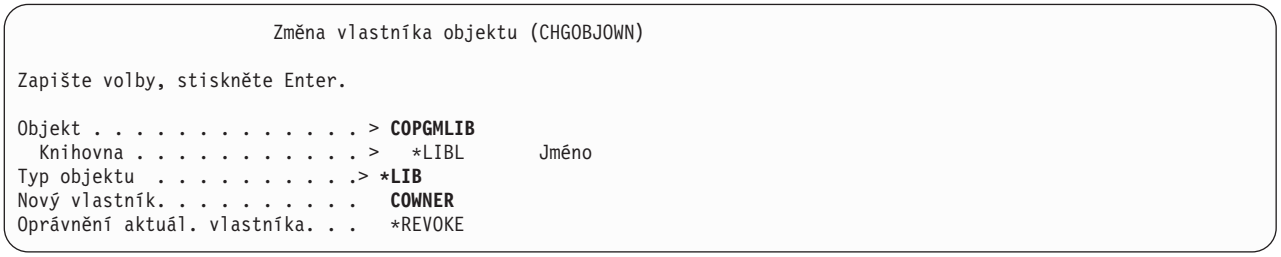
Po vytvoření profilu vlastníka můžete změnit vlastnictví knihovny.

Změna vlastnictví knihovny

Tímto krokem se mění vlastnictví knihovny, nikoliv objekty v knihovně.

Upozornění: Před provedením změny vlastnictví jakýchkoliv objektů aplikace se nezapomeňte obrátit na dodavatele vaší aplikace. Některé aplikace používají funkce, které spoléhají na specifické vlastnictví objektů.

1. Napište příkaz CHGOBJOWN (Změna vlastníka objektu) a stiskněte klávesu **F4** (Náznak).
2. Vyplňte jméno knihovny, typ objektu (*LIB) a nového vlastníka.
3. Zkontrolujte potvrzující zprávy.



Možná chyba	Náprava
Obdržíte chybovou zprávu.	Nejčastěji se jedná o zprávu, že buď nebyla nalezena knihovna, nebo nebyl nalezen profil nového vlastníka. Zkontrolujte, zda jste při psaní neudělali nějaké chyby a pak to zkuste znovu.

Po provedení změny vlastnictví knihovny můžete nastavit vlastnictví pro objekty aplikace.

Nastavení vlastnictví u objektů aplikace

Změna vlastnictví objektů aplikace představuje nepříjemný úkol, protože je zapotřebí měnit každý objekt jednotlivě. Je-li to možné, požádejte dodavatele programu nebo aplikace, aby pro vás vlastnictví vytvořil.

Výpis objektů nacházejících se v knihovně

Před provedením změny vlastnictví vytiskněte seznam všech objektů, které se nacházejí v knihovně. K tomu použijte příkaz Zobrazení knihovny. Můžete jej použít jako kontrolní seznam. Napište DSPLIB *jméno-knihovny* *PRINT.

Volba optimální metody

Vyberte si jednu z níže uvedených dvou metod používaných pro změnu vlastnictví objektů v knihovně aplikací:

Tabulka 61. Metody změny vlastnictví objektů

Metoda	Jak funguje	Kdy ji použít
Příkaz WRKOBJOWN (Práce s objekty dle vlastníka)	Ukáže se obrazovka, kde je uveden seznam všech objektů, které profil vlastní. K provedení změny vlastníka objektu použijte volbu na obrazovce.	Tato metoda je snadněji použitelná. Pokud však vlastní objekty buď profil QPGMR, nebo profil QSECOFR, IBM tuto metodu nedoporučuje. Tyto profily vlastní mnoho objektů a seznam uvedený na obrazovce by byl velice dlouhý.
Příkaz CHGOBJOWN (Změna vlastnictví objektu)	Je nutný samostatný příkaz pro každý objekt. Můžete však použít příkaz *Načtení* (**F9**), kterým zopakujete předcházející příkaz a omezíte množství nutného psaní.	Tato metoda je rychlejší, pokud objekty vlastní buď profil QPGMR, nebo profil QSECOFR.

Používání příkazu WRKOBJOWN (Práce s objekty dle vlastníka): Tuto metodu používejte ke změně vlastnictví objektů v knihovně, pokud profily dodávané IBM, jako jsou například QPGMR nebo QSECOFR, *ne*vlastní objekty:

1. Napište příkaz WRKOBJOWN *jméno-profilu-vlastníka*. Na obrazovce se ukáže seznam všech objektů, které tento uživatelský profil vlastní.
2. Napište volbu **9** (Změna vlastníka) před každý z objektů v knihovně, na kterém pracujete.
3. Na řádek *Parametery nebo příkaz*, který se nachází ve spodní části obrazovky, napište NEWOWN(*jméno-profilu-vlastníka*) a stiskněte klávesu **Enter**.
4. Systém provede u každého označeného objektu změnu z původního vlastníka na nového vlastníka, kterého jste napsali ve spodní části. Ve spodní části obrazovky se objeví potvrzující zprávy. Objekty se již na obrazovce neobjeví, protože je profil již nevlastní.
5. Kroky 2 a 4 opakujte, dokud neprovedete změnu vlastnictví u všech objektů nacházejících se v knihovně.

```
                          Práce s objekty dle vlastníka

Uživatelský profil . . . . :   OLDOWNER

Zapište volby, stiskněte Enter.
  2=Změna oprávnění       4=Výmaz   5=Zobrazení oprávnění
  8=Zobrazení popisu      9=Změna vlastníka

Vol  Objekt        Knihovna      Typ      Atribut
     COPGMMSG      COPGMLIB      *MSGQ
9    CUSTMAS       CUSTLIB       *FILE
9    CUSTMSGQ      CUSTLIB       *MSGQ
     ITEMMSGQ      ITEMLIB       *MSGQ


   ⋮

Parametry nebo příkaz
===> NEWOWN(COWNER)
F3=Konec   F4=Náznak   F5=Obnova   F9=Vyvolání
F18=Konec seznamu
```

Možná chyba	Náprava
Vidíte obrazovku Změna vlastníka objektu.	Tuto obrazovku vidíte, pokud zadáte volbu **9** (Změna vlastníka) a do spodní části obrazovky Práce s objekty dle vlastníka nezapíšete žádné parametry. Tato obrazovka se objeví v případě, že parametry zapíšete nesprávně. Stiskněte klávesu **F12** (Zrušení); vrátíte se na obrazovku Práce s objekty dle vlastníka. Zkuste to znovu. Zkontrolujte si, zda jste parametr napsali tak, jak uvádí příklad.

Můžete použít příkaz CHGOBJOWN (Změna vlastníka objektu) k provedení změny vlastnictví u objektů, které vlastní profil QPGMR nebo QSECOFR.

Používání příkazu CHGOBJOWN (Změna vlastníka objektu): Tuto metodu použijte, pokud chcete změnit vlastnictví objektů v knihovně, v případě, že profily QPGMR nebo QSECOFR *vlastní* nějaké objekty.

1. Napište příkaz CHGOBJOWN a stiskněte klávesu **F4** (Náznak).
2. Na obrazovce vyplňte informace týkající se prvního objektu z vašeho seznamu a stiskněte klávesu **Enter**.

```
                       Změna vlastníka objektu (CHGOBJOWN)

Zapište volby, stiskněte Enter.

Objekt . . . . . . . . . . . . . > CUSTMAS
  Knihovna . . . . . . . . . . . >   CUSTLIB
Typ objektu  . . . . . . . . . . > *FILE
Nový vlastník. . . . . . . . . .  COWNER
Oprávnění aktuál. vlastníka. . .   *REVOKE
```

3. Dostanete potvrzující zprávu o provedení změny ve vlastnictví objektů. Zaškrtněte položku seznamu.
4. Stiskněte klávesu **F9** (Načtení) k vyhledání napsaného příkazu.
5. Stiskněte klávesu **F4** (Náznak). Na obrazovce Změna vlastníka objektu zadejte informace týkající se následujícího objektu v knihovně a stiskněte klávesu **Enter**.
6. U každého objektu v knihovně zopakujte kroky čtyři a pět.

Kontrola práce

Chcete-li se přesvědčit, zda jste změnili vlastnictví u všech objektů v knihovně, použijte příkaz WRKOBJOWN (Práce s objekty dle vlastníka). Napište příkaz WRKOBJOWN *profil-nového-vlastníka*. Porovnejte obrazovku se seznamem objektů v knihovně.

Po provedení změny vlastnictví objektů v knihovně můžete nastavit veřejný přístup ke knihovně.

Nastavení veřejného přístupu ke knihovně

Po nastavení vlastnictví objektů aplikace můžete použít příkaz EDTOBJAUT (Editování oprávnění k objektu), kterým změníte veřejné oprávnění ke knihovně:

1. Napište EDTOBJAUT *jméno-knihovny* *LIB.
2. Přemístěte kurzor svisle na řádek, kde je uvedeno **PUBLIC*.
3. Napište oprávnění, u kterého chcete nastavit veřejný přístup ke knihovně, a stiskněte klávesu **Enter**.

```
                          Editování oprávnění k objektu

Objekt . . . . . :   CUSTLIB         Vlastník  . . . . . :   COWNER
  Knihovna  . . . . . :    QSYS          Primární skupina  . . . :   *NONE
Typ objektu  . . . . :   *LIB

Zapište změny aktuálních oprávnění, stiskněte Enter.

  Objekt je zabezpečený seznamem oprávnění  . . . . . .   --

                         Oprávnění
Uživatel        Skupina      k
COWNER                   objektu
*PUBLIC                  *CHANGE
```

4. Na obrazovce se ukáže nové oprávnění.

Nyní můžete nastavit veřejné oprávnění ke všem objektům v knihovně.

Nastavení veřejného oprávnění ke všem objektům v knihovně

Pro odstranění aktuálního veřejného oprávnění k objektům v knihovně použijte příkaz RVKOBJAUT (Zrušení oprávnění k objektu). Pro nastavení veřejného oprávnění ke všem objektům v knihovně použijte příkaz GRTOBJAUT (Udělení oprávnění k objektu):

1. Napište RVKOBJAUT a stiskněte **F4** (Náznak).
2. Vyplňte obrazovku uvedeným způsobem a současně nahraďte jméno vaší knihovny aplikací a stiskněte klávesu **Enter**.

```
                    Zrušení oprávnění k objektu (RVKOBJAUT)

Zapište volby, stiskněte Enter.

Objekt . . . . . .   *all
  Knihovna . . . . . .     custlib
Typ objektu  . . . . . .   *all
Uživatelé  . . . . . .   *public
             + další hodnoty
Oprávnění  . . . . . .   *all
```

Poznámka: Pokud má knihovna větší počet objektů, může trvat několik minut, než systém zpracuje váš požadavek.

3. Napište GRTOBJAUT a stiskněte klávesu **F4** (Náznak).
4. Vyplňte obrazovku uvedeným způsobem, nahraďte jméno vaší knihovny aplikací a požadované oprávnění a stiskněte klávesu **Enter**.

```
                    Udělit oprávnění k objektu (GRTOBJAUT)

Zapište volby, stiskněte Enter.

Objekt . . . . . .   *all
  Knihovna . . . . . .    custlib
Typ objektu  . . . . . .   *all
Uživatelé  . . . . . .   *public
             + další hodnoty
Oprávnění  . . . . . .   *use
```

Poznámka: Pokud má knihovna větší počet objektů, může trvat několik minut, než systém zpracuje váš požadavek.

Po dokončení nastavení veřejného oprávnění ke všem objektům v knihovně můžete pro kontrolu další práce použít protokol úlohy.

Použití protokolu úlohy ke kontrole práce: Pokud k provedení vícenásobných změn oprávnění použijete příkaz GRTOBJAUT, prohlédněte si protokol úlohy, abyste se přesvědčili, že změny byly skutečně provedeny.

1. Napište DSPJOBLOG (Zobrazení protokolu úloh).
2. Stiskněte klávesu **F10** (Zobrazení podrobných zpráv).
3. Měli byste dostat zprávu o změně oprávnění ke každému objektu nacházejícímu se v knihovně. Při kontrole zpráv si odškrtávejte objekty uvedené na vašem seznamu.

```
                           Zobrazení zpráv
                         Systém:   RCHASxxx
Úloha . . :   QPADEV0010    Uživatel . . :   JCHEIDEL      Číslo . . . :   025457

7 > GRTOBJAUT OBJ(CUSTLIB/*ALL) OBJTYPE(*ALL) USER(*PUBLIC) AUT(*USE)
  Oprávnění uděleno uživateli *PUBLIC k objektu CUSTMAS v CUSTLIB typ objektu
    *FILE.
  Oprávnění uděleno uživateli *PUBLIC k objektu CUSTMSGQ v CUSTLIB typ objektu
    *MSGQ.
  Oprávnění uděleno ke 2 objektům. Nebylo uděleno k 0 objektům. Částečně uděleno k 0
    objektům.
  Uděleno oprávnění k objektu.
7>> dspjoblog
```

Možná chyba	Náprava
Váš protokol úlohy indikuje, že některé objekty v knihovně nebyly změněny.	Použijte nápovědu (**F1**), kde získáte více informací týkajících se této zprávy. Pomocí příkazu EDTOBJAUT nastavíte oprávnění k těmto objektům individuálně.

Nyní můžete nastavit veřejné oprávnění k novým objektům.

Nastavení veřejného oprávnění k novým objektům

Popis knihovny má parametr označovaný jako CRTAUT (Vytvoření oprávnění) určující veřejné oprávnění k novým objektům, které jsou vytvořeny v knihovně. Příkazy, které vytvářejí objekty, používají oprávnění CRTAUT knihovny objektů jako předvolbu. Pro knihovnu byste měli vytvořit parametr CRTAUT stejný jako veřejné oprávnění k většině existujících objektů v knihovně.

1. Napište příkaz CHGLIB *jméno-knihovny* a stiskněte klávesu **F4** (Náznak).
2. Stiskněte klávesu **F10** (Přídavné parametry).
3. Zadejte volbu do pole *Vytvořit oprávnění*.

```
                    Změna knihovny (CHGLIB)

Zapište volby, stiskněte Enter.

Knihovna  . . . . . . . . . . . . > CUSTLIB
Typ knihovny  . . . . . . . . . .   *PROD
Text  . . . . . . . . . . . . . .   'Záznamy zákazníka'


                    Přídavné parametry

Vytvořit oprávnění . . . . . .   *CHANGE
Create object auditing . . . . .   *SYSVAL
```

Pokud nastavíte parametr CRTAUT k hodnotě *SYSVAL, systém použije aktuální nastavení pro systémovou hodnotu QCRTAUT v případě, že vytvoříte v knihovně nový objekt. Nastavení specifického oprávnění CRTAUT ke každé knihovně poskytuje ochranu proti budoucím změnám systémové hodnoty QCRTAUT.

Nyní můžete pracovat se skupinovými a osobními knihovnami.

Práce se skupinovými a osobními knihovnami

Váš profil vlastní skupinové a osobní knihovny, které jste vytvořili při nastavování skupinových a individuálních uživatelů.

Použijte výše uvedené procedury ke změně vlastnictví ze skupinových knihoven na skupinový profil a změny z osobních knihoven na profily individuálních uživatelů. Použijte příkaz EDTOBJAUT.

Nastavte parametr CRTAUT pro každou skupinovou a osobní knihovnu za účelem stanovení veřejného oprávnění ke všem novým objektům v těchto knihovnách. Použijte příkaz CHGLIB.

Ještě než začnete vytvářet seznamy oprávnění, dokončete tyto úkoly:

- Použijte formuláře Instalace aplikace a Popis knihovny a ujistěte se, že jste vytvořili záznam o vlastnictví a veřejné oprávnění ke všem knihovnám aplikací.
- Nastavte vlastnictví a vytvořte oprávnění ke všem skupinovým a osobním knihovnám, které jste vytvořili.

Poznámka: Můžete získat seznam všech knihoven nacházejících se ve vašem systému tím, že napíšete příkaz DSPOBJD *ALL *LIB *PRINT.

Vytvoření seznamu oprávnění

Po nastavení vlastnictví a veřejného oprávnění jste připraveni instalovat seznamy oprávnění. Na základě informací uvedených ve formulářích Seznam oprávnění vytvořte všechny seznamy oprávnění, které jsou zapotřebí pro zabezpečení knihovny. Použijte příkaz CRTAUTL (Vytvoření seznamu oprávnění):

1. Napište příkaz CRTAUTL a stiskněte klávesu **F4** (Náznak).
2. Vyplňte informace, které jsou uvedeny ve formuláři Seznam oprávnění.
3. Stiskněte klávesu **F10** (Přídavné parametry).
4. Pomocí parametru oprávnění specifikujte veřejné oprávnění k objektům, které jsou zabezpečeny seznamem.
5. Zkontrolujte potvrzující zprávy.

```
                    Vytvoření seznamu oprávnění (CRTAUTL)

Zapište volby, stiskněte Enter.

Seznam oprávnění . . . . . .   custlst1
Text . . . . . .   Files cleared at

                        Přídavné parametry

Oprávnění  . . . . . .   *ALL
```

Možná chyba	Náprava
Nesprávně jste zapsali jméno seznamu.	Jakmile systém vytvořil jméno seznamu, není možné jej měnit. Vymažte seznam (DLTAUTL) a zkuste to znovu.
Zapomněli jste specifikovat veřejné oprávnění k seznamu.	Použijte příkaz EDTAUTL (Editování seznamu oprávnění).

Nyní můžete zabezpečit objekty pomocí seznamu oprávnění.

Zabezpečení objektů pomocí seznamu oprávnění

Jakmile jste vytvořili seznam oprávnění, pomocí příkazu EDTOBJAUT (Editování oprávnění k objektu) zabezpečte položky uvedené ve formuláři Seznam oprávnění:

1. Napište EDTOBJAUT a stiskněte klávesu **F4** (Náznak).
2. Vyplňte náznakovou obrazovku a stiskněte klávesu **Enter**.
3. Na obrazovce Editování oprávnění k objektu zadejte jméno seznamu oprávnění.
4. Pokud veřejné oprávnění k objektu pochází ze seznamu oprávnění, změňte veřejné oprávnění na *AUTL.
5. Tento postup opakujte u každého objektu uvedeného ve formuláři Seznam oprávnění.

```
                          Editování oprávnění k objektu

Objekt . . . . . :   ARFILE01        Vlastník  . . . . . :   OWNAR
  Knihovna  . . . . . :     CUSTLIB       Primární skupina  . . . :   *NONE
Typ objektu  . . . . :   *FILE

Zapište změny aktuálních oprávnění, stiskněte Enter.

  Objekt je zabezpečený seznamem oprávnění . . . . . .    CUSTLST1

                          Oprávnění
Uživatel        Skupina    k objektu
OWNER                      *ALL
*PUBLIC   *AUTL
```

Nyní můžete přidat uživatele do seznamu oprávnění.

Přidání uživatelů do seznamu oprávnění

Po zabezpečení objektů pomocí seznamu oprávnění použijte příkaz EDTAUTL (Editování seznamu oprávnění), kterým se přidají uživatelé uvedení ve formuláři Seznam oprávnění:

1. Napište EDTAUTL *jméno-seznamu-oprávnění*.
2. Na obrazovce Editování seznamu oprávnění stiskněte klávesu **F6** (Přidání nových uživatelů).
3. Zadejte jména uživatelů nebo skupin a oprávnění, která by měli mít k položkám uvedeným na seznamu, a stiskněte klávesu **Enter**.

4. Na seznamu by se měli objevit noví uživatelé.

```
                          Přidání nových uživatelů

Objekt . . . . . :   WSLST1          Vlastník  . .
  Knihovna  . . . . :    QSYS

Zapište nové uživatele, stiskněte Enter.

            Oprávnění       Seznam
Uživatel    k objektu        Říz
QSECOFR    *CHANGE
```

Možná chyba	Náprava
Uživateli nebo skupině jste poskytli nesprávné oprávnění k seznamu.	Oprávnění se může změnit na obrazovce Editování seznamu oprávnění.
Přidali jste do seznamu nesprávného uživatele nebo skupinu.	Uživatele nebo skupinu můžete odstranit pomocí příkazu RMVAUTLE (Odstranění záznamu ze seznamu oprávnění) nebo můžete přepsat mezery přes oprávnění uživatele na obrazovce Editování seznamu oprávnění.

Kontrola práce

Pomocí příkazu DSPAUTL (Zobrazení seznamu oprávnění) projděte seznam všech oprávnění uživatele k seznamu oprávnění. Klávesou **F15** z obrazovky vytvořte seznam všech objektů zabezpečených pomocí seznamu oprávnění.

Před nastavením specifických oprávnění dokončete tyto úkoly:

- Příkazem CRTAUTL vytvořte všechny seznamy oprávnění, které potřebujete pro aplikaci.
- Zabezpečte objekty pomocí seznamů oprávnění příkazem EDTOBJAUT.
- Příkazem EDTAUTL přidejte uživatele do seznamů oprávnění.

Nastavení specifických oprávnění

V části ″Nastavení vlastnictví a veřejného oprávnění″ jste se dozvěděli, jak používat příkaz GRTOBJAUT pro nastavení veřejného oprávnění ke všem objektům v knihovně na základě informací uvedených v části 1 formuláře Popis knihovny. Nyní můžete použít příkaz EDTOBJAUT (Editování oprávnění k objektu), kterým nastavíte specifické oprávnění ke knihovně a k objektům nacházejícím se v knihovně podle informací uvedených v části 2 formuláře Popis knihovny.

Informace o nastavení specifických oprávnění najdete v těchto tématech:

- Nastavení specifického oprávnění ke knihovně.
- Nastavení specifického oprávnění k objektu.
- Nastavení oprávnění k více objektům současně.

Nastavení specifického oprávnění ke knihovně

Knihovna skutečně představuje zvláštní typ objektu. Oprávnění ke knihovně nastavujete stejným způsobem jako ke každému jinému objektu, to znamená příkazem EDTOBJAUT. Všechny knihovny jsou v paměti knihovny dodávané IBM, která je označena názvem QSYS. Obrazovky uvedené v následujících případech používají část 2 formuláře Popis knihovny pro knihovnu CONTRACTS společnosti JKL Toy Company:

Vytvořte seznam specifických oprávnění k objektům knihoven				
Skupinový nebo uživatelský profil	Jméno objektu	Typ objektu	Potřebné oprávnění	Seznam oprávnění

DPTSM	CONTRACTS	*LIB	*USE	
DPTMG	CONTRACTS	*LIB	*USE	

1. Napište příkaz EDTOBJAUT a stiskněte klávesu **F4** (Náznak).
2. Vyplňte náznakovou obrazovku a stiskněte klávesu **Enter**.

```
                     Editování oprávnění k objektu (EDTOBJAUT)

Zapište volby a stiskněte Enter.

Objekt . . . . . . . . . . . . .   CONTRACTS
  Knihovna  . . . . . . . . . . .     QSYS
Typ objektu  . . . . . . . . . .   *LIB
```

3. Na obrazovce Editování oprávnění k objektu stiskněte **F6** (Přidání nových uživatelů) za účelem poskytnutí oprávnění těm uživatelům, které obrazovka nezobrazuje na seznamu.
4. Stiskněte klávesu **Enter**.

```
                              Přidání nových uživatelů

Objekt . . . . . . . :   CONTRACTS       Vlastník  . . . . . . . :   OWNCP
  Knihovna  . . . . . :     QSYS          Primární skupina  . . . :   *NONE
Typ objektu  . . . . :   *LIB


Zapište nové uživatele, stiskněte Enter.

                    Oprávnění
Uživatel            k objektu
DPTSM       *USE
DPTMG       *USE
```

5. Obrazovka Editování oprávnění k objektu by měla odpovídat informacím uvedeným jak v části 1, tak i v části 2 formuláře Popis knihovny.

```
                           Editování oprávnění k objektu
Objekt . . . . . . . :   CONTRACTS       Vlastník  . . . . . . . :   OWNCP
  Knihovna  . . . . . :     QSYS         Primární skupina  . . . :   *NONE
Typ objektu . . . . :   *LIB

Zapište změny aktuálních oprávnění, stiskněte Enter.

  Objekt je zabezpečený seznamem oprávnění  . . . . . . . . . . . .   --

                           Oprávnění
Uživatel    Skupina       k objektu
OWNCP                     *ALL
DPTSM                     *USE
DPTMG                     *USE
*PUBLIC                  *EXCLUDE
```

Veřejné oprávnění k novým objektům (CRTAUT)se nezobrazuje na obrazovce Editování oprávnění k objektu pro knihovnu. Použijte příkaz DSPLIB (Zobrazení knihovny) za účelem zobrazení CRTAUT ke knihovně.

Tento postup můžete také použít pro nastavení specifického oprávnění k objektu v systému.

Nyní můžete nastavit specifické oprávnění k objektu.

Nastavení specifického oprávnění k objektu

Tento postup nastavení specifického oprávnění k objektu v knihovně aplikací je stejný jako nastavení specifického oprávnění ke knihovně. Příklad používá část 2 formuláře Popis knihovny pro knihovnu COPGMLIB JKL Toy Company:

Tabulka 62. Formulář Popis knihovny JKL Toy Company

Skupinový nebo uživatelský profil	Jméno objektu	Typ objektu	Potřebné oprávnění	Seznam oprávnění
PUBLIC	COMSGQ01	*MSGQ	*CHANGE	

1. Napište příkaz EDTOBJAUT a stiskněte klávesu **F4** (Náznak).
2. Vyplňte informace uvedené na náznakové obrazovce a stiskněte klávesu **Enter**.
3. Vyplňte informace týkající se oprávnění na obrazovce Editování oprávnění k objektu a stiskněte klávesu **Enter**.

```
                          Editování oprávnění k objektu
Objekt . . . . . :   COMSGQ01        Vlastník  . . . . . :   OWNCO
  Knihovna  . . . . :     COPGMLIB      Primární skupina  . . . :   *NONE
Typ objektu  . . . . :   *MSGQ

Zapište změny aktuálních oprávnění, stiskněte Enter.

  Objekt je zabezpečený seznamem oprávnění  . . . . . .   --

                          Oprávnění
Uživatel    Skupina       k objektu
OWNCO                    *ALL
*PUBLIC                   *CHANGE
```

Nyní můžete nastavit oprávnění k více objektům současně.

Nastavení oprávnění k více objektům současně

V příkladech se až dosud příkaz EDTOBJAUT používal pro nastavení specifického oprávnění k jedinému objektu. Použijte příkaz GRTOBJAUT (Udělení oprávnění k objektu) pro nastavení zabezpečení pro několik objektů. Napište GRTOBJAUT a stiskněte klávesu **F4** (Náznak). V následujícím textu jsou uvedeny některé příklady provádění vícenásobných změn oprávnění.

- Pole zadaná na následující obrazovce nastavují veřejné oprávnění ke všem frontám zpráv v knihovně CUSTLIB na typ*CHANGE.

```
                     Udělit oprávnění k objektu (GRTOBJAUT)

Zapište volby, stiskněte Enter.

Objekt . . . . . .   *all
  Knihovna . . . . . .     custlib
Typ objektu  . . . . . .   *msgq
Uživatelé  . . . . . .   *public
            + další hodnoty
Oprávnění  . . . . . .   *change
```

- Pole zadaná na následující obrazovce poskytují uživateli AMES oprávnění typu *ALL ke všem souborům v knihovně CUSTLIB, jejichž název začíná znaky WRK.

```
                    Udělit oprávnění k objektu

Zapište volby, stiskněte Enter.

Objekt . . . . . .   WRK*
  Knihovna . . . . . .    custlib
Typ objektu  . . . . . .   *file
Uživatelé. . . . . .   AMES
             + další hodnoty
Oprávnění  . . . . . .   *all
```

Tento příklad používá techniku pro specifikování parametrů označovanou jako **generické** pojmenování. Mnoho příkazů umožňuje u parametru specifikaci pomocí počátečních znaků, po kterých následuje hvězdička (*). Systém provádí operace na každém objektu, jehož jméno začíná těmito znaky. Online informace o příkazu uvádějí, které parametry povolují generická jména.

- Bude zapotřebí provést dva kroky za účelem zabezpečení všech souborů, které začínají znaky AR, a to pomocí seznamu oprávnění pod názvem ARLST1, a přiřadit souborům veřejné oprávnění ze seznamu. Tyto obrazovky ukazují požadované kroky.

```
                    Udělit oprávnění k objektu

Zapište volby, stiskněte Enter.

Objekt . . . . . .   AR*
  Knihovna . . . . . .    CUSTLIB
Typ objektu  . . . . . .   *FILE

   ⋮
Seznam oprávnění . . . . . .   ARLST1
```

```
                     Udělit oprávnění k objektu

Zapište volby, stiskněte Enter.

Objekt . . . . . .   AR*
  Knihovna . . . . . .    CUSTLIB
Typ objektu  . . . . . .   *FILE
Uživatelé. . . . . .   *PUBLIC
             + další hodnoty
Oprávnění  . . . . . .   *AUTL
             + další hodnoty
```

Použijte příkaz DSPJOBLOG způsobem popsaným v tématu ″Použití protokolu úlohy ke kontrole práce″ k ověření, zda systém provedl požadované změny oprávnění.

Než přejdete k části ″Zabezpečení tiskového výstupu″, použijte k nastavení specifických oprávnění příkaz EDTOBJAUT nebo GRTOBJAUT z části 2 formuláře Popis knihovny.

Zabezpečení tiskového výstupu

Po nastavení specifických oprávnění můžete chránit důvěrný tiskový výstup pomocí informací uvedených u těchto témat:

- Vytvoření výstupní fronty a kontrola, kdo ji může spravovat.
- Přiřazení speciálního tiskového výstupu k frontě.

Vytvoření výstupní fronty

1. Napište příkaz CRTOUTQ (Vytvoření výstupní fronty) a stiskněte klávesu **F4** (Náznak).
2. Vyplňte jméno výstupní fronty a knihovny.
3. Stiskněte klávesu **F10** (Přídavné parametry).
4. Pomocí klávesy Page down vyhledejte informace o zabezpečení pro výstupní frontu.

```
                    Vytvoření výstupní fronty (CRTOUTQ)

Zapište volby, stiskněte Enter.

Výstupní fronta . . . . . . . . . . >   NEWCP
  Knihovna . . . . . . . . . . . .      CONTRACTS
Max.vel. souboru pro soub. tisk:
  Počet stránek.. . . . . . . . .   *NONE         Číslo, *NONE
  Počáteční čas . . . . . . . . .                 Čas
  Koncový čas . . . . . . . . . .                 Čas
            + další hodnoty
Pořadí souborů ve frontě . . . .   *FIFO
Vzdálený systém. . . . . . . . .   *NONE

   ⋮
Text. . . . . . . . . . . . . . .  New Contracts Queue
```

5. Vyplňte informace uvedené ve formuláři Zabezpečení výstupních front a pracovních stanic, abyste zkontrolovali, kdo může používat a spravovat výstupní frontu.
6. Stiskněte klávesu **Enter** a zkontrolujte potvrzující zprávy.

```
                    Vytvoření výstupní fronty (CRTOUTQ)

Zapište volby, stiskněte Enter.


Přídavné parametry

Zobrazení jakéhokoliv souboru. .   *NO
Oddělovače úloh. . . . . . . . .   0
Řízeno operátorem . . . . . . .    *NO
Datová fronta. . . . . . . . . .   *NONE
  Knihovna . . . . . . . . . . .
Oprávnění ke kontrole. . . . . .   *OWNER
Oprávnění. . . . . . . . . . . .   *LIBCRTAUT
```

Možná chyba	Náprava
Stiskli jste klávesu **Enter** namísto klávesy **F10**.	Použijte příkaz CHGOUTQ (Změna výstupní fronty) pro zadání dalších informací.
Vytvořili jste výstupní frontu v nesprávné knihovně.	Použijte příkaz MOVOBJ (Přesun objektu), kterým ji přesunete do správné knihovny.

Nyní můžete přiřadit výstupní frontě tiskový výstup.

Přiřazení tiskového výstupu výstupní frontě

Po vytvoření výstupní fronty můžete výstupní frontě přiřadit tiskový výstup. Tiskový soubor obvykle řídí místo určení tiskového výstupu. Obraťte se na poskytovatele aplikace za účelem vyhledání jmen knihoven tiskových souborů určených pro důvěrné zprávy.

Pokud nemáte k těmto informacím přístup, vytiskněte sestavu a pozastavte ji ve výstupní frontě. Použijte volbu Attribute z obrazovky Work with Spooled Files a vyhledejte jméno tiskového souboru. Tiskový soubor se objeví v poli *Device file* na obrazovce Work with Spooled File Attributes.

Chcete-li změnit místo určení (výstupní frontu) tiskového souboru, použijte příkaz CHGPRTF (Změna tiskového souboru):

```
CHGPRTF FILE(jméno-knihovny/jméno-tiskového-souboru)
        OUTQ(jméno-knihovny/jméno-výstupní-fronty)
```

Při každém následujícím vyžádání sestavy je tato sestava nasměrována do nového místa určení. Chcete-li změnit místo určení v případě souboru pro souběžný tisk, který se již nachází ve výstupní frontě, použijte volbu Change z obrazovky Work with Spooled Files.

Například Sharon Jonesová ve společnosti JKL Toy Company chce přiřadit tiskový soubor ceník PRCLST1 výstupní frontě PRICEQ. Napíše:

```
CHGPRTF FILE(CONTRACTS/PRCLST1) OUTQ(CONTRACTS/PRICEQ)
```

Pokud by chtěla přiřadit výstupní frontě PRICEQ všechny sestavy s ceníky, musela by Sharon použít jméno generického tiskového souboru:

```
CHGPRTF FILE(CONTRACTS/PRCLST*) OUTQ(CONTRACTS/PRICEQ)
```

Pokud by se měly všechny nové smlouvy nasměrovat do výstupní fronty NEWCP, musela by Sharon změnit výstupní frontu přiřazenou ke vzorovému dokumentu, který se používá pro vytváření obchodních smluv.

Kontrola práce

Nejlepším způsobem, jak zkontrolovat vaši strategii ochrany důvěrného tiskového výstupu, je jeho vytištění. Zkontrolujte, zda je nasměrován do správné výstupní fronty. Přihlašte se jako systémový operátor a uvidíte, zda si můžete prohlížet soubory ve frontě nebo s nimi manipulovat.

Předtím, než provedete zabezpečení pracovních stanic, přesvědčte se, zda:

- jste vytvořili výstupní fronty uvedené ve formuláři Zabezpečení výstupních front a pracovních stanic, a to pomocí příkazu CRTOUTQ.
- jste přiřadili tiskový výstup novým výstupním frontám pomocí příkazu CHGPRTF.

Zabezpečení pracovních stanic

Po zabezpečení tiskového výstupu byste měli zabezpečit pracovní stanice. Oprávnění k pracovním stanicím se poskytuje stejným způsobem jako k jiným objektům v rámci systému. Příkazem EDTOBJAU poskytnete uživatelům oprávnění k pracovním stanicím.

K přihlášení do systému na pracovní stanici musí mít uživatelé musí mít oprávnění typu *CHANGE. Pokud je systémová hodnota QLMTSECOFR nastavena na ″ne″ (0), může se správce systému nebo kdokoliv s oprávněním typu *ALLOBJ přihlásit na kterékoliv pracovní stanici.

Pokud je systémová hodnota QLMTSECOFR nastavena na ″ano″ (1), při nastavení oprávnění k pracovním stanicím postupujte podle těchto pokynů:

Uživatelé s oprávněním k přihlášení do systému na pracovní stanici	Veřejné oprávnění	Oprávnění QSECOFR	Oprávnění individuálního uživatele
Všichni uživatelé	*CHANGE	*CHANGE	Nepožaduje se
Pouze vybraní uživatelé	*EXCLUDE	Bez oprávnění	*CHANGE
Vybraní uživatelé a uživatelé s oprávněním ke všem objektům	*EXCLUDE	*CHANGE	*CHANGE

Uživatelé s oprávněním k přihlášení do systému na pracovní stanici	Veřejné oprávnění	Oprávnění QSECOFR	Oprávnění individuálního uživatele
Všichni uživatelé s výjimkou uživatelů s oprávněním ke všem objektům	*CHANGE	Bez oprávnění	Nepožaduje se

Předtím než omezíte přístup k frontě zpráv operátora systému, zabezpečte pracovní stanice pomocí příkazu EDTOBJAUT založeném na informacích uvedených ve formuláři Zabezpečení výstupních front a pracovních stanic.

Omezení přístupu k frontě zpráv operátora systému

Úroveň zabezpečení můžete ještě zvýšit zabezpečením tiskového výstupu, zabezpečením pracovních stanic a omezením přístupu k frontě zpráv operátora systému.

Volba pro zpracování zpráv v menu ASSIST umožňuje uživatelům používat k zobrazení fronty zpráv operátora systému (QSYSOPR) funkční klávesu. Nesprávné odpovědi na zprávy systémového operátora mohou vyvolat problémy v systému. Uživatelé vyžadují oprávnění *CHANGE, aby mohli odpovídat na zprávy ve frontě zpráv a mazat je. Toto oprávnění by měli mít pouze systémoví operátoři. Podle formuláře Odpovědnost za systém zkontrolujte, kdo by měl mít oprávnění typu *CHANGE pro frontu zpráv operátora systému.

Použijte příkaz EDTOBJAUT:

1. Napište EDTOBJAUT QSYSOPR *MSGQ a stiskněte klávesu **Enter**.
2. Stiskněte **F11** k zobrazení podrobných informací o oprávnění k objektu.
3. Poskytněte veřejné oprávnění *OBJOPR, jak je uvedeno na stejné obrazovce, a stiskněte klávesu **Enter**.

```
                    Editování oprávnění k objektu

Objekt . . . . . :   QSYSOPR         Vlastník  . . . . . :   QSYS
  Knihovna  . . . . . :    QSYS          Primární skupina  . . . :   *NONE
Typ objektu  . . . . :   *MSGQ

Zapište změny aktuálních oprávnění, stiskněte Enter.

  Objekt je zabezpečený seznamem oprávnění  . . . . . .   --

                         Oprávnění     ----------Objekt-----------
Uživatel       Skupina       Oprávnění  Oper  Říz  Exist  Změna  Odkaz
*PUBLIC                 USER DEF    X
```

4. Systém změní sloupec *Oprávnění k objektu* na USER DEF (definovaný uživatelem).
5. Znovu stiskněte klávesu **F11** a zobrazí se podrobné informace týkající se oprávnění.
6. Poskytněte veřejné oprávnění *ADD, jak je uvedeno na stejné obrazovce, a stiskněte klávesu **Enter**.

```
                   Editování oprávnění k objektu

Objekt . . . . . :   QSYSOPR         Vlastník  . . . . . :   QSYS
  Knihovna  . . . . . :    QSYS          Primární skupina  . . . :   *NONE
Typ objektu  . . . . :   *MSGQ

Zapište změny aktuálních oprávnění, stiskněte Enter.

  Objekt je zabezpečený seznamem oprávnění  . . . . . .   --

                         Oprávnění k    ---------------Údaje---------------
Uživatel        Skupina      objektu   Číst  Přidat  Aktualizovat  Vymazat  Provést
*PUBLIC                 USER DEF          X
```

7. Pomocí klávesy **F6** (Přidání uživatelů) přidejte uživatele, kteří potřebují odpovídat na zprávy QSYSOPR. Udělte jim oprávnění typu *CHANGE.

Upozornění: Nevytvářejte veřejné oprávnění typu *EXCLUDE. Všechny úlohy (a uživatelé) musí být schopni přidávat zprávy do fronty zpráv QSYSOPR.

Chcete-li se ujistit o dokončení nastavení zabezpečení prostředků, měli byste:

- Přesvědčit se pomocí formulářů Seznam oprávnění a Popis knihovny, zda jste provedli zabezpečení všech knihoven aplikací.
- Zkontrolovat formulář Zabezpečení výstupních front a pracovních stanic a přesvědčit se, zda jste nastavili ochranu u pracovních stanic a vytvořili všechny speciální výstupní fronty.
- Omezit přístup k frontě zpráv systémového operátora (QSYSOPR).
- Uložit knihovny aplikací podle instrukcí uvedených v aplikacích. Systém ukládá informace o vlastnictví a veřejném oprávnění v aplikacích.
- Použijte příkaz SAVSECDTA (Uložení informací o zabezpečení), který uloží informace o zabezpečení, jež jste vytvořili. Informace najdete v tématu ″Uložení informací o zabezpečení″.

Nyní můžete začít s testováním nastaveného zabezpečení.

Testování zabezpečení

Toto téma se zabývá technikami používanými pro testování zabezpečení, které jste nastavili ve vašem systému. Testováním v tomto kontextu rozumíme ověřování, zda vše, co jste nastavili, funguje předpokládaným způsobem. Téma ″Monitorování zabezpečení″ se zabývá hodnocením účinnosti zabezpečení vašeho systému.

Zabezpečení otestujte vždy při provedení větších změn systému. Mohlo by se jednat o přidání nové aplikace, nastavení zabezpečení prostředků pro existující aplikaci, přidání nové skupiny uživatelů nebo o změnu úrovně zabezpečení.

Prostudováním následujících témat získáte informace o metodách testování a diagnostikování problémů při provádění změn v oblasti zabezpečení:

- Testování uživatelských profilů.
- Testování zabezpečení prostředků

Testování uživatelských profilů

Na začátku testování zabezpečení budete chtít otestovat uživatelský profil vždy, když do systému nastavíte novou skupinu. Proveďte test u jednoho z individuálních profilů, které jste zkopírovali ze skupinového profilu.

- Můžete se úspěšně přihlásit do systému s uživatelským profilem? Pokud to není možné, zkontrolujte protokol úlohy, který byl zapsán při neúspěšném pokusu o přihlášení do systému. Pomocí volby Práce s tiskovým výstupem z menu ASSIST vyhledejte protokol úlohy, kde naleznete více informací.

  Nejpravděpodobněji se jedná o tyto problémy:

  – Neexistuje jeden z potřebných objektů, jako například počáteční menu, aktuální knihovna nebo počáteční program.
  – Seznam knihoven specifikovaný v popisu úlohy způsobuje chyby. Buď neexistuje knihovna, nebo jste zapomněli do seznamu knihoven začlenit QGPL a QTEMP.
  – Uživatel nemá oprávnění k pracovní stanici.
- Ukázala obrazovka při vašem přihlášení do systému správné počáteční menu nebo správný počáteční program?
- Co se stalo, když jste zadali počáteční menu nebo aktuální knihovnu na obrazovce Přihlášení? Pokud je u uživatelského profilu uvedeno Omezené schopnosti (YES), měli byste dostat chybovou zprávu.
- Objevila se po stisku klávesy Attn správná obrazovka?
- Směřuje výstup do správné tiskárny? Pokud ne, použijte volbu Práce s tiskovým výstupem menu ASSIST, jejíž pomocí zjistíte, kam směřoval. Zkontrolujte uživatelský profil a popis úlohy a zjistěte, proč výstup směřoval do jiné tiskárny.
- Můžete zobrazit příkazový řádek?

- Můžete provádět požadované funkce aplikace, aniž by docházelo k chybám v zabezpečení? Další podrobnosti naleznete v tématu ″Testování zabezpečení prostředků″.
- Můžete provádět nezbytné systémové úlohy, jako je například správa tiskáren či uložení knihoven?

Pokud systém požaduje, abyste při přihlašování do systému s profilem přiřadili nové heslo, po dokončení testování nastavte heslo zpět do jména uživatelského profilu:

1. Přihlašte se do systému s vaším vlastním profilem (s oprávněním správce systému).
2. Napište CHGUSRPRF *jméno-profilu* PASSWORD(*jméno-profilu*) PWDEXP(*YES).

Nyní, když jste otestovali uživatelské profily, můžete začít testovat zabezpečení prostředků.

Testování zabezpečení prostředků

Po otestování uživatelských profilů můžete otestovat rovněž vaše zabezpečení prostředků. Při provádění testu zabezpečení prostředků vyhledáváte:

- Uživatele, kteří nemají dostatečné oprávnění pro provádění jejich úkolů.
- Uživatele, kteří mají větší oprávnění, než jste měli v úmyslu.

Testování nedostatečného oprávnění

Proveďte test jak u interaktivních, tak i u dávkových funkcí, a ověřte, zda mají uživatelské profily dostatek oprávnění.

Interaktivní testování

Chcete-li provést test zabezpečení prostředků pro aplikaci, je možné, že se budete muset přihlásit do systému s několika různými uživatelskými profily. Vaším cílem je otestovat vzorové uživatele, abyste se přesvědčili, zda je jejich přiřazené oprávnění dostatečné.

- Proveďte testování funkcí, které vyžadují rozdílné úrovně oprávnění: prohlížení, změna a vymazání.
- Testujte programy, ne pouze jednotlivá menu. Výběr volby z menu nemusí být pro testování oprávnění postačující. Někdy systém nezpřístupní soubor, dokud se skutečně nepokusíte provést určitou operaci, jako například vymazání záznamu. Ke kontrole oprávnění dochází, když necháte systém otevřít soubor. Uspořádání aplikace určuje, kdy systém otvírá soubor.
- Uchovejte záznam o chybách souvisejících se zabezpečením a vyřešte je. Pokud nastane chyba oprávnění, měla by se na obrazovce objevit zpráva s informací, že máte nedostatečné oprávnění pro tuto operaci a pro objekt, který se pokoušíte použít.

Testování dávek

- Spusťte vzorové dávkové úlohy z aplikace pomocí profilů uživatelů, kteří budou úlohy předkládat.
- Proveďte test u dávkových úloh, které vyžadují odlišné úrovně oprávnění, jako například: informace o tisku, změna informací nebo vymazání souborů na konci měsíce.
- Zkontrolujte frontu zpráv QSYSOPR a protokol QHST z hlediska chyb v zabezpečení. Pro prohlížení protokolu QHST použijte příkaz DSPLOG. Zprávy o zabezpečení jsou v tomto rozsahu: CPF2200, CPI2200, CPC2200, CPD2200, CPF4A00, CPI4A00, CPC4A00 a CPD4A00.

  Můžete také použít funkci prověrky zabezpečení pro protokolování chyb souvisejících s oprávněním a s dalšími záležitostmi z oblasti zabezpečení.

Testování příliš rozsáhlého oprávnění

Jestliže jste nastavili zabezpečení prostředků z důvodu ochrany důvěrných informací, proveďte test u vzorových uživatelských profilů, abyste se přesvědčili, že zabezpečení funguje. Přihlašte se do systému s profilem uživatele, který by neměl mít přístup k důvěrnému souboru.

- Můžete se dostat do menu, které umožňuje přístup k souboru?

- Co se stane, vyberete-li volbu z menu, které používá soubor?
- Můžete zobrazit příkazový řádek?
- Můžete spustit příkaz k vyhledání souboru na seznamu, jako je například CPYF FROMFILE(*jméno-souboru*) TOFILE(QSYSPRT)?
- Můžete použít dotazovací nástroj k prohlížení souboru?

Výsledky vašeho testování mohou naznačovat, že potřebujete změnit informace o zabezpečení.

Změna informací o zabezpečení

Nyní, když jste naplánovali zabezpečení systému, musíte zajistit, aby byl váš záměr stále funkční, a to i při provádění nezbytných změn v činnosti.

Toto téma zdůrazňuje jednoduchost jako základní cíl při navrhování zabezpečení. Navrhli jste uživatelské skupiny jako vzory pro individuální uživatele. Spíše než specifická individuální oprávnění jste se pokusili využívat veřejného oprávnění, seznamů oprávnění a oprávnění ke knihovnám. Při správě zabezpečení využijte výhod, které poskytuje následující metoda:

- Přidáváte-li novou skupinu uživatelů nebo novou aplikaci, použijte techniky, které jste používali při plánování zabezpečení.
- Pokud potřebujete provést změny v zabezpečení, raději se při řešení konkrétního problému pokuste dát přednost obecné metodě před zaváděním výjimek.

Téma Příkazy pro zabezpečení se zabývá příkazy používanými při zobrazení, změně a vymazání informací o zabezpečení.

Informace o možnostech různých změn jsou uvedeny v rámci těchto témat:

- Přidání nového uživatele do systému.
- Vytvoření nové skupiny uživatelů.
- Změna skupiny uživatelů.
- Přidání nové aplikace.
- Přidání nové pracovní stanice.
- Změna odpovědnosti uživatele.
- Odstranění uživatele ze systému.

Příkazy pro zabezpečení

Následující tabulka uvádí, které příkazy se používají pro práci s objekty zabezpečení v rámci systému. Tyto příkazy můžete použít pro plnění těchto úkolů:

- Prohlížení a procházení seznamu informací o zabezpečení.
- Změna informací o zabezpečení.
- Vymazání informací o zabezpečení.

Tabulka 63. Příkazy pro zabezpečení

Objekt zabezpečení	Jak prohlížet	Jak měnit	Jak vymazat
Systémová hodnota	WRKSYSVAL DSPSYSVAL	WRKSYSVAL CHGSYSVAL	Nelze vymazat
Popis úlohy	WRKJOBD DSPJOBD	WRKJOBD CHGJOBD	DLTJOBD
Skupinový profil	WRKUSRPRF DSPUSRPRF DSPAUTUSR	WRKUSRPRF CHGUSRPRF	DLTUSRPRF[1],[2]

Tabulka 63. Příkazy pro zabezpečení (pokračování)

Objekt zabezpečení	Jak prohlížet	Jak měnit	Jak vymazat
Uživatelský profil	WRKUSRPRF DSPUSRPRF DSPAUTUSR	WRKUSRPRF CHGUSRPRF CHGUSRAUD	DLTUSRPRF[1]
Oprávnění k objektu	DSPAUT DSPOBJAUT DSPUSRPRF TYPE(*OBJAUT)	CHGAUT EDTOBJAUT GRTOBJAUT WRKAUT	EDTOBJAUT RVKOBJAUT WRKAUT
Vlastnictví objektu	WRKOBJOWN DSPOBJAUT DSPUSRPRF TYPE(*OBJOWN)	CHGOBJOWN CHGOWN	CHGOBJOWN CHGOWN umožňuje odvolat práva předešlého vlastníka.
Primární skupina	DSPOBJAUT WRKOBJPGP DSPUSRPRF TYPE(*OBJPGP)	CHGOBJPGP CHGPGP	CHGOBJPGP CHGPGP (nastavit primární skupinu na *NONE)
Prověření objektu	DSPOBJD	CHGOBJAUD CHGAUD	CHGOBJAUD (nastaveno na *NONE) CHGAUD
Seznam oprávnění	DSPAUTL DSPAUTLOBJ	EDTAUTL (oprávnění uživatele k seznamu) EDTOBJAUT (objekt zabezpečen seznamem) ADDAUTLE CHGAUTLE GRTOBJAUT	DLTAUTL (celý seznam)[3] RMVAUTLE (odstranění oprávnění uživatele k seznamu) EDTOBJAUT (objekt zabezpečen seznamem) RVKOBJAUT

1. IBM doporučuje pro vymazání profilu použít volbu pro odstranění z obrazovky Work with User Enrollment. Pomocí této volby můžete vymazat všechny objekty, které profil vlastní, nebo je opětovně přidělit novému vlastníkovi. Určité parametry příkazu DLTUSRPRF umožňují vymazat všechny objekty, které vlastní uživatel, nebo umožňují je přiřadit novému vlastníkovi. Profil nemůžete vymazat, pokud nevymažete nebo znovu nepřiřadíte vlastněné objekty. Zároveň nemůžete vymazat profil, který je primární skupinou pro jakékoliv objekty.
2. Nemůžete vymazat skupinový profil, který obsahuje nějaké členy. Pro vytvoření seznamu členů skupiny použijte volbu *GRPMBR z příkazu DSPUSRPRF. Předtím, než vymažete skupinový profil, změňte pole *Skupinový profil* v každém z jednotlivých skupinových profilů.
3. Nemůžete vymazat seznam oprávnění, který se používá pro zabezpečení objektů. Pomocí příkazu DSPAUTLOBJ procházejte seznam objektů, které jsou zabezpečené pomocí seznamu. Pomocí příkazu EDTOBJAUT změňte oprávnění ke všem objektům, které jsou zabezpečeny pomocí seznamu.

Prohlížení a výpis informací o zabezpečení

Seznam informací o zabezpečení můžete procházet pomocí příkazu zobrazit (DSP) u volby tisk (*PRINT). Například pro zobrazení seznamu oprávnění pod názvem MYLIST napište DSPAUTL MYLIST *PRINT.

Některé příkazy obrazovek nabízejí volby pro různé typy seznamů. Pokud jste například vytvořili profily individuálních uživatelů, použili jste volbu *GRPMBR z příkazu DSPUSRPRF pro prohlížení seznamu všech členů uživatelského profilu. Použijte zobrazování náznaků (**F4**) a online informací k vyhledání seznamů, které jsou dostupné pro objekty zabezpečení.

Můžete použít příkazy typu ″zobrazení″ (DSP) k prohlížení informací o zabezpečení na obrazovkové stanici. Můžete také použít příkazy typu ″práce s″ (WRK), které poskytují více funkcí. Příkazy typu ″práce s″ (WRK) poskytují obrazovku seznamů. Tuto obrazovku můžete použít ke změně, vymazání a prohlížení informací.

Příkazy pro ″zabezpečení″ můžete použít rovněž k procházení seznamu nebo pro prohlížení informací pomocí generického jména. Napíšete-li WRKUSRPRF DPT*, pak obrazovka Work with User Enrollment nebo obrazovka Práce s uživatelskými profily zobrazí pouze ty profily, které začínají znaky *DPT*. Chcete-li zjistit, které parametry povolují generická jména, používejte pro příkaz pouze online informace.

Změna informací o zabezpečení

Můžete interaktivně měnit informace o zabezpečení pomocí příkazu typu ″práce s″ (WRK) nebo ″editace″ (EDT). Po provedení změny můžete informace prohlížet, měnit je a znovu prohlížet.

Zároveň můžete měnit informace o zabezpečení, aniž byste je před provedením změny či po něm prohlíželi, a to pomocí příkazu typu ″změna″ (CHG) nebo ″udělení″ (GRT). Tato metoda je obzvlášť užitečná pro provádění změny u více objektů současně. Příkladem může být použití příkazu GRTOBJAUT pro nastavení veřejného oprávnění ke všem objektům v knihovně. Viz téma “Nastavení veřejného oprávnění ke všem objektům v knihovně” na stránce 93.

Vymazání informací o zabezpečení

Některé typy informací o zabezpečení můžete interaktivně vymazat nebo odstranit pomocí příkazů typu ″práce s″ (WRK) nebo ″editace″ (EDT). Vymazat informace o zabezpečení můžete také pomocí příkazů typu ″výmaz″ (DLT), ″odstranění″ (RMV) a ″odvolání″ (RVK). Často musíte splnit určité podmínky a teprve potom systém povolí vymazat informace o zabezpečení. Poznámky, které jsou uvedeny v tématu Příkazy pro zabezpečení, uvádějí některé z těchto podmínek.

Přidání nového uživatele do systému

Potřebujete-li do systému přidat nového uživatele, postupujte tímto způsobem:

1. Zařaďte osobu do skupiny uživatelů. Použijte formulář Popis skupiny uživatelů, kde naleznete referenční informace.
2. Rozhodněte, zda nový uživatel potřebuje provádět systémové funkce. Pokud ano, přidejte tuto informaci do formuláře Odpovědnost za systém.
3. Přidejte osobu do formuláře Profil individuálního uživatele.
4. Přezkoumejte formulář Odpovědnost za systém a formulář Popis skupiny uživatelů, abyste zjistili, zda nový uživatel potřebuje hodnoty, které se liší od hodnot skupiny.
5. Vytvořte uživatelský profil zkopírováním skupinového profilu nebo profilu člena skupiny. Přesvědčte se, zda jste nastavili dočasnou platnost hesla. (Informace najdete v tématu ″Kopírování skupinového profilu″.)
6. Předejte novému uživateli kopii vašeho sdělení týkajícího se zabezpečení.

Návod, jak vytvořit novou skupinu uživatelů, najdete v tématu ″Vytvoření nové skupiny uživatelů″.

Vytvoření nové skupiny uživatelů

Vytvořit novou skupinu uživatelů by mohlo být zapotřebí z několika důvodů:

- Systém potřebují používat další oddělení.
- Zjistíte, že potřebujete vytvořit konkrétnější skupiny uživatelů, které by splňovaly vaše potřeby související se zabezpečením prostředků.
- Vaše společnost reorganizovala některá oddělení.

Chcete-li vytvořit novou skupinu uživatelů, postupujte takto:

1. Vyplňte formulář Popis skupiny uživatelů podle pokynů uvedených v tématu ″Plánování skupin uživatelů″.
2. Přidejte skupinu uživatelů do diagramu aplikací, knihoven a skupin uživatelů.
3. Zvažte, zda někteří členové skupiny potřebují provádět systémové funkce. Aktualizujte formulář Odpovědnost za systém. (Informace najdete v tématu ″ Určení, kdo má být odpovědný za systémové funkce″.)
4. K vyplnění formuláře Profil individuálního uživatele použijte informace uvedené ve formuláři Popis skupiny uživatelů a ve formuláři Odpovědnost za systém.
5. Vytvořte skupinovou knihovnu.
6. Vytvořte popis úlohy pro skupinu.
7. Vytvořte skupinový profil.

   Poznámka: Informace týkající se kroků pět, šest a sedm najdete v tématu ″ Nastavení skupin uživatelů″.

8. Vytvořte profily individuálních uživatelů pro členy skupiny. (Informace najdete v tématu ″Nastavení individuálních uživatelů″.)
9. Vyhodnoťte formuláře Popis knihovny pro všechny aplikace, které skupina potřebuje. Proveďte veškeré kroky nezbytné pro to, aby se skupině poskytl přístup k objektům aplikace pomocí technik popsaných v tématu ″ Nastavení zabezpečení prostředků″.
10. Všem členům skupiny předejte kopii vašeho sdělení týkající se zabezpečení.

Provádění změny skupiny uživatelů je uvedeno v tématu ″Změna skupiny uživatelů″.

Změna skupiny uživatelů

Bude zapotřebí provádět různé změny v charakteristikách skupin, a to různými způsoby. V následujícím textu jsou uvedeny některé příklady změn a způsob jejich provádění:

Změna oprávnění skupiny

Může se stát, že zjistíte, že skupina potřebuje oprávnění k objektům, se kterými jste v počátečním plánu nepočítali. Postupujte takto:

1. Pomocí příkazu EDTOBJAUT (Editování oprávnění k objektu) poskytnete skupině požadovaný přístup k objektům nebo k odpovídajícímu seznamu oprávnění. Téma “Nastavení specifických oprávnění” na stránce 97 uvádí příklady, jakým způsobem to provést. Poskytnete-li skupině oprávnění, dostává oprávnění k objektu každý člen skupiny.
2. Pokud skupině poskytnete oprávnění k důvěrnému objektu, můžete požadovat prověření stávajících členů skupiny. K procházení seznamu členů skupiny použijte příkaz DSPUSRPRF *jméno-skupinového-profilu* *GRPMBR.

Změna přizpůsobení pro skupinu

Můžete požadovat změnu nastavení uživatelského prostředí pro členy skupiny. Pokud například oddělení získá svou vlastní tiskárnu, chcete, aby byla nová tiskárna předvolená pro členy skupiny uživatelů z tohoto oddělení. Nebo v případě, že se do systému nainstaluje nová aplikace, mohou členové skupiny uživatelů požadovat při přihlášení do systému jiné počáteční menu.

Skupinový profil poskytuje vzor, který můžete zkopírovat za účelem vytvoření profilů individuálních uživatelů pro členy skupiny. Avšak přizpůsobení hodnot ve skupinovém profilu neovlivní profily individuálních uživatelů po jejich vytvoření. Například změna pole *Tiskové zařízení* ve skupinovém profilu neovlivní členy skupiny. Je nezbytné změnit pole *Tiskové zařízení* v každém profilu individuálního uživatele.

Pomocí obrazovky Práce s uživatelskými profily můžete změnit parametr pro více uživatelů najednou. Příklad ukazuje změnu výstupní fronty pro všechny členy skupiny:

1. Napište WRKUSRPRF *ALL a stiskněte klávesu **Enter**.
2. Pokud jste na obrazovce Work with User Enrollment, změňte ji pomocí klávesy **F21** (Výběr úrovně asistence) na obrazovku Práce s uživatelskými profily.

```
                        Práce s uživatelskými profily

Zapište volby, stiskněte Enter.
  1=Vytvoření   2=Změna   3=Kopie  4=Výmaz   5=Zobrazení
  12=Práce s objekty dle vlastníka

          Uživatelský
Vol       profil                 Text

                HARRISOK         Harrison, Keith
2               HOGANR           Hogan, Richard
                JONESS           Jonesová, Sharon
2               WILLISR          Willisová, Rose

   ⋮
                                                                  Další...
Parametry pro volby 1, 2, 3, 4 a 5 nebo příkaz
===> PRTDEV(PRT02)
F3=Konec   F5=Obnova   F12=Zrušení   F16=Opakovat umístění na   F17=Umístění na
F21=úrovně asistence      F24=Další klávesy
```

3. Vedle každého profilu, který chcete změnit, napište **2** (Změna).
4. Na řádek parametry v dolní části obrazovky napište jméno parametru a novou hodnotu. Neznáte-li jméno parametru, stiskněte klávesu **F4** (Náznak).
5. Stiskněte klávesu **Enter**. Dostanete potvrzující zprávu pro každý změněný profil.

   Ačkoliv změna přizpůsobení pole ve skupinovém profilu nemá žádný vliv na členy skupiny, může vám to pomoci v budoucnosti. Skupinový profil poskytuje vzor pro případ, že chcete později přidat členy do skupiny. Zároveň představuje záznam standardních hodnot pole pro skupinu.

Poskytnutí přístupu skupiny k nové aplikaci

Pokud skupina uživatelů potřebuje přístup k nové aplikaci, musíte analyzovat informace o skupině a o aplikaci. Doporučujeme tuto metodu:

1. Ve formuláři Popis aplikace vyhledejte novou aplikaci a diagram aplikací, knihoven a skupin uživatelů, aby bylo patrné, které knihovny aplikace používá. Tyto knihovny doplňte do formuláře Popis skupiny uživatelů.
2. Aktualizujte váš diagram aplikací, knihoven a skupin uživatelů za účelem zobrazení nového vztahu mezi skupinou uživatelů a aplikací.
3. Jestliže by měl počáteční seznam knihoven obsahovat knihovny, změňte popis úlohy skupiny příkazem CHGJOBD (Změna popisu úlohy). Pokud potřebujete pomoc při práci s popisy úloh, vyhledejte informace v tématu “Vytvoření popisu úlohy” na stránce 80.

   Poznámka: Jestliže přidáváte knihovny do počátečního seznamu knihoven v popisu úlohy, není zapotřebí měnit uživatelské popisy, které používají popis úlohy. Když se uživatel přihlásí příště, jeho počáteční seznam knihoven přidá tyto knihovny automaticky.
4. Zhodnoťte, zda potřebujete měnit buď počáteční program, nebo počáteční menu kvůli přístupu skupiny k nové aplikaci. Je zapotřebí provést individuální změnu v počátečním menu nebo v programu každého uživatelského profilu pomocí příkazu CHGUSRPRF.
5. Z formulářů Popis knihovny zjistěte všechny knihovny, které aplikace používá. Určete, zde veřejný přístup, který je k dispozici pro knihovny, dostatečným způsobem vyhovuje potřebám skupiny. Pokud ne, bude možná zapotřebí poskytnout skupině oprávnění ke knihovně, ke konkrétním objektům nebo k seznamům oprávnění. Za tímto účelem použijte příkazy EDTOBJAUT (Editování oprávnění k objektu) a EDTAUTL (Editování seznamu oprávnění). (Případné další informace najdete v tématu ″Nastavení zabezpečení prostředků″.)

Informace týkající se přidání aplikací do systému najdete v tématu ″Přidání nové aplikace″.

Přidání nové aplikace

Zabezpečení pro všechny nové aplikace byste měli plánovat stejně pečlivě jako pro vaše původní aplikace. Postupujte stejným způsobem:

1. Připravte pro aplikaci formuláře Popis aplikace a Popis knihovny.
2. Aktualizujte diagram aplikací, knihoven a skupin uživatelů.
3. Dodržujte postupy uvedené v tématu ″Plánování zabezpečení prostředků″, abyste mohli stanovit způsob, jak zabezpečit novou aplikaci.
4. Připravte si formulář Instalace aplikace pomocí metody popsané v tématu ″Plánování instalace aplikací″.
5. Posuďte, zda nějaký tiskový výstup z aplikace lze považovat za důvěrný a vyžadující ochranu. V případě potřeby aktualizujte formulář Zabezpečení výstupních front a pracovních stanic.
6. Při instalaci a zabezpečení aplikace dodržujte postup uvedený v tématu ″Nastavení vlastnictví a veřejného oprávnění″ a v tématu ″Nastavení zabezpečení prostředků″ při instalaci a zabezpečení aplikace.

Chcete-li do systému přidat pracovní stanici, najdete informace v tématu ″Přidání nové pracovní stanice″.

Přidání nové pracovní stanice

Pokud přidáte do systému novou pracovní stanici, vezměte v úvahu požadavky na zabezpečení.

1. Představuje fyzické umístění nové pracovní stanice nějaká bezpečnostní rizika? (Informace související s aktualizací paměti najdete v tématu ″Plánování fyzického zabezpečení″.)
2. Pokud pracovní stanice představuje riziko, aktualizujte formulář Zabezpečení výstupních front a pracovních stanic.
3. Obvykle byste měli vytvořit nové pracovní stanice pomocí veřejného oprávnění typu *CHANGE. Pokud tento způsob nevyhovuje vašim požadavkům na zabezpečení pracovní stanice, k zadání odlišného oprávnění použijte příkaz EDTOBJAUT.

Informace týkající se odpovědnosti uživatele v rámci systému najdete v tématu ″Změna odpovědností uživatele″.

Změna odpovědností uživatele

Jakmile uživatel systému získá novou úlohu nebo nový okruh odpovědností v rámci společnosti, je zapotřebí vyhodnotit, jak tyto skutečnosti ovlivní uživatelský profil.

1. Měl by uživatel patřit do jiné skupiny uživatelů? Ke změně skupiny uživatelů použijte příkaz CHGUSRPRF.
2. Potřebujete změnit některé přizpůsobené hodnoty v profilu, jako je například tiskárna nebo počáteční menu? K jejich změně můžete také použít příkaz CHGUSRPRF.
3. Jsou oprávnění k aplikaci těchto nových skupin uživatelů pro danou osobu postačující?
   - Pomocí příkazu DSPUSRPRF (Zobrazení uživatelského profilu) si prohlédněte oprávnění pro staré a nové skupinové profily.
   - Dále se podívejte na oprávnění profilu individuálního uživatele.
   - Pomocí příkazu EDTOBJAUT proveďte všechny nezbytné změny.
4. Vlastní uživatel nějaké objekty? Měli byste změnit vlastnictví těchto objektů? Použijte příkaz WRKOBJOWN (Práce s objekty dle vlastníka).
5. Vykonává uživatel systémové funkce? Je zapotřebí, aby uživatel v rámci nového úkolu vykonával systémové funkce? Aktualizujte formulář Odpovědnost za systém a v případě potřeby změňte uživatelský profil.

Informace o způsobu, jak odstranit uživatele ze systému, najdete v tématu ″Odstranění uživatele ze systému″.

Odstranění uživatele ze systému

Pokud někdo ze společnosti odejde, je nezbytné ihned odstranit uživatelský profil ze systému. Předtím, než budete moci vymazat uživatelský profil, musíte buď vymazat, nebo přenést vlastnictví všech objektů vlastněných profilem. K tomu můžete použít příkaz WRKOBJOWN nebo můžete použít volbu **4** (Odstranění) z obrazovky Work with User Enrollment.

Vyberete-li pro profil volbu **4** (Odstranění) z obrazovky Work with User Enrollment, zobrazí se další obrazovky, které vám umožní pracovat se všemi objekty, které uživatel vlastní. Všechny objekty můžete buď poskytnout novému vlastníkovi, nebo můžete s objekty pracovat individuálně:

```
                              Odstranění uživatele

Uživatel . . . . . . . . . . . :   HOGANR
Popis uživatele. . . . . . . . :   oddělení prodeje a marketingu

Pro odstranění tohoto uživatele zapište volbu, stiskněte Enter.

    1. Předat všechny objekty, které uživatel vlastní, novému vlastníkovi.
    2. Vymazat nebo změnit vlastníka objektů, které tento uživatel vlastní.
```

Pokud jste se rozhodli pracovat s objekty individuálně (volba **2**), na obrazovce se ukáže seznam všech objektů, které uživatel vlastní:

```
                              Odstranění uživatele

Uživatel . . . . . . . . . . . :    HOGANR
Popis uživatele . . . . . . . . :   Oddělení prodeje a marketingu

Nový vlastník  . . . . . . . . .                   Jméno, F4 - seznam

Pro odstranění tohoto uživatele vymažte nebo změňte vlastníka všech objektů.
Zapište volbu a stiskněte Enter.
  2=Změna na nového vlastníka   4=Vymazat   5=Podrobnosti obrazovky

Vol  Objekt        Knihovna      Popis
 4   HOGANR        QUSRSYS       Hogan, Richard message queue
 4   QUERY1        DPTWH         Inventory Query
```

Pokud jste zvolili vymazání objektů, objeví se obrazovka pro potvrzení výmazu. Jakmile systém vymaže objekty, můžete odstranit uživatelský profil. Potom se znovu ukáže obrazovka Work with User Enrollment se zprávou oznamující, že systém odstranil uživatele.

Uložení informací o zabezpečení

Toto téma uvádí přehled o tom, jakým způsobem se ukládají a obnovují informace o zabezpečení. Jestliže plánujete zálohování a obnovu systému, musíte vzít v úvahu jak samotné informace, tak i jejich zabezpečení. Informace, které vám pomohou sestavit a realizovat plán zálohování a obnovy, najdete v aplikaci Information Center, pod tématem Zálohování, obnova a dostupnost.

Následující témata popisují způsob zálohování a obnovování informací o zabezpečení, které jste vytvořili při nastavení zabezpečení.

- Uložení systémových hodnot.
- Uložení skupinových a uživatelských profilů.
- Uložení popisů úloh.
- Uložení informací o zabezpečení prostředků.
- Uložení předvoleného profilu vlastníka (QDFTOWN).
- Obnova z poškozeného seznamu oprávnění.

Uložení systémových hodnot

Systémové hodnoty jsou uloženy v systémové knihovně QSYS. Systémovou knihovnu QSYS uložíte, budete-li postupovat následujícím způsobem:

- Použijte příkaz SAVSYS (Uložení systému).

- Z menu Uložení vyberte volbu pro uložení celého systému.
- Z menu Uložení vyberte volbu pro uložení systémových informací.
- Z menu RUNBCKUP (Run Backup) použijte volbu pro zálohování celého systému.

Potřebujete-li obnovit celý systém, systémové hodnoty automaticky obnovíte při obnově operačního systému.

Informace najdete v tématu ″Uložení skupinových a uživatelských profilů″.

Uložení skupinových a uživatelských profilů

Skupinové a uživatelské profily jsou uloženy v knihovně QSYS. Uložíte je pomocí příkazu SAVSYS (Uložení systému) nebo vybráním volby pro uložení celého systému.

Skupinové a uživatelské profily můžete také uložit příkazem SAVSECDTA (Uložení informací o zabezpečení).

Obnovte uživatelské profily pomocí příkazu RSTUSRPRF (Obnova uživatelských profilů). Obvyklá posloupnost je následující:

1. Proveďte obnovu operačního systému, v jejímž rámci proběhne obnova knihovny QSYS.
2. Obnovte uživatelské profily.
3. Obnovte zbývající knihovny.
4. Obnovte oprávnění k objektům pomocí příkazu RSTAUT (Obnova oprávnění).

Informace jsou uvedeny v následující části ″Uložení popisů úloh″.

Uložení popisů úloh

Vytvoříte-li popis úlohy, určíte i knihovnu, kde by měl být uložen v paměti. IBM doporučuje vytvořit popisy úlohy do knihovny QGPL.

Popisy úloh můžete uložit uložením knihovny, kde jsou uloženy v paměti. K provedení použijte příkaz SAVLIB (Uložení knihovny). Popis úlohy můžete také uložit pomocí příkazu SAVOBJ (Uložení objektu).

Obsah knihovny můžete obnovit pomocí příkazu RSTLIB (Obnova knihovny). Jednotlivý popis úlohy můžete obnovit příkazem RSTOBJ (Obnova objektu).

Informace naleznete v navazující části ″Uložení informací o zabezpečení prostředků″.

Uložení informací o zabezpečení prostředků

Zabezpečení prostředků definující způsob, jakým mohou uživatelé pracovat s objekty, se skládá z různých typů informací, které jsou uloženy na několika odlišných místech:

Tabulka 64. Uložení a obnova informací o zabezpečení prostředků

Typ informací	Kde jsou uloženy	Jak jsou uloženy	Jak se obnovují
Veřejné oprávnění	u objektu	příkaz SAVxxx [1]	příkaz RSTxxx [2]
Hodnota prověřování objektu	u objektu	příkaz SAVxxx [1]	příkaz RSTxxx [2]
Vlastnictví objektu	u objektu	příkaz SAVxxx [1]	příkaz RSTxxx [2]
Primární skupina	u objektu	příkaz SAVxxx [1]	příkaz RSTxxx [2]
Seznam oprávnění	knihovna QSYS	SAVSYS nebo SAVSECDTA	RSTUSRPRF USRPRF(*ALL)
Spojení mezi objektem a seznamem oprávnění	u objektu	příkaz SAVxxx [1]	příkaz RSTxxx [2]
Soukromé oprávnění	u uživatelského profilu	SAVSYS nebo SAVSECDTA	RSTAUT

Tabulka 64. Uložení a obnova informací o zabezpečení prostředků (pokračování)

Typ informací	Kde jsou uloženy	Jak jsou uloženy	Jak se obnovují

1. Většinu typů objektů můžete uložit pomocí příkazů SAVOBJ nebo SAVLIB. Některé typy objektů, jako například konfigurace, se ukládají zvláštním příkazem.
2. Většinu typů objektů můžete obnovit pomocí příkazů RSTOBJ nebo RSTLIB. Některé typy objektů, jako například konfigurace, mají pro obnovení zvláštní příkaz.

Potřebujete-li obnovit aplikaci nebo celý systém, musíte velice pečlivě naplánovat jednotlivé kroky, včetně obnovení oprávnění k objektům. Následují základní kroky, které jsou nutné pro obnovení informací o zabezpečení prostředků pro aplikaci:

1. V případě potřeby obnovte uživatelské profily, včetně profilů, které vlastní aplikaci. Pomocí příkazu RSTUSRPRF můžete obnovit konkrétní profily nebo všechny profily.
2. Obnovte všechny seznamy oprávnění, které aplikace používá. Seznamy oprávnění obnovíte pomocí příkazu RSTUSRPRF USRPRF(*ALL).

   Poznámka: Tím se ze zálohovacích médií obnoví všechny hodnoty uživatelského profilu, včetně hesel.
3. Knihovny aplikací obnovte pomocí příkazů RSTLIB nebo RSTOBJ. Tím se obnoví vlastnictví objektů, veřejné oprávnění a spojení mezi objekty a seznamy oprávnění.
4. Soukromá oprávnění k objektům obnovte pomocí příkazu RSTAUT. Příkazem RSTAUT se zároveň obnoví oprávnění uživatele uvedená na seznamech oprávnění. Můžete obnovit buď konkrétní uživatele, nebo všechny uživatele.

Informace o obnově objektu a profilu vlastníka, který není ve vašem systému, najdete v tématu ″Používání předvoleného profilu vlastníka (QDFTOWN)″.

Používání předvoleného profilu vlastníka (QDFTOWN)

Pokud obnovujete objekt a profil vlastníka není v systému, systém přenese vlastnictví objektu na předvolený profil, který se nazývá QDFTOWN. Jakmile jednou obnovíte profil vlastníka nebo jej vytvoříte znovu, můžete vlastnictví přenést zpět, a to pomocí příkazu WRKOBJOWN (Práce s objekty dle vlastníka).

Informace o obnově seznamu oprávnění jsou uvedeny v tématu ″Obnova z poškozeného seznamu oprávnění″.

Obnova z poškozeného seznamu oprávnění

Pokud seznam oprávnění zabezpečuje určitý objekt a dojde k poškození tohoto seznamu, mají k tomuto objektu přístup pouze uživatelé se speciálním oprávněním pro všechny objekty (*ALLOBJ).

Provedení obnovy z poškozeného seznamu oprávnění vyžaduje provedení dvou kroků:

1. Obnovte uživatele a jejich oprávnění na seznamu oprávnění.
2. Obnovte přiřazení seznamu oprávnění k objektům.

Tyto kroky může provést uživatel se zvláštním oprávněním *ALLOBJ.

Krok 1: Obnovení seznamu oprávnění

Znáte-li oprávnění uživatele podle seznamu oprávnění, vymažte seznam oprávnění, vytvořte jej znovu a doplňte do něj uživatele.

Pokud neznáte všechna oprávnění uživatele podle seznamu oprávnění, obnovte je z vašich posledních pásek SAVSYS nebo SAVSECDTA pomocí těchto kroků:

1. Vymažte poškozený seznam oprávnění:
   ```
   DLTAUTL AUTL(jméno-seznamu-oprávnění)
   ```

2. Obnovte seznam oprávnění:
   ```
   RSTUSRPRF USRPRF(*ALL)
   ```
3. Doplňte uživatele do seznamu pomocí příkazu RSTAUT (Obnova oprávnění).

Krok 2: Obnova přiřazení objektů k seznamu oprávnění

Poté, co jste obnovili seznam oprávnění nebo jste jej vytvořili znovu, musíte vytvořit spojení mezi seznamem a objekty, které jsou pomocí seznamu zabezpečeny:

1. Použijte příkaz RCLSTG (Náprava paměti). Příkazem RCLSTG se přiřazují objekty, které mají být zabezpečeny pomocí poškozených nebo chybějících seznamů oprávnění, k předvolenému seznamu, jenž je uváděn pod názvem QRCLAUTL.
2. Zobrazte seznam objektů, které zabezpečuje seznam oprávnění QRCLAUTL:
   ```
   DSPAUTLOBJ AUTL(QRCLAUTL)
   ```
3. Použijte příkaz GRTOBJAUT pro zabezpečení objektů pomocí správného seznamu oprávnění. Například pro zabezpečení souboru ARWRK01 v knihovně CUSTLIB pomocí seznamu oprávnění ARLST01 napište:
   ```
   GRTOBJAUT OBJ(CUSTLIB/ARWRK01) OBJTYPE(*FILE) +
             AUTL(ARLST01)
   ```

Monitorování zabezpečení

Toto téma se zabývá základními podněty pro monitorování účinnosti bezpečnostních opatření ve vašem systému.

Pravidelné monitorování zabezpečení má dva základní cíle:

- Ověření adekvátní kontroly objektů společnosti.
- Odhalování nepovolených pokusů o získání přístupu do systému a k informacím společnosti.

Zrevidujte vaši strategii zabezpečení a sdělení o zabezpečení určené pro uživatele v okamžiku, kdy se rozhodnete, které úlohy související s monitorováním budete provádět pravidelně.

Další informace o monitorování zabezpečení najdete v následujících tématech:

- Kontrolní seznamy pro monitorování zabezpečení.
- Prověřování zabezpečení.

Kontrolní seznamy pro monitorování zabezpečení

Následují kontrolní seznamy určené pro přezkoumání různých aspektů zabezpečení vašeho systému. Použijte je pro vypracování vlastního plánu.

Monitorování fyzického zabezpečení

- Ochrana zálohovacích médií před poškozením a krádeží.
- Omezení přístupu k pracovním stanicím ve veřejných prostorách. Chcete-li zjistit, kdo vlastní oprávnění *CHANGE pro pracovní stanice, použijte příkaz DSPOBJAUT.

Monitorování systémových hodnot

- Ověřte, zda nastavení odpovídá formuláři Výběr systémových hodnot. Použijte příkaz PRTSYSSECA (Tisk atributů zabezpečení systému).
- Přezkoumejte své rozhodnutí týkající se systémových hodnot, zejména při instalaci nových aplikací.

Monitorování skupinových profilů

- Ověřte, zda skupinové profily nemají žádná hesla. Pomocí příkazu DSPAUTUSR ověřte, zda všechny skupinové profily mají heslo *NONE.
- Zkontrolujte, zda mezi členy skupiny byly zařazeny správné osoby. Pomocí příkazu DSPUSRPRF s volbou *GRPMBR vytvořte seznam všech členů skupiny.

- Zkontrolujte zvláštní oprávnění pro každý skupinový profil. Použijte příkaz DSPUSRPRF. Pokud máte nastavenu úroveň zabezpečení 30, 40, nebo 50, neměly by skupinové profily mít oprávnění typu *ALLOBJ.

Monitorování uživatelských profilů

- Ověřte, zda uživatelské profily v systému patří do jedné z těchto kategorií:
  - Uživatelské profily pro běžné zaměstnance.
  - Skupinové profily.
  - Profily vlastníků aplikace.
  - Profily dodávané IBM (tyto profily začínají písmenem Q).
- Odstraňte uživatelský profil případě, že společnost převádí uživatele, nebo pokud uživatel opouští společnost. Pomocí příkazu CHGEXPSCDE (Změna záznamu o plánovaném ukončení platnosti) automaticky vymažte nebo zablokujte profil, jakmile uživatel odejde ze společnosti.
- Vyhledejte neaktivní profily a odstraňte je. Můžete použít příkaz ANZPRFACT (Analýza aktivity profilu), kterým se automaticky zablokují profily, pokud jsou po určitou dobu neaktivní.
- Určete, kteří uživatelé mají heslo totožné se jménem jejich uživatelského profilu. Použijte příkaz ANZDFTPWD (Analýza předvolených hesel). Pomocí volby tohoto příkazu přinuťte uživatele, aby si při příštím přihlášení do systému změnili hesla.

  Upozornění: Ze systému neodstraňujte žádné profily dodané IBM. Profily, které dodala IBM, začínají znakem Q.
- Uvědomte si, které osoby mají jinou třídu uživatele, než je *USER, a z jakého důvodu. Pomocí příkazu PRTUSRPRF (Tisk uživatelských profilů) získáte seznam všech uživatelů, jejich třídu uživatele a jejich zvláštní oprávnění. Porovnejte tyto informace s formulářem Odpovědnost za systém.
- Zkontrolujte, které uživatelské profily mají pole *Omezení schopností* nastavené na *NO.

Monitorování kritických objektů

- Přezkoumejte, kdo má přístup ke kritickým objektům. Pro monitorování objektů použijte příkaz PRTPVTAUT (Tisk soukromých oprávnění) a příkaz PRTPUBAUT (Tisk objektů s veřejným oprávněním). Pokud má přístup celá skupina, zkontrolujte členy skupiny pomocí volby *GRPMBR z příkazu DSPUSRPRF.
- Prověřte, kdo může používat aplikační programy poskytující přístup k objektům prostřednictvím jiné zásady zabezpečení, jako je například adoptované oprávnění. Použijte příkaz PRTADPOBJ (Tisk adoptovaných objektů).

Monitorování neoprávněného přístupu

- Vydejte systémovým operátorům pokyn, aby věnovali pozornost varovným zprávám týkajícím se zabezpečení ve frontě zpráv QSYSOPR. Zejména je zapotřebí, aby informovali správce systému o opakovaných neúspěšných pokusech přihlásit se do systému. Zprávy týkající se zabezpečení se pohybují v rozmezí 2200 až 22FF a 4A00 až 4AFF. Mají předpony CPF, CPI, CPC, a CPD.
- Nastavte prověřování zabezpečení s cílem vytvořit protokol neoprávněných pokusů o přístup k objektům.

Informace najdete v tématu Prověřování zabezpečení.

Prověřování zabezpečení

Při monitorování zabezpečení může operační systém zaznamenávat události zabezpečení, které se v systému vyskytnou. Tyto události se zaznamenávají ve zvláštních systémových objektech nazývaných **příjemce žurnálu**. Žurnálové příjemce lze nastavit tak, aby zaznamenávaly různé typy událostí zabezpečení, například změnu systémové hodnoty nebo uživatelského profilu, popř. neúspěšný pokus o přístup k objektu. To, které události se zaznamenávají, určují tyto hodnoty:

- systémová hodnota QAUDCTL
- systémová hodnota QAUDLVL
- hodnota AUDLVL v uživatelských profilech
- hodnota OBJAUD v uživatelských profilech
- hodnota OBJAUD v objektech

Informace z monitorovacích žurnálů se používají k těmto účelům:

- detekce pokusů o narušení zabezpečení
- plánování migrace na vyšší úroveň zabezpečení
- monitorování použití citlivých objektů, například důvěrných souborů

K zobrazení informací z monitorovacích žurnálů různými způsoby lze použít příslušné příkazy.

Formuláře pro plánování základního zabezpečení systému

Tyto formuláře můžete zkopírovat nebo vytisknout z prohlížeče.

Chcete-li vytisknout veškeré informace o základním zabezpečení, vyberte pravé podokno a klepněte na ikonu PDF na banneru aplikace Information Center.

Chcete-li vytisknout jeden plánovací formulář, klepněte na odkaz odpovídající požadovanému formuláři. Klepněte na pravé podokno a poté klepněte v prohlížeči na ikonu Tisknout. Vybraný formulář tak vytisknete.

Zde je úplný výpis všech plánovacích formulářů, které jsou nezbytné k úspěšnému plánování a používání základního zabezpečení systému:

- formulář Plánování fyzického zabezpečení
- formulář Popis aplikace
- formulář Konvence pojmenování
- formulář Popis knihovny
- formulář Výběr systémových hodnot
- formulář Odpovědnost za systém
- formulář Identifikace skupiny uživatelů
- formulář Popis skupiny uživatelů
- formulář Profil individuálního uživatele
- formulář Seznam oprávnění
- formulář Zabezpečení výstupních front a pracovních stanic
- formulář Instalace aplikace

Formulář Plánování fyzického zabezpečení systému

Tabulka 65. Formulář Plánování fyzického zabezpečení systému

Formulář Plánování fyzického zabezpečení systému	
Zhotovil(a):	Datum:
Pokyny • Více informací o tomto formuláři najdete v tématu ″Plánování zabezpečení prostředků″. • Tento formulář použijte pro popis všech otázek zabezpečení, které se týkají fyzického umístění systémové jednotky a připojených zařízení. • Nemusíte zadávat informace z tohoto formuláře do systému.	
Systémová jednotka:	
Popište bezpečnostní opatření sloužící k ochraně systémové jednotky (například uzamčená místnost):	
Jaké nastavení uzamčení klíčem se obvykle používá?	
Kde je uložen klíč?	
Další poznámky týkající se systémové jednotky:	
Záložní média a dokumentace:	

Tabulka 65. Formulář Plánování fyzického zabezpečení systému (pokračování)

Kde jsou na vašem pracovišti uloženy záložní pásky?	
Kde jsou uloženy záložní pásky mimo vaše pracoviště?	
Kde jsou uložena hesla správce systému, obsluhy a heslo DST?	
Kde je uložena důležitá systémová dokumentace, jako je sériové číslo a konfigurace?	

Formulář Plánování fyzického zabezpečení systému			část 2 ze 2
Další pokyny pro část 2 • Níže vytvořte seznam všech pracovních stanic nebo tiskáren, jejichž umístění by mohlo znamenat bezpečnostní riziko. Určete, jaká ochranná opatření podniknete. Pro tiskárnu uveďte ve sloupci *Security Exposure* příklady důvěrných tištěných zpráv. • Umožníte-li systému, aby automaticky konfiguroval lokální zařízení, nebudete možná před instalací systému znát jména pracovních stanic a tiskáren. Pokud neznáte jména během přípravy tohoto formuláře, vyplňte pouze popis (jako například umístění) a jména přidejte později.			
Fyzické zabezpečení pracovních stanic a tiskáren			
Jméno pracovní stanice nebo tiskárny	Její umístění nebo popis	Bezpečnostní riziko	Nezbytná ochranná opatření

Formulář Popis aplikace

Tabulka 66. Formulář Popis aplikace

Formulář Popis aplikace	
Zhotovil(a):	Datum:
Pokyny • Více informací o tomto formuláři najdete v tématech ″Popis aplikace″ a ″Zabezpečení prostředků″. • Připravte si samostatný formulář pro každou aplikaci. • Nemusíte zadávat informace z tohoto formuláře do systému.	
Jméno aplikace:	Zkratka:
Stručný popis aplikace:	
Jméno primárního menu:	Knihovna:
Jméno počátečního programu:	Knihovna:
Uveďte seznam knihoven, které aplikace používá pro soubory a programy:	
Definujte pro aplikace cíle v oblasti zabezpečení, jako například to, zda jsou některé informace důvěrné.	

Formulář Konvence pojmenování

Tabulka 67. Formulář Konvence pojmenování

Formulář Konvence pojmenování	
Zhotovil(a):	Datum:
Pokyny • Více informací o tomto formuláři najdete v tématu ″Popis aplikací″. • Nemusíte zadávat informace z tohoto formuláře přímo do systému. • Tento formulář použijte k popsání toho, jakým způsobem budete přiřazovat jména objektům v systému. Uveďte příklady pro každý objekt.	
Typ objektu	**Konvence pojmenování**
Skupinové profily	
Uživatelské profily	
Seznamy oprávnění	
Knihovny	
Soubory	
Kalendáře	
Zařízení	
Pásky	

Formulář Popis knihovny

Tabulka 68. Formulář Popis knihovny

Formulář Popis knihovny	část 1 ze 2
Zhotovil(a):	Datum:
Pokyny: • Více informací o tomto formuláři najdete v tématech ″Plánování zabezpečení uživatele″ a ″Plánování zabezpečení prostředků″. • Tento formulář použijte pro popis hlavních knihoven a definování jejich požadavků na zabezpečení prostředků. • Vyplňte jeden formulář pro každou hlavní knihovnu aplikací v systému. • V tématu ″Nastavení zabezpečení prostředků″ si přečtěte, jak zadat informace z tohoto formuláře.	
Jméno knihovny:	Popisné jméno (text):
Popište stručně funkci této knihovny:	
Definujte pro knihovnu cíle v oblasti zabezpečení, jako například to, zda jsou některé informace důvěrné:	
Veřejné oprávnění ke knihovně:	
Veřejné oprávnění k objektům v knihovně:	
Veřejné oprávnění pro nové objekty (CRTAUT):	
Vlastník knihovny:	

Formulář Popis knihovny		část 2 ze 2
Zhotovil(a):	Datum:	
Jméno knihovny:		
Další pokyny pro část 2: • V rámci níže uvedeného diagramu vytvořte seznam všech jednotlivců nebo objektů vyžadujících specifické oprávnění. • Zadejte typ požadovaného oprávnění: *ALL, *CHANGE, *USE nebo *EXCLUDE.		

Vytvořte seznam specifických oprávnění pro objekty knihoven.				
Skupinový nebo uživatelský profil	Jméno objektu	Typ objektu	Potřebné oprávnění	Seznam oprávnění

Formulář Výběr systémových hodnot

Tabulka 69. Formulář Výběr systémových hodnot

Formulář Výběr systémových hodnot		část 1 ze 2
Zhotovil(a):		Datum:
Pokyny • Více informací o tomto formuláři najdete v tématu ″Plánování celkové strategie zabezpečení″. • Použijte tento formulář k zaznamenání svých voleb pro systémové hodnoty, které ovlivňují zabezpečení a přizpůsobení. • Pro vyplnění části 1 tohoto formuláře použijte volbu **1** z menu SETUP.		
Hodnoty z obrazovky Změna systémových voleb		
Systémová hodnota / síťový atribut	**Doporučená volba**	**Vaše volba**
Jméno systému		
QDATSEP (Oddělovač datumu)		
QDATFMT (Formát datumu)		
QTIMSEP (Časový oddělovač)		
QDEVNAMING (Formát pojmenování zařízení pro nová zařízení)	1 (systém iSeries)	
QPRTDEV (Systémová tiskárna)		
QSECURITY (Úroveň zabezpečení)	40	
QLMTSECOFR (Povolit správcům systému, aby se přihlásili k libovolné obrazovkové stanici)	N	
QACGLVL (Uložit informace o účtování úloh pro dokončený tiskový výstup)	N (*NONE)	

Formulář Výběr systémových hodnot		část 2 ze 2
Další pokyny pro část 2 • Více informací o části 2 tohoto formuláře najdete v tématu ″Nastavení systémových hodnot″. • Pro vyplnění části 2 použijte příkaz WRKSYSVAL (Práce se systémovými hodnotami).		
Systémové hodnoty zabezpečení		
Systémová hodnota	**Doporučená volba**	**Vaše volba**
QINACTITV (Interval prodlevy neaktivní úlohy)	30 až 60	
QINACTMSGQ (Fronta zpráv neaktivní úlohy)	*DSCJOB	

QLMTDEVSSN (Omezení relací zařízení)	1 (ano)	
QMAXSGNACN (Operace použitá v případě selhání pokusů o přihlášení se do systému)	3 (zablokovat oba)	
QMAXSIGN (Maximum povolených pokusů o přihlášení se do systému)	3 až 5	
QPWDEXPITV (Interval ukončení platnosti hesla)	30 až 60	
QPWDMAXLEN (Maximální délka hesla)	8	
QPWDMINLEN (Minimální délka hesla)	6	
QPWDPRQDDIF (Vyžadovat odlišná hesla)	7 (6 jedinečných hesel)	
Ostatní systémové hodnoty		
Systémová hodnota	**Doporučená volba**	**Vaše volba**
QDSCJOBITV (Interval prodlevy odpojené úlohy)	300	
Poznámka: Možná budete chtít nastavit některé další systémové hodnoty týkající se zabezpečení. V kapitole 3 publikace *Zabezpečení - referenční informace* (SC41-5302-04) najdete úplný seznam systémových hodnot týkajících zabezpečení a doporučeného nastavení.		

Formulář Odpovědnost za systém

Tabulka 70. Formulář Odpovědnost za systém

Formulář Odpovědnost za systém			
Zhotovil(a):			Datum:
Pokyny: • Více informací o tomto formuláři najdete v tématu ″Plánování profilů individuálních uživatelů″. • Tento formulář použijte k definování seznamu všech osob, které mají jinou třídu uživatele než *USER. • Přeneste informace z tohoto formuláře do sloupce *Třída uživatele* ve formuláři Profil individuálního uživatele.			
Kdo je vaším hlavním správcem systému? Kdo je zástupcem správce systému?			
Jméno profilu	Jméno uživatele	Třída	Poznámky

Formulář Identifikace skupiny uživatelů

Tabulka 71. Formulář Identifikace skupiny uživatelů

Formulář Identifikace skupiny uživatelů	
Zhotovil(a):	Datum:

Tabulka 71. Formulář Identifikace skupiny uživatelů (pokračování)

Pokyny:

- Více informací o tomto formuláři najdete v tématu ″Plánování skupin uživatelů″.
- Tento formulář vám pomůže určit skupiny uživatelů, které potřebují podobné aplikace.
  1. V horní části formuláře definujte seznam vašich hlavních aplikací.
  2. V levém sloupci uveďte seznam uživatelů.
  3. Označte potřebné aplikace pro každého uživatele.
- Nemusíte zadávat informace z tohoto formuláře do systému.

		Přístup potřebný pro aplikace						
Jméno uživatele	Oddělení	AP:	AP:	AP:	AP:	AP:	AP:	AP:

Poznámka:

- Pokud máte *volné* prostředí zabezpečení, označte symbolem **X** aplikace, které uživatelé potřebují.
- Pokud máte *přísné* prostředí zabezpečení, budete možná muset použít **C** (change - změnit) a **V** (view - prohlížet), abyste určili, *jak* jsou aplikace používány.

Formulář Popis skupiny uživatelů

Tabulka 72. Formulář Popis skupiny uživatelů

Formulář Popis skupiny uživatelů	část 1 ze 2
Zhotovil(a):	Datum:

Pokyny pro část 1

- V tématu ″Plánování skupin uživatelů″ si přečtěte, jak připravit tento formulář.
- V tématu ″Zabezpečení uživatele″ si přečtěte, jak vyplnit tento formulář.
- Připravte si samostatný formulář pro každou skupinu, která bude používat systém.
- Použijte příkaz CRTJOBD (Vytvoření popisu úlohy) a vytvořte popis úlohy pro skupinu. Popis úlohy obsahuje počáteční seznam knihoven skupiny.

Jméno skupinového profilu:

Popis skupiny:

Primární aplikace pro skupinu:

Definujte seznam ostatních aplikací požadovaných skupinou:

Zapište do seznamu všechny knihovny, které skupina potřebuje. Označte (✓) každou skupinu, která by měla být na počátečním seznamu knihoven pro skupinu:

Poznámka: Ve formuláři Popis aplikace vyhledejte všechny aplikace, které jsou uvedeny v předchozí části, a zjistěte, které knihovny tyto aplikace používají.

Formulář Popis skupiny uživatelů		část 2 ze 2
Další pokyny pro část 2 • Níže uvedené tabulky obsahují seznam všech polí, která se objevují na obrazovce Vytvoření profilu uživatele. Pole jsou rozdělena do dvou skupin: pole, u kterých musíte provést výběr, a pole, u kterých společnost IBM doporučuje použít předvolené hodnoty. • Použijte obrazovku Práce s uživatelskými profily nebo příkaz CRTUSRPRF (Vytvoření uživatelského profilu) a zadejte informace z této části formuláře do systému.		
Zvolte hodnoty pro tato pole ve skupinovém profilu:		
Jméno pole	**Doporučená volba**	**Vaše volba**
Jméno skupinového profilu (uživatel)		
Heslo	*NONE	
Třída uživatele (typ uživatele)	*USER	
Aktuální knihovna (předvolená knihovna)	*stejné jako jméno skupinového profilu*	
Počáteční program, který má být volán (program pro přihlášení se do systému)		
Knihovna počátečního programu		
Počáteční menu (první menu)		
Knihovna počátečního menu		
Omezení schopností (omezené použití příkazového řádku)	*YES	
Text (popis uživatele)		
Popis úlohy	*stejné jako jméno skupinového profilu*	
knihovna popisu úlohy		
Jméno skupinového profilu (skupina uživatelů)	*NONE	
Tiskové zařízení (předvolená tiskárna)		
Výstupní fronta	*DEV	
Poznámka: Pole jsou uvedena v pořadí, ve které se zobrazí na obrazovce Vytvoření uživatelského profilu (pomocí F4).		
Pro níže uvedená pole použijte hodnoty dodané systémem (předvolby):		
Účtovací kód	Ukládání údajů z klávesnice do vyrovnávací paměti	Veřejné oprávnění
Úroveň asistence	ID jazyka	Nastavit dočasnou platnost hesla
Program Attn	Omezení relací zařízení	Třídicí posloupnost
ID kódované znakové sady	Maximální paměť	Zvláštní oprávnění
ID země nebo regionu	Fronta zpráv	Zvláštní prostředí
Zobrazit informace o přihlášení se do systému	Interval ukončení platnosti hesla	Stav
Heslo dokumentu	Limit priority	Uživatelské volby
Poznámka: Pole v tomto seznamu jsou uspořádána v abecedním pořádku.		

Formulář Profil individuálního uživatele

Tabulka 73. Formulář Profil individuálního uživatele

Formulář Profil individuálního uživatele	
Zhotovil(a):	Datum:

Tabulka 73. Formulář Profil individuálního uživatele (pokračování)

Pokyny: • V tématu ″Plánování profilů individuálních uživatelů″ najdete informace o tom, jak vytvořit tento formulář. • Tento formulář použijte pro záznam informací o profilech individuálních uživatelů systému. Vyplňte jeden formulář pro každou skupinu uživatelů (skupinový profil), která se nachází ve vašem systému. • Použijte prázdné sloupce vpravo pro všechna další pole, která chcete specifikovat pro individuální uživatele. • V tématu ″Nastavení individuálních uživatelů″ si přečtěte, jak vyplnit tento formulář.						
Jména skupinových profilů						
Vlastník vytvořených objektů:			Skupinové oprávnění k vytvořeným objektům:			
Typ skupinového oprávnění:						
Zadejte záznam pro každého člena skupiny:						
Uživatelský profil	Text (popis)	Třída uživatele	Omezení schopností			

Formulář Seznam oprávnění

Tabulka 74. Seznam oprávnění, formulář

Formulář Seznam oprávnění					
Zhotovil(a):			Datum:		
Pokyny • Více informací o tomto formuláři najdete v tématu ″Plánování zabezpečení prostředků″. • Připravte si jeden formulář pro každý seznam oprávnění. • Pomocí tohoto formuláře vytvořte seznam objektů, které budou zabezpečovány tímto seznamem oprávnění a skupinami nebo jednotlivci, kteří mají k seznamu přístup. • V tématu ″Nastavení zabezpečení prostředků″ si přečtěte návod, jak vyplnit tento formulář.					
Jméno seznamu oprávnění:					
Popis:					
Vytvořte seznam objektů, které jsou zabezpečovány seznamem oprávnění.					
Jméno objektu	Typ objektu	Knihovna objektu	Jméno objektu	Typ objektu	Knihovna objektu

Tabulka 74. Seznam oprávnění, formulář (pokračování)

Vytvořte seznam skupin a uživatelů, kteří mají přístup k seznamu oprávnění.					
Skupina nebo uživatel	Typ povoleného přístupu	Správa seznamu?	Skupina nebo uživatel	Typ povoleného přístupu	Správa seznamu?

Formulář Zabezpečení výstupních front a pracovních stanic

Tabulka 75. Formulář Zabezpečení výstupních front a pracovních stanic

Formulář Zabezpečení výstupních front a pracovních stanic				
Zhotovil(a):	Datum:			
Pokyny • Více informací o tomto formuláři najdete v tématu ″Ochrana tiskového výstupu″. • V tomto formuláři zadejte údaje pro všechny pracovní stanice nebo výstupní fronty, které vyžadují zvláštní ochranu. • V tématu ″Ochrana pracovních stanic″ si přečtěte, jak vyplnit tento formulář.				
Vytvořte seznam parametrů pro vyhrazené výstupní fronty:				
Jméno výstupní fronty	Knihovna výstupní fronty	Zobrazit libovolný soubor (DSPDTA)	Oprávnění, které má být zkontrolováno (AUTCHK)	Řízení operátorem (OPRCTL)
Pracovní stanice správce systému: Pokud omezíte přístup správce systému pouze na některé pracovní stanice (systémová hodnota QLMTSECOFR je YES), vytvořte seznam pracovních stanic, ke kterým má oprávnění správce systému a jakákoliv jiná osoba s oprávněním *ALLOBJ:				
Vytvořte seznam oprávnění pro vyhrazené pracovní stanice:				
Jméno pracovní stanice	Skupiny nebo uživatelé, kterým bylo poskytnuto oprávnění (oprávnění *CHANGE)			
Poznámka: Vyhrazené pracovní stanice by měly mít veřejné oprávnění nastavené na *EXCLUDE.				

Formulář Instalace aplikace

Tabulka 76. Formulář Instalace aplikace

Formulář Instalace aplikace	část 1 ze 2

Tabulka 76. Formulář Instalace aplikace (pokračování)

Zhotovil(a):		Datum:
Pokyny • Více informací o tomto formuláři najdete v tématu ″Plánování instalace aplikací″. • Připravte si jeden formulář pro každou aplikaci, kterou budete instalovat. • Použijte tento formulář pro plánování toho, jak stanovíte vlastnictví a veřejné oprávnění k aplikacím po jejich zavedení. • V tématu ″Nastavení zabezpečení prostředků″ si přečtěte návod, jak vyplnit tento formulář.		
Jméno aplikace:		
Popis:		
Uveďte a popište všechny profily, které musí být vytvořeny, aby mohla být nainstalována aplikace:		
Jméno knihovny:		
	Před instalací	Po instalaci
Vlastník knihovny		
Vlastník objektu		
Veřejné oprávnění ke knihovně		
Veřejné oprávnění k objektu		
Veřejné oprávnění pro nové objekty		
Jméno knihovny:		
	Před instalací	Po instalaci
Vlastník knihovny		
Vlastník objektu		
Veřejné oprávnění ke knihovně		
Veřejné oprávnění k objektu		
Veřejné oprávnění pro nové objekty		

Formulář Instalace aplikace		část 2 ze 2
Jméno knihovny:		
	Před instalací	Po instalaci
Vlastník knihovny		
Vlastník objektu		
Veřejné oprávnění ke knihovně		
Veřejné oprávnění k objektu		
Veřejné oprávnění pro nové objekty		
Jméno knihovny:		
	Před instalací	Po instalaci
Vlastník knihovny		
Vlastník objektu		
Veřejné oprávnění ke knihovně		
Veřejné oprávnění k objektu		
Veřejné oprávnění pro nové objekty		
Jméno knihovny:		
	Před instalací	Po instalaci

Vlastník knihovny		
Vlastník objektu		
Veřejné oprávnění ke knihovně		
Veřejné oprávnění k objektu		
Veřejné oprávnění pro nové objekty		

Dodatek. Poznámky

Tyto informace platí pro produkty a služby nabízené v USA.

IBM nemusí v ostatních zemích nabízet produkty, služby ani a funkce popsané v tomto dokumentu. Informace o produktech a službách, které jsou ve Vašem regionu momentálně dostupné, získáte od místního zástupce IBM. Žádný odkaz na produkt, program nebo službu IBM není zamýšlen jako prohlášení nebo naznačení toho, že smí být používán pouze tento produkt, program nebo služba IBM. Místo toho je možné použít jakýkoliv z hlediska funkčnosti ekvivalentní produkt, program nebo službu, které neporušují žádné z autorských práv IBM. Za vyhodnocení a ověření činnosti libovolného produktu, programu či služby jiného výrobce než IBM však odpovídá uživatel.

IBM může mít patenty nebo podané žádosti o patent, které zahrnují předmět tohoto dokumentu. Získání tohoto dokumentu uživateli neposkytuje licenci na tyto patenty. Písemné dotazy ohledně licencí můžete zaslat na adresu:

IBM Director of Licensing
IBM Corporation
500 Columbus Avenue
Thornwood, NY 10594-1785
U.S.A.

S dotazy ohledně licencí týkajícími se informací v dvoubajtové znakové sadě (DBCS) se obraťte na oddělení IBM pro duševní vlastnictví ve své zemi nebo ve Vašem regionu, nebo zašlete písemně dotaz na adresu:

IBM World Trade Asia Corporation
Licensing
2-31 Roppongi 3-chome, Minato-ku
Tokyo 106, Japan

Následující odstavec se netýká Velké Británie nebo kterékoliv jiné země, kde taková opatření odporují místním zákonům: SPOLEČNOST INTERNATIONAL BUSINESS MACHINES CORPORATION TUTO PUBLIKACI POSKYTUJE TAKOVOU, "JAKÁ JE", BEZ JAKÝCHKOLIV ZÁRUK, VYJÁDŘENÝCH NEBO ODVOZENÝCH, VČETNĚ, BEZ OMEZENÍ, ODVOZENÝCH ZÁRUK NEPORUŠENÍ PRÁV TŘETÍCH STRAN, ZÁRUKY PRODEJNOSTI NEBO VHODNOSTI PRO URČITÝ ÚČEL. Právní řády některých zemí nepřipouštějí vyloučení vyjádřených nebo odvozených záruk v určitých transakcích a proto se na Vás výše uvedené omezení nemusí vztahovat.

Tato publikace může obsahovat technické nepřesnosti nebo typografické chyby. Informace zde uváděné jsou pravidelně aktualizovány a v příštích vydáních této publikace již budou tyto změny zahrnuty. IBM může produkt(y) anebo program(y) popsané v této publikaci kdykoli bez ohlášení zdokonalit nebo změnit.

Jakékoliv odkazy v této publikaci na webové stránky jiných společností než IBM jsou poskytovány pouze pro pohodlí uživatele a nemohou být žádným způsobem vykládány jako doporučení těchto webových stránek ze strany IBM. Materiály obsažené na takovýchto webových stránkách nejsou součástí materiálů tohoto produktu IBM a mohou být používány pouze na vlastní riziko.

Držitelé licence na tento program, kteří si přejí mít přístup i k informacím o programu za účelem (i) výměny informací mezi nezávisle vytvořenými programy a jinými programy (včetně tohoto) a (ii) vzájemného použití sdílených informací, mohou kontaktovat:

IBM Corporation
Software Interoperability Coordinator, Department 49XA
3605 Highway 52 N
Rochester, MN 55901
U.S.A.

Informace tohoto typu mohou být dostupné za určitých podmínek. V některých případech připadá v úvahu zaplacení poplatku.

Licencovaný program popsaný v těchto informacích a veškeré dostupné licencované materiály jsou společností IBM poskytovány na základě podmínek uvedených ve smlouvě IBM ICA (Customer Agreement), v Mezinárodní licenční smlouvě IBM na programy (IPLA) nebo v jiné ekvivalentní smlouvě.

Informace týkající se produktů jiných firem než IBM byly získány od dodavatelů těchto produktů, z jejich publikovaných sdělení, nebo z jiných veřejně dostupných zdrojů. IBM tyto produkty netestovala a nemůže potvrdit přesnost údajů o výkonu, kompatibilitě nebo jiná tvrzení, která se k produktům od jiných společností vztahují. Dotazy, které se týkají vlastností produktů jiných firem než IBM, musí být adresovány jejich dodavatelům.

Tyto informace slouží pouze pro účely plánování. Informace uvedené v tomto dokumentu podléhají změně před zpřístupněním produktů uvedených v této publikaci.

Tyto informace obsahují příklady dat a sestav používaných v každodenních operacích. Za účelem co nejpřesnější ilustrace obsahují tyto příklady jména osob, společností, značek a produktů. Všechna tato jména jsou smyšlená a jakákoliv podobnost se jmény a adresami používanými ve skutečném podniku je čistě náhodná.

Ochranné známky

Následující výrazy jsou ochrannými známkami IBM ve Spojených státech a případně v dalších jiných zemích.

Application System/400
AS/400
e (logo)
IBM
iSeries
Operating System/400
OS/400
400

Lotus, Freelance a WordPro jsou ochranné známky společností International Business Machines Corporation (IBM) a Lotus Development Corporation ve Spojených Státech a případně v dalších jiných zemích.

C-bus je ochranná známka společnosti Corollary Microsystems, Inc. ve Spojených státech a případně v dalších jiných zemích.

ActionMedia, LANDesk, MMX, Pentium a ProShare jsou ochranné známky nebo registrované ochranné známky společnosti Intel Corporation ve Spojených státech a případně v dalších jiných zemích.

Microsoft, Windows, Windows NT a logo Windows jsou ochranné známky společnosti Microsoft Corporation v USA a případně v dalších jiných zemích.

SET a logo SET jsou ochranné známky společnosti SET Secure Electronic Transaction LLC.

Java a všechny ochranné známky obsahující slovo Java jsou ochranné známky společnosti Sun Microsystems, Inc. v USA a případně v dalších jiných zemích.

UNIX je registrovaná ochranná známka skupiny The Open Group ve Spojených Státech a případně v dalších jiných zemích.

Ostatní jména společností, produktů a služeb mohou být ochrannými známkami nebo servisními značkami jiných firem.

Ustanovení a podmínky pro stahování a tisk publikací

Oprávnění k používání publikací, které jste se rozhodli stáhnout, závisí na níže uvedených ustanoveních a podmínkách a na Vašem potvrzení, že je akceptujete.

Osobní použití: Pokud zachováte všechny výhrady týkající se vlastnických práv, můžete tyto publikace kopírovat pro své osobní nekomerční použití. Bez výslovného souhlasu IBM nesmíte tyto publikace ani jejich části distribuovat, prezentovat ani z nich vytvářet odvozená díla.

Komerční použití: Pokud zachováte všechny výhrady týkající se vlastnických práv, můžete tyto publikace kopírovat, distribuovat a prezentovat výhradně uvnitř svého podniku. Bez výslovného souhlasu IBM nesmíte z těchto publikací vytvářet odvozená díla ani je (nebo jejich části) nesmíte kopírovat, distribuovat či prezentovat mimo rámec svého podniku.

Kromě oprávnění, která jsou zde výslovně udělena, se na publikace a veškeré informace, data, software a další duševní vlastnictví obsažené v těchto publikacích nevztahují žádná další vyjádřená ani odvozená oprávnění, povolení či práva.

IBM si vyhrazuje právo odvolat oprávnění zde udělená, kdykoli IBM usoudí, že používání publikací poškozuje její zájmy nebo že výše uvedené pokyny nejsou řádně dodržovány.

Tyto informace můžete stahovat, exportovat či reexportovat pouze při dodržení všech příslušných zákonů a nařízení včetně veškerých vývozních zákonů a nařízení USA. IBM NEPOSKYTUJE ŽÁDNOU ZÁRUKU, POKUD JDE O OBSAH TĚCHTO PUBLIKACÍ. PUBLIKACE JSOU POSKYTOVÁNY NA BÁZI ″JAK JSOU″ (AS-IS), BEZ JAKÝCHKOLIV ZÁRUK, VYJÁDŘENÝCH NEBO ODVOZENÝCH, VČETNĚ, BEZ OMEZENÍ, ODVOZENÉ ZÁRUKY PRODEJNOSTI NEBO VHODNOSTI PRO URČITÝ ÚČEL.

Stažením nebo vytištěním publikace z tohoto serveru vyjadřujete svůj souhlas s těmito ustanoveními a podmínkami.

Vytištěno v Dánsku společností IBM Danmark A/S.