Bankovní institut vysoká škola Praha

Katedra informačních technologií a elektronického obchodování

Kompletní zabezpečení systému IBM i

Bakalářská práce

Autor: **Filip Borůvka**

Informační technologie, správce informačních systémů

Vedoucí práce: **Ing. Vladimír Beneš**

Praha **Březen, 2009**

Prohlášení:

Prohlašuji, že jsem bakalářskou práci zpracoval samostatně a s použitím uvedené literatury.

V Praze dne 31. 3. 2009 Filip Borůvka

Poděkování

Rád bych poděkoval vedoucímu práce Ing. Vladimíru Benešovi za konzultace při vedení práce.

Také děkuji mému zaměstnavateli GE Money Bank, a.s. za možnost používat testovací systém IBM i pro potřeby této práce. Všem ostatním děkuji za pochopení a trpělivost.

Anotace práce

Tato práce se v první kapitole věnuje stručným základům systému IBM i. Tyto základy jsou důležité pro pochopení struktury a seznamuje čtenáře s prací na systému. Další část je věnována fyzické bezpečnosti, tj. vhodnému umístění systému, tak aby byly zajištěny optimální podmínky pro jeho činnost.
Třetí kapitola řeší koncepci zabezpečení, jak systém monitorovat a pravidelně revidovat. Ve čtvrté závěrečné kapitole je pojednáno o zálohování jako ochraně před ztrátou dat a prevenci chyb obsluhy. Tato kapitola také pojednává o replikaci dat mezi systémy.
Se vzrůstající digitalizací a množstvím citlivých dat uchovávaných elektronicky, je velmi důležité, aby bylo zajištěno adekvátní zabezpečení informačních technologií, což systém IBM i splňuje, ovšem za předpokladu dodržování pravidel uvedených v této práci.

Klíčová slova: IBM, IBM i, AS/400, iSeries, i5/OS, DB2, OS/400, System i, Bezpečnost

Annotation

The first chapter of this thesis contains brief introduction to the basics of System IBM i. This is important for understanding of the structure the work on the System is introduced. Next part is dedicated to physical security such as appropriate placement of the System so that optimal conditions for its operation are provided.
The third chapter deals with security concept for system monitoring and regular revisions. The fourth final chapter describes system backups as a way of protecting data from loss and errors caused by an operator. This chapter also describes data replication between systems.
With increasing digitalisation and increasing amount of sensitive data stored electronically it is very important that appropriate security is implemented in information technologies. System IBM i fully satisfies IT security requirements, but only if principles described in this thesis are met.

Key words: IBM, IBM i, AS/400, iSeries, i5/OS, DB2, OS/400, System i, Security

Obsah

Úvod

Cílem této práce je seznámit odbornou veřejnost (a případně další zájemce) s efektivním způsobem zabezpečení systému IBM i, aby se předešlo rizikům a případné kompromitaci systému. Druhotným cílem je seznámení se systémem IBM i, který není v ČR příliš v povědomí.

Slovo „kompletní“ v názvu může znít jako nadnesené při tomto omezeném počtu stránek, avšak pro začínajícího správce či odbornou veřejnost, která systém IBM i nezná, je shrnuto to podstatné z rozsáhlé odborné literatury.

Systém IBM i je vysoce stabilní, výkonný, bezpečný a právě bezpečnost se v současnosti dostává do popředí a bude čím dál tím důležitější.

Tato práce byla napsána na základě mých dlouholetých zkušeností se správou systému IBM i.

Pro názornost a lepší pochopení jsou obrazovky (emulace 5250) použity v původním terminálovém vzhledu (černo-zelený) a podle něj jsou často nazývány „zelené obrazovky“ anglicky „green screen“.

Pro usnadnění studia bakalářské práce v elektronickém formátu jsou v textu použity hypertextové odkazy.

1 Seznámení se systémem IBM i

IBM i (dříve AS/400 či iSeries či System i – z marketingových důvodů bylo několikrát přejmenováno) má předchůdce v systému System/38, který IBM uvolnila v roce 1978 a byl vyvinut na základě nových principů (objektová architektura).

Systém prošel za 30 let své existence několikerým přejmenováním a to jak hardwaru, tak i operačního systému. V textu dále je užíváno pro OS označení, jak IBM i, tak i5/OS a je rovnocenné.

Tabulka 1 - Vývoj jmen hardware a operačního systému

Období		**Jméno Hardware**	**Jméno OS**
říjen	1978	System/38	CPF
21. červen	1988	AS/400 (CISC)	OS/400
červen	1995	AS/400 (RISC)	OS/400
říjen	2000	eServer iSeries	OS/400
2. květen	2004	eServer i5	i5/OS
31. leden	2006	System i	i5/OS
duben	2008	Power Systems	IBM i

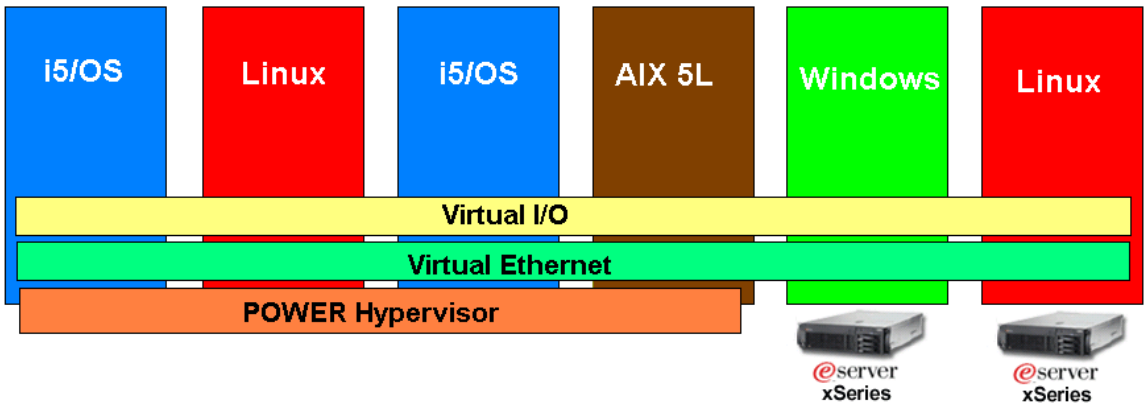
Zdroj: http://systeminetwork.com/article/they-say-it%E2%80%99s-your-birthday

IBM i je robusní, objektově orientovaný systém s integrovanou relační databází, založený na technologii PowerPC.

Systémy IBM i mohou provozovat prakticky libovolnou aplikaci, neboť se dokáží rychle a snadno přizpůsobit aplikacím, které by mohly být v budoucnosti implementované. Primární operační systém - IBM i (i5/OS) nabízí díky své šíři a rozsáhlé funkčnosti největší přizpůsobení a provozní efektivitu. Toho dosahuje prostřednictvím nativní souběžné podpory aplikací zabudovaných do RPG, COBOL, C, C++, Java, WebSphere a Domino.

Zásadní výhodou systému, je virtualizace s možností vytvoření velkého počtu tzv. LPARů logických partition (10 LPARů na 1 procesor), které jsou z hlediska OS zcela nezávislé. Na jednom fyzickém HW je možno provozovat OS IBM i, Unix, Linux a při vložení speciálního HW i OS Windows. Mezi jednotlivými LPARy je možno dynamicky (za provozu) přesouvat CPU (po 0,1 dílu CPU), operační paměť, jednotlivé karty např. řadiče páskových zařízení, síťové karty. Mezi jednotlivými LPARy je možné komunikovat přes virtuální ethernet, takže komunikace se nedostává do běžné sítě a tím pádem ji nezatěžuje.

Obrázek 1 - Integrace různých OS pomocí LPAR



Zdroj: Vlastní

Systém IBM i je firmou IBM doporučován jako integrační platforma, i5/OS má v sobě implementován PASE, které umožňuje portaci libovolné Unixové nebo Linuxové aplikace. Nejnověji je v IBM i integrován OpenSSL, PHP, MYSQL a IBM uvažuje i o dalších aplikacích.[1]

1.1 Základní principy

Systém IBM i je založen na tzv. vrstvené architektuře – je navržen tak, aby jednotlivé vrstvy byly zaměnitelné bez zásahu do vrstev ostatních tzn. upgrade HW bez zásahu do vrstvy OS a aplikační vrstvy, upgrade OS bez zásahu do aplikační vrstvy. Tyto podmínky jsou víceméně dodržovány, ovšem v případě zásadních změn, mohou být stanoveny určité prerekvizity (např. nutnost nasazení nové verze OS, bude-li použit procesor nové generace).

Systém IBM i je založen na objektové architektuře, tzn. to co se do systému ukládá nebo se z něj načítá, je objekt (programy, databázové soubory, fronty zpráv, komunikační zařízení a uživatelské účty). Objekt se skládá ze záhlaví (společný tvar pro všechny typy objektů) a funkční části (pro každý typ objektu je jiné).

1.1.1 Paměť

Veškerá paměť systému operační i disková je adresována jednotně (jedné se o tzv. virtuální paměť), je to jedna souvislá vrstva, takže se uživatel nemusí zabývat o to, kde se jednotlivé objekty nachází – jen se na ně odvolává jménem. Díky použití virtuální paměti, lze bez

[1] ***System i – operační systém***, *http://www-03.ibm.com/systems/cz/i/software/os/*

modifikace aplikačních a systémových programů využívat nových technologií pamětí a procesorů. [2]

1.1.2 Licenční programy

Vlastní OS se skládá z jednotlivých modulů – licenčních programů, které je možné instalovat, vyjímat a fixovat samostatně, základní licenční programy jsou v uvedeny tabulce:

Tabulka 2 - Základní označení licenčních programů systému IBM i

Kód	Popis	Použití
5761999	Licence Internal Code	Rozhraní mezi HW a OS
5761SS1	i5/OS	Vlastní operační systém – včetně dalších licenčních podprogramů tzv. options
5761TC1	IBM TCP/IP Connectivity Utilities for i5/OS	Implementace TCP/IP protokolu – Telnet, FTP a další služby
5761DG1	IBM HTTP server for i5/OS	Webový server
5761JV1	IBM Developer Kit for Java	Java Virtual Machine

Zdroj: Vlastní

1.1.3 Prostředí systému

Systém IBM i má dvě prostředí pro ukládání objektů nebo souborů a to:

- **Objektové prostředí** (Obrázek 2) – objekty jsou uloženy v tzv. knihovnách.

  V tomto prostředí jsou uloženy objekty různých typů (Databázový soubor je objekt typu *FILE, program typu *PGM, příkaz typu *CMD, uživatelský profil tyou *USRPRF.) Každý objekt musí být přiřazen do nadřazené složky, která se nazývá knihovna (library).

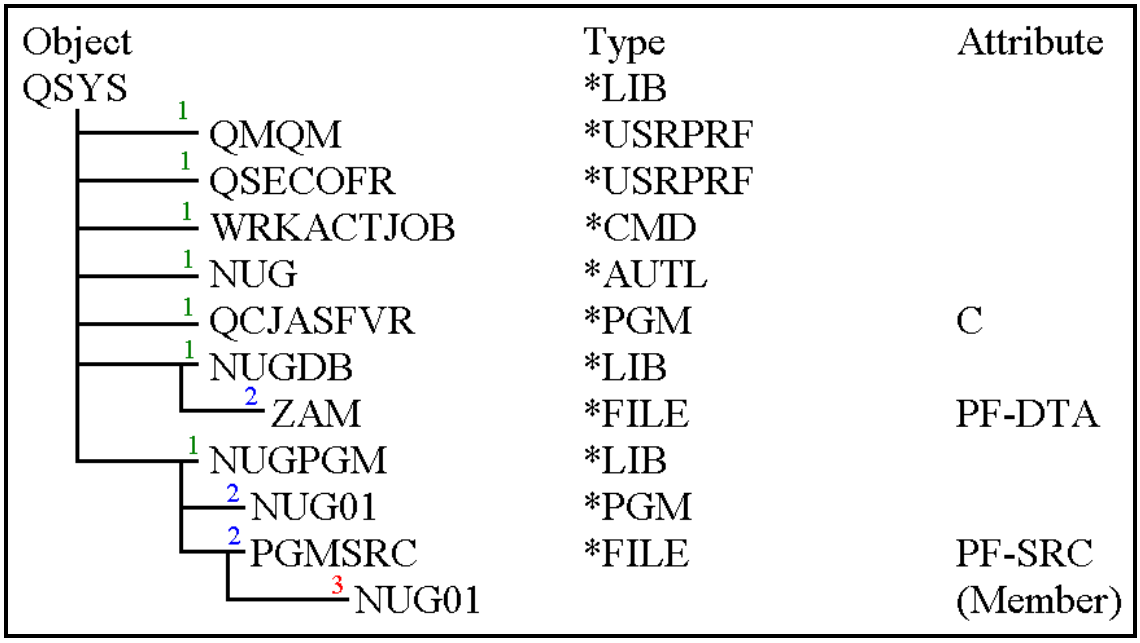
  Knihovna je též objekt a to typu *LIB – všechny knihovny a systémové objekty jsou v hlavní systémové knihovně, která se jmenuje QSYS (všechny systémové objekty začínají písmenem Q* a není radno je měnit).

  Systémové objekty mohou být pouze v knihovně QSYS a jedná se o objekty typu Library *LIB, User Profile *USRPRF, Device Description *DEVD, Line Description *LIND, Controller Description *CTLD, Authorization Lists *AUTL. Obrázek 2 podrobně ukazuje objektovou strukturu systému IBM i

  (1 – úroveň knihovna, 2 – úroveň objekt, 3 – úroveň člen (member))

[2] ***ŽUPKA, Vladimír; kolektiv IBM***. *Základy AS/400. 1. vyd. Praha*

Obrázek 2 – Struktura objektového prostředí

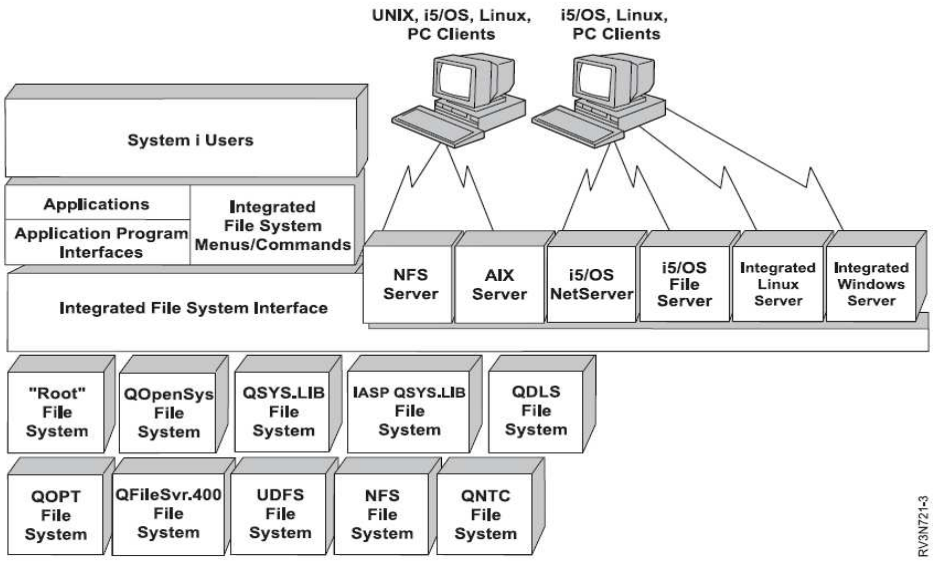


Zdroj: Vlastní

- **Souborové (integrované) prostředí** (IFS) – jsou v něm uloženy soubory kompatibilní se soubory typu UNIX/Linux, Windows, Netware, případně lze vytvořit vlastní souborový systém (filesystem).

  Souborové prostředí je z hlediska funkčnosti stejné jako pro systém Windows, tj. obsahuje adresáře a soubory, jen oprávnění je řešeno podrobněji.

Obrázek 3 – Souborový systém (IFS)



Zdroj: http://publib.boulder.ibm.com/infocenter/systems/scope/i5os/index.jsp?topic=/ifs/rzaaxfsknow.htm

1.2 Obsluha systému – uživatelské rozhraní

Operační systém IBM i (i5/OS) má perfektním způsobem vymyšlenou a propracovanou obsluhu a práci v režimu příkazové řádky, na základě emulace 5250[3]. Pro správu OS, je též možné použít grafickou nadstavbu - Navigator for i[4].

Práce v systému probíhá pomocí příkazů řídícího jazyka (CL), příkazy jsou koncipovány na základě zkratek pro činnost a objekt činnosti:

Nejdůležitější činnosti:	**Význam:**
ADD, RMV	Add – přidat, Remove – vyjmout
CHG	Change – změnit
DSP	Display – zobrazit
GO	Go – jít (na nabídku v menu)
PRT	Print – tisknout
RST, SAV	Restore – obnovit, Save – uložit
SBM	Submit – předat k dávkovému zpracování
WRK	Work with – pracovat s (objekty, činnostmi, stavy)

Činnost+Objekt činnosti:	**Význam:**
WRKACTJOB	Work with Active Jobs
WRKCMD	Work with Commands
WRKCTLD	Work with Ctl Descriptions
WRKHDWRSC	Work with Hardware Resources
WRKJOB	Work with Job
WRKJOBQ	Work with Job Queue
WRKJRN	Work with Journal
WRKLIB	Work with Libraries

Obdobně lze místo WRK použít i další zkratky pro činnosti.

Pro každý příkaz lze pomocí klávesové zkratky **F4** získat prompt příkazu a použitím **F1** dostaneme nápovědu. Při stisku F1 mimo volby dostaneme nápovědu celkovou, při stisku

[3] http://www-03.ibm.com/systems/i/software/access/

[4] http://www-03.ibm.com/systems/i/software/navigator/

nad konkrétní volbou dostaneme nápovědu ke konkrétní položce. Pomocí klávesy F9 lze vyvolat dříve zadané příkazy. [5]

1.3 Zabezpečení

Zabezpečení systému IBM i bylo v systému navrženo už v jeho počátcích, je vždy přítomné a nelze jej obejít – je vždy aktivní, dá se jen řídit jeho úroveň[6].

Zabezpečení systému se skládá z několika částí – Systémové hodnoty (systémový audit, bezpečnostní pravidla); uživatelské a skupinové profily, autorizační listy; exit pointy (při použití určité funkčnosti je zavolán nadefinovaný program, který provede příslušnou kontrolu). Více je o zabezpečení pojednáno v dalších kapitolách.

1.4 Databáze

Databáze v Systému IBM i je integrovaná DB2 for i5/OS, je dodávána společně se systémem. DB2 for i5/OS také poskytuje mnoho dalších funkcí a vlastností, např. triggers, uložené procedury a další.

Jako interface do DB2 for i5/OS slouží licenční produkt IBM DB2 Query Manager and SQL Development Kit for i5/OS, který pomáhá zadávat SQL dotazy formou průvodce.

Databáze je tvořena sadou tabulek (objekt typu *FILE, atribut PF-DTA) a logických souborů (*FILE, LF). Veškeré změny v databázi jsou současně se změnou dat v tabulce z důvodu případného návratu k určitému bodu logovány, jedná se o žurnálování. Žurnálování umožňuje nejen vrácení databáze do určitého stavu, ale též dohledat veškeré změny, které byly provedeny a dohledat kdo je, kdy a odkud provedl. Pro práci s databází se používá SQL nebo častěji RPG programy, které jsou nativním programovacím jazykem i5/OS a jsou výrazně výkonnější než SQL. V systému i5/OS je možné též provozovat programovací jazyky C, C++, Cobol, Java. Zdrojové kódy se ukládají do objektů typu *FILE s atributem PF-SRC, v jednom souboru může být více zdrojových položek – memberů. Objekt typu *FILE, PF-DTA mohou mít také více členů (memberů), ale to se využívá v podstatě pouze pro logy - třeba za každý den jeden, kvůli lepší práci s nima.

1.5 Řízení práce (Work Management)

V systému běží úlohy, které jsou pod konkrétními subsystémy, při přihlášení uživatele do systému se vytvoří úloha, které se přidělí do interaktivního subsystému (QINTER). Pokud

[5] ***ŽUPKA, Vladimír; kolektiv IBM***. *Základy AS/400. 1. vyd. Praha*

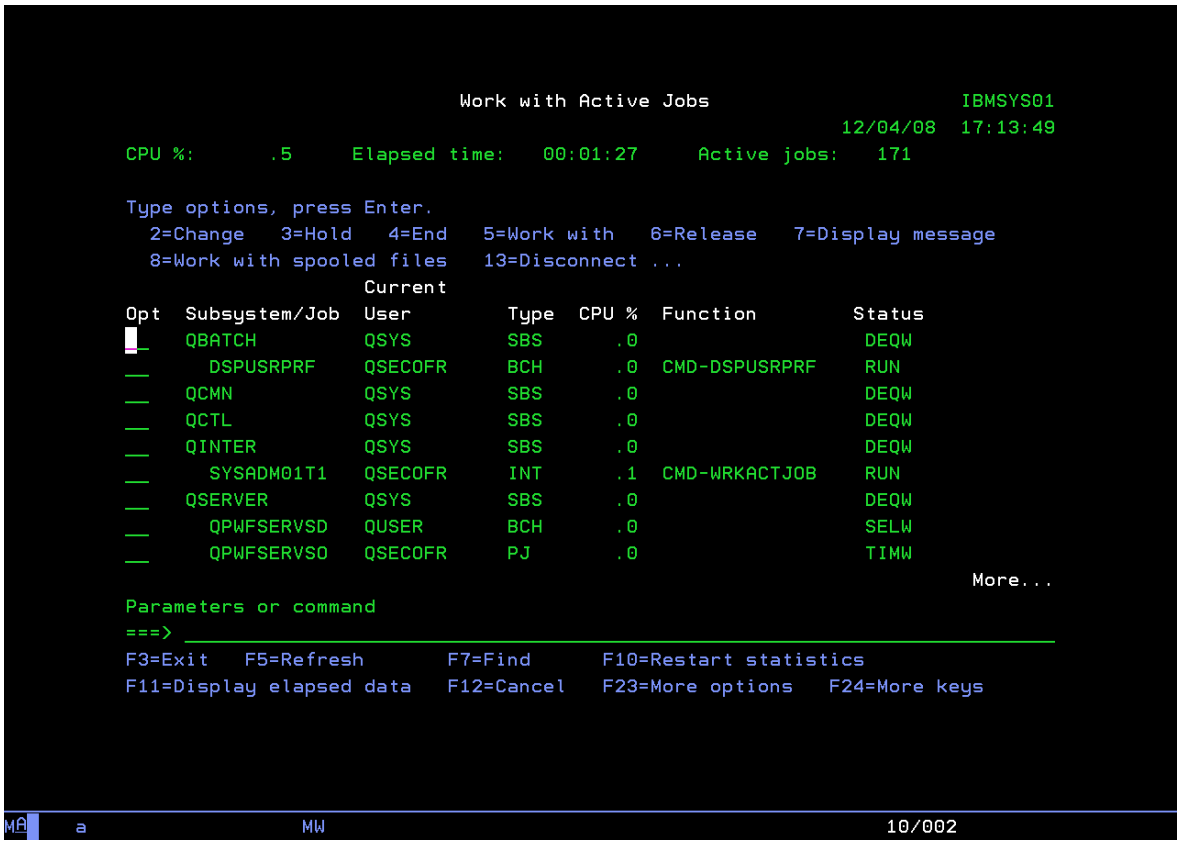
[6] ***SOLTIS G., Frank***. *Systém AS/400 zevnitř, 1. vyd. Praha*

se spustí dávkové zpracování, je příslušná úloha přidělena do dávkového subsystému (QBATCH)

V úloze je možné řídit různé parametry, priority, logování, tiskové výstupy a řadu dalších (celkem se jedná o 40 parametrů).

Přidělování úloh do subsystémů se provádí na základě nastavení různých parametrů. V subsystému lze nastavovat specifické parametry a to zejména pevné alokování paměti (WRKSHRPOOL) a priority subsystému. Všechny aktivní subsystémy a úlohy lze zobrazit příkazem WRKACTJOB viz obrázek.

Obrázek 4 - Výstup příkazu WRKACTJOB



Zdroj: Vlastní

1.6 Komunikace

Systém IBM i podporuje komunikační protokoly SNA a TCP/IP.

Před vlastní konfigurací protokolů je potřeba nastavit komunikační linky, na kterých se nastavuje, která fyzická síťová karta bude použita, MAC adresa, rychlost, duplex a popis linky.

1.6.1 Protokol SNA

Protokol SNA byl vyvinut firmou IBM a sloužil pro komunikaci mezi serverovými systémy a posléze i pro komunikaci Klient-Server. Jedná se o protokol robusní, avšak poměrně složitý při nastavování na rozdíl od protokolu TCP/IP.

V současnosti se od protokolu SNA ustupuje, protože při jeho nativním používání se musí používat síťové prvky, které SNA pakují do TCP/IP a na druhé straně SNA zase rozbalí.
Pro zajištění kompatibility implementovala firma IBM do systému službu AnyNet (SNA over TCP/IP), v této službě je prováděno pakování SNA do TCP/IP protokolu přímo v systému, takže odpadá používání speciálních síťových prvků, navíc nové síťové karty pro midrange a mainframe systémy už protokol SNA nepodporují.

Od verze V5R4 implementovala firma IBM službu Enterprise Extender (EE), která nahrazuje AnyNet, EE je snadnější na konfiguraci a výkonnější (používá UDP porty 12000 – 12004)

1.6.2 Protokol TCP/IP

Protokol TCP/IP je v systému implementován jako licenční program, některé části jsou licenční podprogramy operačního systému 5722SS1 (Option 12 - Host Servers, option 31 - Domain Name System a kryptografický modul – option 34 - Digital Certificate Manager)
Systém podporuje TCP/IP verze 4 a verze 6.
Hlavní menu TCP/IP se zavolá pomocí příkazu CFGTCP, v tomto menu lze nastavit všechny potřebné parametry (Konfigurace TCP/IP interface, default gateway, Domain information (Host name, Domain name, Domain search list, Host name search priority a DNS servery) globální parametry TCP/IP a parametry jednotlivých služeb (FTP, Telnet, SMTP, NTP, SNMP, DRDA, DDM, RouteD – RIP2, OSPF a další proprietární služby IBM)
V systému je implementována služba NetServer, která emuluje službu sdílení souborů ve Windows (SMB protokol)
Pomocí aplikace DCM – Digital Certificate Manager je možné vytvořit certifikační autoritu (CA), serverové certifikáty a ty přidělovat jednotlivým službám pro možnost komunikace pomocí SSL. V případě potřeby je možné použít i VPN službu. Pro zajištění

kontinuity komunikace pří výpadku síťové karty je možné použít virtuální IP adresy, které jsou vázané na konkrétní adresy fyzických rozhraní.

1.7 Shrnutí kapitoly

Obsluha systému IBM i, byla už v počátcích navržena, tak aby byla jednoduchá (v minulosti, před rozšířením počítačových sítí, jak je známe dnes se k práci používaly twinaxové terminály) a příkazy logicky odvoditelné, případně zjistitelné v dobře zpracované nápovědě. Příkazový prompt (CL) díky své propracovanosti výrazně zjednodušuje správu systému a ani v současnosti používané grafické programy pro správu systému (Navigator for i[7]) implementovaný prompt[8] nepřekonaly.

[7] http://www-03.ibm.com/systems/i/software/navigator/

[8] CL command information and documentation : http://publib.boulder.ibm.com/infocenter/systems/scope/i5os/index.jsp?topic=/rbam6/rbam6alphalist.htm&tocNode=int_96278

2 Fyzická bezpečnost systému IBM i

Základním předpokladem bezpečného systému je jeho umístění v adekvátním prostoru (fyzické omezení vstupu, vhodné klimatické podmínky, požární bezpečnost a trvalý dozor nad tímto prostorem) - tento specializovaný prostor se nazývá datové centrum (též počítačový sál, či slangem: serverovna; anglicky: data center, computer room, server room). Dále bude pro datové centrum používána zkratka DC.

Tato kapitola slouží jako přehled, co je třeba zajistit pro umístění počítačových systémů, podrobný popis by vydal na samostatnou práci. Prezentace včetně fotografií k tomuto tématu lze nalézt v prezentaci „Vybavení datového centra[9]“

2.1 Umístění DC

Při umístění datového centra je třeba pamatovat na:

- Umístění počítačového sálu je ideální v 1. NP (podzemní podlaží jsou rizikové z hlediska průniku vody, kondenzace vlhkosti a následné vzniku plísně, přízemí je rizikové z hlediska průniku cizí osoby).
- Nosnost základní podlahy a zdvojené (zvýšené) podlahy.
- Stěhovací cestu (nákladní výtah, vhodné schodiště).
- Stavební a další povolení.

2.2 Prostor DC

Prostorem DC je myšlen hrubý prostor sálu tj. podlaha, strop a stěny, kde při dodržování určitých pravidel dojde ke zvýšení bezpečnosti DC a snížení nákladů.

2.2.1 Podlaha

Podlaha může být jednoduchá nebo zvýšená:

- Jednoduchá – použitelné jen pro malé místnosti a malým počtem umístěné techniky.
- Zvýšená (anglicky: raised floor) (mezera mezi základní a zvýšenou podlahou (prostor je ideálně kolem 80 cm)) .
    - Malá mezera (do 50 cm) mezi základní betonovou deskou.
    - Velká mezera (nad 50 cm) mezera mezi základní betonovou deskou.

[9] http://vse.boruvka.cz/03_Prez_200812_Vybaveni_datoveho_centra_IBM_i.ppt

- Pro zvýšenou podlahu lze použít samonosné desky (vhodné pro sály, kde je častý přístup pod podlahu) nebo šroubovací desky (jsou levnější, ale při častém otevírání, dochází k poškození vnějších závitů šroubů a vnitřních závitů v ocelové konstrukci nosníků zvýšené podlahy).

2.2.2 Strop

- Je vhodné opatřit speciální tenkou izolační vrstvou, která zajistí zvukovou a tepelnou izolaci mezi DC a sousedícím podlažím.
- V případě malého prostoru uvnitř zvýšené podlahy je možné na strop umístit rošty pro vedení datových kabelů (to je vhodné zejména pro optické kabely).

2.2.3 Stěny a okna

- U menších počítačových sálů je vhodné opatřit okna ochrannou folií, která zabrání pohledu do DC a výrazně sníží zahřívání DC z okolního prostředí. Je nezbytné aby okna měla patřičnou kvalitu.
- Je možné použít i vhodné žaluzie.
- U větších počítačových sálů lze vybudovat druhou vnitřní izolační stěnu a vzniklý prostor použít jako sklad (okna se chrání výše uvedeným způsobem).

2.3 Napájení DC

Veškerá zařízení umístěna v DC je nezbytné zajistit proti výpadku napájení, pro to je třeba splnit:

- Zdvojené silové napájení (ideálně dva motorgenerátory (diesel agregáty), dvě UPS, dvě kabelová vedení – v praxi se běžně používá jen jeden motorgenerátor, vzhledem k rozměrům, hluku a jeho ceně).
- Napájení klimatizací pouze z motorgenerátoru (krátký výpadek chlazení do náběhu generátoru je zanedbatelný oproti dimenzování UPS pro napájení klimatizací).
- Jsou-li používány dva okruhy, pak je vhodné zásuvky odlišit barevně.
- Pro UPS je nezbytné hlídat kapacitu baterií a včas je vyměnit.
- Pravidelné provádění testů (jednou za měsíc).
- Předřazené prvky zajistí kvalitní napájení elektrickou energií (vyhlazení špiček a dalších poruch na síti a tím ochranu výpočetních systémů).

- Zdvojení silových HW komponent (u některých systémů to bývá volitelné – je to třeba ohlídat při nákupu).
- Každou zásuvku je nutné jistit samostatným jističem s pomalou vypínací charakteristikou (špičkový náběh serverů).
- Je užitečné aby správci systémů, případně další kritické týmy měly svoje osobní počítače napájené taktéž ze záložního zdroje (zajištění kontinuity podpory a navázaných procesů).
- Příkon DC je třeba monitorovat a včas naplánovat navýšení příkonu.

2.4 Chlazení DC

Počítačové systémy svojí činností vytvářejí přebytečné teplo, které je třeba odvádět:

- Centrální klimatizační jednotky vhání do prostoru DC (často i mezi zdvojenou podlahu) chladný vzduch, který počítačové systémy nasávají.
- Lokální stojanové (rackové) chlazení (nad každým stojanem je tzv. čepice, která do přední části (nasávací) vyfukuje studený vzduch).
- Užitečné je na vhodných místech monitorování teploty a vlhkosti, sběr těchto dat v reálném čase jejich grafická prezentace a případné vyvolání poplachu při překročení prahových hodnot.
- Detekování výpadku klimatizačních jednotek.
- Náklady na provoz klimatizačních jednotek je možné snížit zvýšením teploty chlazení tzn. DC zbytečně nepřechlazovat.
- Prostředí DC je též možné upravovat pomocí parních zvlhčovačů (např. NORDMANN série AT 3000, NOVAP 3000,) instalaci je vhodné provést včetně pojistné vany, pro případný únik vody. Pro zvlhčovač prostředí je nezbytný přívod vody a odpad.
- Pro zachycení prachu a zamezení případné kontaminace prostředí DC lze u vstupu do prostoru použít speciální rohože (např. rohož 3M™ Nomad™ Contamination Control 4300).

2.5 Požární bezpečnost DC

I když veškerá zařízení používaná v DC jsou velmi spolehlivá, tak může dojít k jejich poruše a následkem toho k zahoření, pak je vhodné použití detekčních a zhášecích zařízení:

- Lokální zhášení a detekce zahoření ve stojanu - detekční trubička pod tlakem, kdy při dosažení 100 °C dojde k jejímu protržení a následkem toho zhášení z nádoby s inertním halonovým plynem umístěné pod podlahou a současně s tím dojde k vyhlášení poplachu.
- Ohňových čidel.
- Kouřová čidla s přisáváním (kvůli proudění vzduchu je potřeba pro detekci kouře použití aktivního přisávání vzduchu).
- Detekční a zhášecí zařízení je třeba umístit i do zdvojené podlahy.
- Centrální zhášení – k aktivaci automatického zhášení dojde při kombinaci více poplachů, případně ho lze spustit ručně (Pro centrální zhášení lze použít plyn, to je ale poměrně drahé a pravidelně se musí měnit. Lze také použít generátory hasícího aerosolu, které mají dlouhou trvanlivost a také zabírají méně místa, než bomby při centrálním zhášení plynem.
- V případě zahoření stojanu je potřeba provést ohledání dílů zasažených nejen ohněm, ale i kouřem, který je agresivní a zasažené díly se díky agresivitě zplodin hoření stávají nespolehlivými a začínají korodovat.

2.6 Dozor 24/7 a monitorování DC

Jedná-li se o kritické pracoviště je třeba zajistit stálý dozor operátorů DC, monitoring kritických systémů a parametrů DC:

- Jedná se většinou o 12ti hodinové směny.
- Operátoři DC vykonávají potřebné úkony (noční zpracování) a vše zapisuji.
- Operátoři DC reagují na poplach z monitoringu.
- Je nezbytné zajištění pracovní pohotovosti příslušných osob, pokud na nastalou situaci neexistuje zdokumentovaný postup řešení – zajišťují systémoví specialisté či aplikační podpora.

2.7 Elektronické zabezpečení DC

Datové centrum je třeba zajistit proti vstupu neoprávněných osob a samotný prostor monitorovat, to zajistí:

- Čtečka vstupních karet.
- Kamerový systém (se záznamem).
- Elektronický zabezpečovací systém (EZS).

- Nouzový systém (okamžité vyvolání poplachu aktivací speciálního tlačítka např. při úrazu, nevolnosti).

2.8 Záložní DC

Při živelné pohromě nebo po provedení hasebního zásahu HZS vodou z důvodu zahoření celé budovy, či záchrany osob z ohroženého prostoru dojde k odstavení celého DC, pak je nezbytné mít data případně celé systémy v dostatečně vzdálené lokalitě:

- Jedná se o záložní pracoviště (DRC - Disaster Recovery Centrum).
- Pro méně kritické systémy jen umístění záloh (křížové zálohování) a pak teprve na připravené (smluvně zajištěné) systémy provést obnovu – 1 až 2 denní výpadek.
- Pro kritické systémy provádět replikaci dat v reálném čase (uživatelské účty, programové objekty) a dat (databáze – aplikace žurnálových změn).
- Vzdálené (křížové) zálohování – z jedné lokality do druhé (úplné (full) a přírůstkové (incremental)).
- Rozšíření kapacity přenosových optických linek – technologie DWDM (Multiplexing).
- Existence krizových plánů.
- Pravidelné testování přechodu na záložní DC (pokud bylo plánované přepnutí 3x za sebou v pořádku, lze uvažovat o předem neohlášeném (je znám jen měsíc kdy k tomu dojde), avšak kontrolovaném přepnutí).

2.9 Shrnutí kapitoly

Pro zajištění kontinuity podnikání je nezbytné zajistit spoustu opatření, která jsou organizačně, technicky i finančně náročná, avšak teprve v krizových situacích je tato investice patřičně zhodnocena a při pohromách většího rozsahu to je velkou konkurenční výhodou.[10]

[10] ***BORŮVKA, Filip.*** *Přednáška VŠE – IT Management*

3 Návrh zabezpečení a preventivní kontroly systému IBM i

Zabezpečení je důležitou částí informačních systémů, bez určitých omezení by všichni mohli dělat vše a neexistovala by kontrola, kdo co udělal a hrozilo by poškození a zneužití dat v informačních systémech. V této kapitole je popsán úvod do zabezpečení systému IBM i, jsou zde uvedeny informace o systémových logách, je nastíněno nastavení systému a uvedena preventivní bezpečnostní opatření.

3.1 Základní principy bezpečnosti systému IBM i

Jak už bylo řečeno v kapitole 1. „Seznámení se systémem IBM i“ vše co je v systému je objekt a to platí i pro zabezpečení systému IBM i, objekty nesoucí bezpečnostní informace jsou:

- **Uživatelské profily (*USRPRF)**

  Uživatelský profil (uživatelský účet) je objekt přidělený uživateli, který určuje jeho identitu. U každého profilu musí být uveden jeho uživatel (vlastník) a jednoznačná identifikační hodnota (např. osobní číslo).

  Zvláštním případem uživatelského profilu je skupinový (group) profil (GRPPRF), ten má přiřazeno GID (Group Identification). Skupinový profil se používá pro hromadné zpřístupnění objektů, na konkrétní objekty je nastaveno oprávnění na skupinový profil, který se přiřadí uživatelskému profilu jako group profile (GRPPRF), ten může být jen jeden nebo suplementar (doplňový) GRPPRF (SUPGRPPRF), těch může být až 15.

  Pro manipulaci s uživatelskými profily lze použít menu CMDUSRPRF (**GO CMDUSRPRF**), ve kterém jsou všechny používané příkazy a odkazy na další související menu. Nejčastěji se používá příkaz **WRKUSRPRF** (Work with User Profiles) a **CHGUSRPRF**[11] (Change User Profile). Seznam parametrů je ukázán na profilu QSECOFR viz Příloha č. 6.

- **Autorizační listy (*AUTL)**

  Autorizační list sdružuje uživatelská oprávnění, ale je založen na jiném principu než skupinový profil. U skupinových profilů je přidáván skupinový profil (GRPPRF) do uživatelského profilu (*USRPRF) a na jeden objekt lze přidat více skupinových

[11] http://publib.boulder.ibm.com/infocenter/systems/scope/i5os/index.jsp?topic=/cl/chgusrprf.htm

profilů, zatímco na jeden objekt je možno přidat jen jeden autorizační list (*AUTL) - a uživatelské profily (*USRPRF) jsou přidávány do autorizačního listu (*AUTL) včetně oprávnění k sadě objektů chráněných tímto autorizačním listem.

Pro manipulaci s autorizačními listy lze použít menu CMDAUTL (**GO CMDAUTL**), ve kterém jsou všechny používané příkazy. Nejčastěji se používá příkaz **WRKAUTL**[12] (Work with Authorization Lists).

3.1.1 Bezpečnostní systémové hodnoty

Bezpečnostní systémové hodnoty (Security System Values) určují jakým způsobem bude systém zabezpečen. Tyto hodnoty lze vypsat příkazem **WRKSYSVAL *SEC**.

Nejdůležitější bezpečnostní hodnoty jsou:

- **QSECURITY (System security level)**

Tato hodnota určuje úroveň zabezpečení systému.

Tabulka 3 - Hodnoty QSECURITY

Hodnota QSECURITY	Popis
10	Při úrovni zabezpečení 10 neexistuje žádná ochrana. Úroveň zabezpečení 10 se proto nedoporučuje.
20	Při úrovni zabezpečení 20 jsou všechny profily standardně vytvořeny se zvláštním oprávněním *ALLOBJ, proto se tato úroveň zabezpečení také nedoporučuje.
30	Systém vyžaduje k přihlášení heslo a uživatelé musí mít oprávnění k přístupu k objektům a systémovým prostředkům.
40	Systém vyžaduje k přihlášení heslo a uživatelé musí mít oprávnění k přístupu k objektům a systémovým prostředkům. Program selže, když se uživatelé pokusí použít objekty přes nepodporovaná rozhraní. Úroveň zabezpečení 40 zabraňuje potenciálnímu vzniku rizika narušení integrity nebo zabezpečení, které ve zvláštních případech mohou vyvolat programy se schopností obejít zabezpečení. Úroveň zabezpečení 50 poskytuje instalacím s přísnými požadavky na zabezpečení rozšířenou ochranu integrity.
50	Systém vyžaduje k přihlášení heslo a uživatelé musí mít oprávnění k přístupu k objektům a systémovým prostředkům. Program selže, když se uživatelé pokusí poslat nepodporované hodnoty parametrů na nepodporovaná rozhraní nebo pokud se pokusí použít objekty přes nepodporovaná rozhraní. Úroveň zabezpečení 50 je navržena tak, aby vyhovovala požadavkům definovaným v profilu CAPP (Controlled Access Protection Profile) a kritériu CC (Common Criteria). Úroveň zabezpečení 50 je určena pro instalace s přísnými požadavky na zabezpečení, protože poskytuje to, co úroveň zabezpečení 40, a navíc nabízí rozšířenou ochranu integrity.

Zdroj: http://publib.boulder.ibm.com/infocenter/systems/scope/i5os/index.jsp?topic=/rzarl/rzarlaudcon.htm

[12] http://publib.boulder.ibm.com/infocenter/systems/scope/i5os/index.jsp?topic=/cl/wrkautl.htm

Hodnota dodávaná s novým systémem je 40 a je plně postačující. Hodnotu 50 některé aplikace nemusí podporovat a mají s ní problémy. Při změně této hodnoty, je aktivace provedena restartem (IPL).

- **QAUDCTL (Auditing control - řízení auditování)**

Definuje, má-li se auditovat, tato hodnota aktivuje auditování událostí na systému.

Pro nastavení auditování na objekty se používají příkazy:

Změna monitorování objektu (CHGOBJAUD)

Změna monitorování uživatele (CHGUSRAUD)

Tabulka 4 - Hodnoty QAUDCTL

Hodnota QAUDCTL	Popis
*NONE	Auditování není prováděno pro uživatelské akce a objekty.
*NOTAVL	Zobrazení této hodnoty indikuje, že systémová hodnota není uživateli k dispozici, protože uživatel nemá ani speciální oprávnění *AUDIT ani speciální oprávnění *ALLOBJ. Systémovou hodnotu nelze nastavit na tuto hodnotu.
*OBJAUD	Provádí se auditování objektů, které byly vybrány pomocí příkazů CHGOBJAUD, CHGDLOAUD a CHGAUD.
*AUDLVL	Je prováděno auditování všech funkcí vybraných systémovými hodnotami QAUDLVL a QAUDLVL2 a parametrem AUDLVL jednotlivých uživatelských profilů. Úroveň auditování uživatele se určí pomocí příkazu CHGUSRAUD (Změna auditování uživatele).
*NOQTEMP	Je-li objekt v knihovně QTEMP, auditování většiny činností není prováděno. Tuto hodnotu musíte zadat spolu s jednou z výše uvedených hodnot (*OBJAUD nebo *AUDLVL).

Zdroj: http://publib.boulder.ibm.com/infocenter/systems/scope/i5os/index.jsp?topic=/rzarl/rzarlaudcon.htm

- **QAUDLVL (Security auditing level)**

Definuje co se má auditovat viz Příloha č. 5, tato systémová hodnota říká, které auditní události se budou zapisovat do auditních logů, tzv. žurnálů.

- **QCRTOBJAUD (Create object auditing)**

Tato hodnota říká jak budou auditovány nově vytvářené objekty. Viz tabulka 5.

Tabulka 6 - Hodnoty QCRTOBJAUD

Hodnota QCRTOBJAUD	Popis
*NONE	Pro objekt není prováděno auditování.
*NOTAVL	Tato hodnota indikuje, že hodnota parametru není uživateli k dispozici, protože uživatel nemá speciální oprávnění *AUDIT nebo *ALLOBJ. Systémovou hodnotu nelze nastavit na tuto hodnotu.
*USRPRF	Auditování objektu je založeno na hodnotě v uživatelském profilu uživatele, který požaduje přístup k objektu.
*CHANGE	Při každé změně objektu, která souvisí se zabezpečením, je zapsán auditní záznam.
*ALL	Při každé operaci důležité pro zabezpečení a ovlivňující obsah objektu je zapsán auditní záznam. Auditní záznam je dále zapsán také při každé změně obsahu objektu, která souvisí se zabezpečením.

Zdroj: http://publib.boulder.ibm.com/infocenter/systems/scope/i5os/index.jsp?topic=/rzarl/rzarlaudcon.htm

3.1.2 Systémové hodnoty týkající se hesel

Tyto hodnoty stanovující pravidla pro hesla při přihlašování uživatelů a mezi nejdůležitější patří:

- **QPWDLVL (Úroveň hesel)**

Stanovuje úroveň hesel. Tato systémová hodnota byla uvedena ve V5R1 i5/OS. Pro změny mezi jednotlivými hodnotami existují přesné postupy, které je třeba dodržet, jinak může dojít ke ztrátě hesel. [13]

Hodnoty 0 a 1 podporují maximálně 10 znaků v hesle, pouze znaky:

A-Z, 0-9, $, @, #, _ a hesla nejsou citlivá na velikost znaků.

Hodnoty 2 a 3 podporují délku hesla až 128 znaků, libovolné znaky a hesla jsou citlivá na velikost znaků.

- **QPWDEXPITV (Interval vypršení platnosti hesla)**

Doba expirace hesla. Doporučná hodnota je 30 dnů.

- **QPWDMINLEN (Minimální délka hesla)**

Minimální počet znaků v hesle. Doporučuje se používat rozmezí 6-8 znaků.

- **QPWDMAXLEN (Maximální délka hesla)**

Maximální počet znaků v hesle. Na systém IBM i je maximální délka hesla 128 znaků.

- **QMAXSIGN (Maximální počet pokusů o přihlášení)**

Maximální počet neplatných pokusů při jejichž překročení je uživatelský profil zablokován. Doporučuje se používat rozmezí 3-5 neplatných pokusů.

[13] http://publib.boulder.ibm.com/infocenter/systems/scope/i5os/index.jsp?topic=/rzarl/rzarlplanpwdchg.htm

- **QPWDRQDDIF (Požadován rozdíl mezi hesly)**

Po kolika změnách lze použít stejné heslo. Doporučuje se rozmezí 10-12.

- **QPWDRQDDGT (Vyžadování číselného znaku v heslech)**

Je-li v hesle je vyžadován číselný znak. Je doporučeno toto pravidlo aktivovat.

- **QPWDCHGBLK (Blokování změny hesla)**

Systémová hodnota QPWDCHGBLK určuje časové období, během něhož je heslo blokováno před změnou po předchozí úspěšné operaci změny hesla.

Heslo nelze změnit během zadaného počtu hodin po předchozí úspěšné operaci změny hesla. Doporučená hodnota je 24.

- **QPWDRULES (Pravidla pro hesla)**

Systémová hodnota QPWDRULES určuje pravidla sloužící ke kontrole správnosti vytvoření hesla. V případě, že není použita hodnota *PWDSYSVAL (jsou akceptovány hodnoty nastavené v QPWD*), můžete do systémové hodnoty QPWDRULES zadat více hodnot, ty jsou rozšiřující a umožňují poměrně detailní nastavení pravidel pro hesla.[14]
QPWDRULES je uvedena od V6R1.

3.1.3 Autorizace objektů

Na každý objekt v systému můžou být nastavena čtyři seskupená oprávnění:

- **ALL** (vše) – povoluje uživateli plný přístup k objektu
- **CHANGE** (změna) – uživatel může měnit obsah objektu
- **USE** (použití) – uživatel má pouze právo ke čtení
- **EXCLUDE** (vyloučení) – uživatel nemá přístup k objektu

[14] http://publib.boulder.ibm.com/infocenter/systems/scope/i5os/index.jsp?topic=/rzarl/rzarlaudcon.htm

Tabulka 7 - Oprávnění definovaná systémem (detailní popis)

	Autorita *USE	Autorita *CHANGE	Autorita *ALL	Autorita *EXCLUDE
Povolené operace pro soubory	Zobrazení informací v souboru.	Zobrazení, změna a smazání záznamu v souboru.	Vytvoření smazání souboru. Přidání, změna a smazání záznamu v souboru. Nastavení oprávnění na soubor pro ostatní uživatele.	Žádné.
Zakázané operace pro soubory	Změna nebo smazání jakékoliv informace v souboru. Smazání souboru.	Smazání nebo vyčištění (clear) celého souboru.	Žádné.	Jakýkoliv přístup do souboru.
Povolené operace pro programy	Spuštění programu.	Změna popisu programu.	Vytvoření, změna a smazání programu. Nastavení oprávnění na program pro ostatní uživatele.	Žádné.
Zakázané operace pro programy	Změna nebo smazání programu.	Změna nebo smazání programu.	Změna vlastníka programu, pokud program používá adoptované autority.	Jakýkoliv přístup na program.
Povolené operace na knihovny	Pro objekty v knihovně podle nastavení oprávnění ke konkrétním objektům. Pro knihovnu - zobrazení popisných informací.	Pro objekty v knihovně podle nastavení oprávnění ke konkrétním objektům. Přidání nových objektů do knihovny. Změna popisu knihovny.	Jakákoliv změna. Smazání knihovny. Nastavení oprávnění na knihovnu pro ostatní uživatele.	Žádné.
Zakázané operace pro knihovny	Přidání nového objektu do knihovny. Změna popisu knihovny. Smazání knihovny.	Smazání knihovny.	Žádné.	Jakýkoliv přístup do knihovny.

Zdroj: http://publib.boulder.ibm.com/infocenter/systems/scope/i5os/index.jsp?topic=/rzamv/rzamvsystemdefauth.htm

3.1.4 Auditní záznamy

Systém při své činnosti zaznamenává do systémového auditního žurnálu události. U každé události je zaznamenáno množství informací, časem počínaje a vzdálenou IP adresou konče.

Každá událost má svůj **kód žurnálu (Journal code)** a **typ záznamů žurnálu (Journal entry types)**:

- Seznam kódů žurnálu (Journal code) - je obecné určení, o jakou skupinu události se jedná. Seznam a popis těchto kódu obsahuje Tabulka 8.

Tabulka 8 - Kódy žurnálu

Žurnálový kód	Popis	Description	Poznámka
A	Systémový účtovací záznam	System Accounting Entry	
B	Integrovaný souborový systém	Integrated File System	
C	Operace s Commitment Control	Commitment Control Operation	
D	Operace s databázovými soubory	Database File Operation	Objekty typu *FILE PF-DTA

E	Operace s datovými oblastmi	Data Area Operation	Objekty typu *DTAARA
F	Databázové operace s členy souborů	Database File Member Operation	
I	Interní systémové operace	Internal Operation	
J	Operace s žurnály nebo přijímačem žurnálu	Journal or Receiver Operation	Objekty typu *JRN nebo *JRNRCV
L	Správa licencí	License Management	Jedná se o licenční vyjímky – neplatný licenční klíc, změna počtu licencí a překročení počtu licencí
M	Správa síťových dat	Network Management Data	Jedná se o QoS, SNMP, IP rules, IP NAT a VPN
P	Záznamy o řízení výkonu	Performance Tuning Entry	
Q	Operace s datovými frontami	Data Queue Operation	Objekty typu *DTAQ
R	Operace se záznamy	Operation on Specific Record	
S	Poštovní služby	Distributed Mail Services	
T	Auditní záznamy	Audit Trail Entry	
U	Uživatelem generované záznamy	User-Generated Entry	Záznamy s tímtu kódem můžou být zaznamenány pomocí příkazu Send Journal Entry (SNDJRNE)
Y	Záznamy o knihovnách	Library Entry	Obsahuje informace o veškerých změnách na knihovny (*LIB)

Zdroj: http://publib.boulder.ibm.com/infocenter/systems/scope/i5os/index.jsp?topic=/rzaki/rzakicodes.htm

- Typ záznamu žurnálu (Journal entry type) - na základě kódu žurnálu blíže specifikuje konkrétní záznam. Pokud nastane událost typu auditní záznam (typ T) a jedná se například a nepovolený přístup k objektu (selhání oprávnění) pak je typ záznamu žurnálu T-AF (Authority Failure). Příloha č. 2 obsahuje seznam typů záznamu žurnálu.

Při monitorování nebo dohledávání konkrétních událostí je potřeba kód žurnálu (Journal code) a záznamů žurnálu (Journal entry type) znát. Způsob analýzy auditních záznamů je popsán v kapitole 3.2.1 Systémový auditní žurnál (QAUDJRN).

Výše uvedené kód žurnálu (Journal code) a typ záznamu žurnálu (Journal entry type) se používají pro dohledávání auditních informací, případně monitorování stanovených událostí.

Význam kódů žurnálu a typů žurnálových záznamů je možné najít v on-line vyhledávači. [15]

[15] http://publib.boulder.ibm.com/infocenter/systems/scope/i5os/index.jsp?topic=/rzaru/rzarufinder.htm

3.2 Systémové logy

V systému IBM i je velké množství různých logů, v této kapitole jsou uvedeny logy, mající souvislost s bezpečností.

3.2.1 Systémový auditní žurnál (QAUDJRN)

Systémový auditní žurnál (QAUDJRN) slouží pro zaznamenávání, monitorování a případné pozdější dohledání událostí. Systémový audit se nastavuje pomocí systémových hodnot, ve kterých se určuje jaké události se budou zaznamenávat – jedná se o systémové hodnoty QAUDCTL a QAUDLVL.

Výpis ze systémové auditního žurnálu lze provést dvěma způsoby:

- **DSPAUDJRNE**

Umožňuje vygenerovat bezpečnostní žurnál audit report (do tiskového výstupu nebo na obrazovku), tento příkaz však už není rozšiřován a nepodporuje všechny typy auditních záznamů, ale je dobré se o něm zmínit.

- **DSPJRN**

Umožňuje zkonvertovat záznamy z libovolného žurnálu do fyzického souboru, tiskového výstupu nebo přímo na obrazovku, je to hlavní příkaz pro zobrazení záznamů v žurnálech, jak pro systémový audit, tak pro tabulky. Příloha č. 7 uvádí příklad použití příkazu DSPJRN pro získání auditních záznamů pro objekty, na než byl uživateli odmítnut přístup (T-AF) a tento výstup je proveden do fyzického souboru a je možné jeho další zpracování, např. pomocí SQL.

3.2.2 Historický log (QHST)

Historický log (History log) poskytuje informace o aktivitách prováděných na systému. Tento log obsahuje zprávy o následujících událostech:

- Nedostatečné oprávnění
- Změna stavu zařízení (*DEVD)
- Komunikační chyby
- Kopie zpráv z fronty QSYSOPR
- Informace o databázi
- Oznámení o HW chybách
- Informace o IPL a instalacích
- Informace na úrovni úloh

- Informace o PTF
- Informace o subsystémech
- Informace na systémové úrovni

Historický log lze zobrazit příkazem DSPLOG (viz Příloha č. 9), lze v něm vyplnit časové období, typ výstupu (na obrazovku, tiskový), logy pro konkrétní úlohu a konkrétní ID zprávy.
Při zobrazení logu na obrazovce, lze klávesou F1 zobrazit detail zprávy, u tiskového výstupu lze stanovit detail výpisu.
Historický log obsahuje důležité informace pro pozdější dohledání, a proto je nezbytné provádět jeho archivaci. Archivovat je vhodné jen uzavřené logy, jejich velikost je možné nastavit systémovou hodnotou QHSTLOGSIZ.
Log QHST je uložen v knihovně QSYS jako soubor QHSTyyddda (*FILE PF-DTA),
kde:

yy: dvě poslední čísla z roku
ddd: datum vytvoření logu v Juliánském formátu
a: alfanumerická koncovka, je-li ddd stejné

Systémové logy a systémové žurnály jsou po určité době automaticky mazány, to lze ovlivnit nastavením v „System Cleanup Option “ (GO CLEANUP, volba 1. Change cleanup options). Jedná se o volbu „System journals and system logs“, lze nastavit hodnotu 1 až 366 dní nebo automatické mazání vypnout (hodnota *KEEP).[16]

3.2.3 Systémové zprávy (QSYSMSG)

Do této fronty jsou zasílány kritické systémové zprávy a zprávy, které mají vztah k zabezpečení (např. zablokování uživatelského profilu). Tato fronta na systému standardně neexistuje, je volitelná, duplikující auditní záznamy, její výhodou je však snadné zobrazení a denně je do ní posláno jen omezené množství zpráv. Pokud jí chceme používat lze jí vytvořit pomocí příkazu:
CRTMSGQ QSYS/QSYSMSG TEXT(‘Optional message queue to receive specific system messages’)
a po vytvoření je potřeba na ní nastavit adekvátní přístupová práva[17].

[16] i5/OS Diagnostic Tools for System Administrators, SG24-8253-01 (s. 91-103)
[17] i5/OS Diagnostic Tools for System Administrators, SG24-8253-01 (s. 57)

3.2.4 Zprávy systémového operátora (QSYSOPR)

Do fronty systémového operátora QSYSOPR jsou odesílány systémové zprávy a zprávy generované aplikací (parametr u příkazů pro posílání zpráv *SYSOPR).
Zprávy systémového operátora lze zobrazit příkazem DSPMSG QSYSOPR nebo použitím funkce System Request a volbou 6, v tomto případě není potřeba vstupovat na příkazový řádek a opouštět otevřené obrazovky.

3.2.5 Synchronizace času

Z důvodů dohledávání v logu přes více systémů je doporučeno provádět synchronizaci času pro všechny systémy pomocí časového serveru. Časový server musí být synchronizován z důvěryhodného časového etalonu. V systému IBM i je čas synchronizován pomocí SNTP.
Pro manipulaci s SNTP lze použít menu CMDNTP (**GO CMDNTP**), ve kterém jsou všechny používané příkazy a odkazy na další související menu. Parametry SNTP lze zobrazit příkazem **CHGNTPA** (Change SNTP Attributes).

3.2.6 Monitorování událostí

Pro včasné zjištění blížících se problémů na systému je vhodné provádět dohled (monitorování) systému v reálném čase. Monitorování lze rozdělit do dvou částí:

- **Činnost systému**
  Jde o monitorování oblastí, které mají přímý vliv na chod systému - disková kapacita (monitorování zaplnění jednotlivých ASP), velikost zátěže CPU a doba odezvy (response time).
- **Bezpečnost systému**
  Při monitorování bezpečnosti lze sledovat velké množství událostí, buď systémových, nebo přímo generované aplikací. Příkladem systémových událostí může být, změna systémové hodnoty, zablokované uživatelské profily, každý neplatný přístup na privilegované profily atd.

Monitorování je vhodné provádět aplikací umístěnou mimo sledovaný systém, často umístěný v druhé lokalitě. Tyto aplikace jsou dostupné od třetích stran, jako příklad uvádím produkt VISUAL Message Center[18] (VMC) od Tango/04.

[18] http://www.tango04.com/products/vmc/index.php

3.3 Stanovení pravidel

Pravidla slouží jako základ pro vlastní nastavení systému, je to soubor doporučení a nařízení, jak systém bezpečně nastavit a provozovat.

Pravidla jsou stanovována při implementaci nového systému a vycházejí z pravidel pro stávající systémy, případně je stanovují existující interní předpisy týkající se informačních systémů. Oblasti systému, pro které nejsou ve firmě stanovena pravidla se stanovují na základě doporučení v příslušné odborné literatuře, dokumentaci k systému (aplikaci), případně je doporučí bezpečnostní konzultant. U mezinárodních korporací bývají pravidla doporučována (vyžadována) v rámci celé společnosti.

Pravidla se během implementace nového systému mohou upravovat (podle potřeb aplikace), protože již existující pravidla nemusí pro nový systém (aplikaci) vyhovovat a po předání do produkčního provozu se bez opory v oficiálních dokumentech nesmí měnit.

3.4 Prvotní nastavení systému

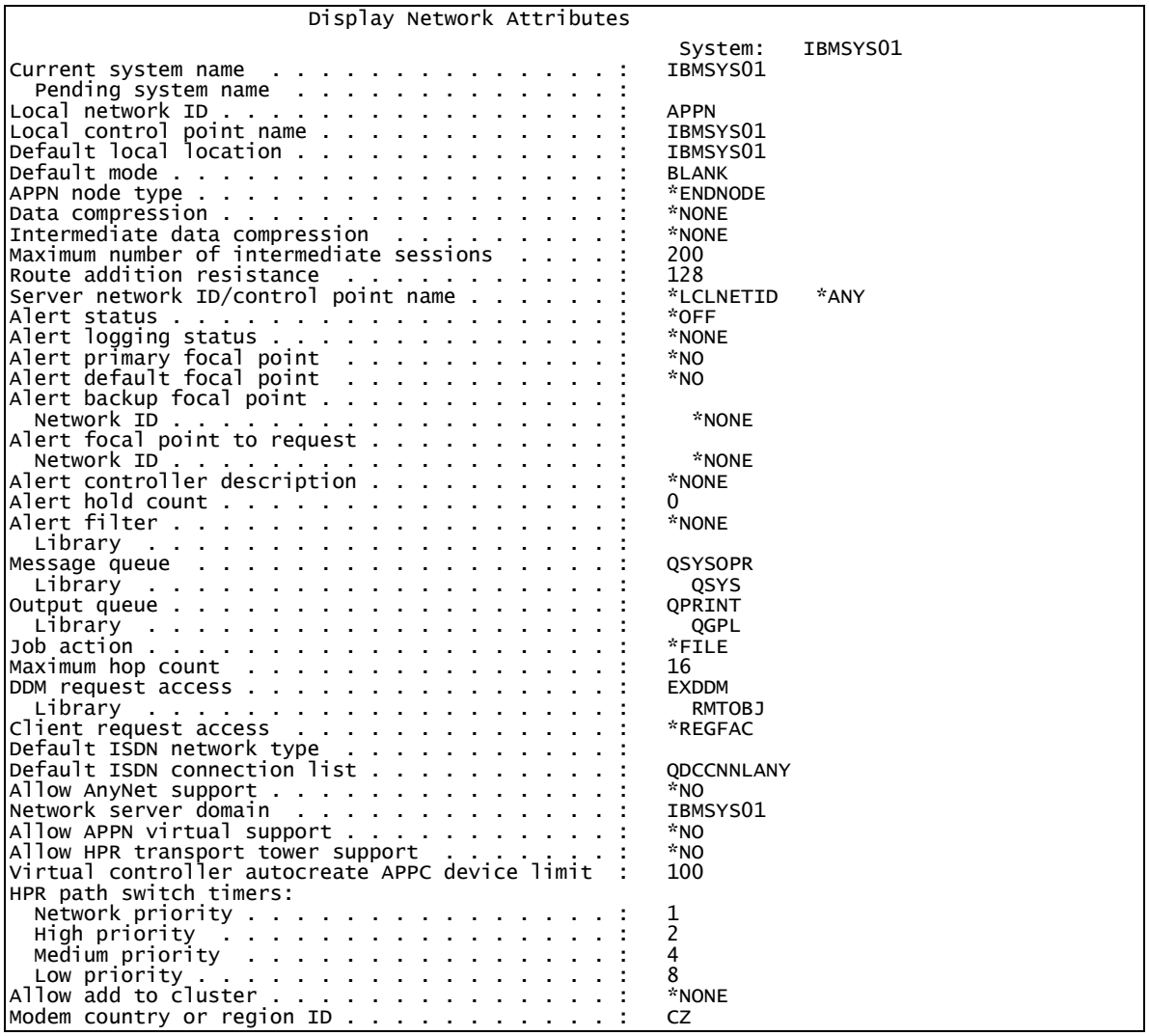
Nový systém je dodáván s defaultním nastavením, které většinou nevyhovuje vyšším standardům pro zabezpečení, a proto je potřeba některé hodnoty upravit.

3.4.1 Nastavení síťových atributů (NETA)

Jedná se o nastavení HW jména systému (defaultně je nastaveno sériové číslo systému) a parametrů pro SNA protokol, který je v současnosti na ústupu, ale bývá často emulován pro starší aplikace. Přes síťové atributy lze aktivovat AnyNet a Enterprise Extender. Pro nové systémy stačí nastavit HW jméno systému.

Pro manipulaci se síťovými atributy se používá příkaz **DSPNETA** pro zobrazení atributů a **CHGNETA** pro změnu příslušného atributu. Při změně některých atributů je třeba provést restart systému (IPL). Viz Obrázek 5.

Obrázek 6 – Příklad konfigurace síťových atributů (DSPNETA



```
                    Display Network Attributes
                                                          System:   IBMSYS01
Current system name  . . . . . . . . . . . . . . :   IBMSYS01
  Pending system name  . . . . . . . . . . . . . :
Local network ID . . . . . . . . . . . . . . . . :   APPN
Local control point name . . . . . . . . . . . . :   IBMSYS01
Default local location . . . . . . . . . . . . . :   IBMSYS01
Default mode . . . . . . . . . . . . . . . . . . :   BLANK
APPN node type . . . . . . . . . . . . . . . . . :   *ENDNODE
Data compression . . . . . . . . . . . . . . . . :   *NONE
Intermediate data compression  . . . . . . . . . :   *NONE
Maximum number of intermediate sessions  . . . . :   200
Route addition resistance  . . . . . . . . . . . :   128
Server network ID/control point name . . . . . . :   *LCLNETID   *ANY
Alert status . . . . . . . . . . . . . . . . . . :   *OFF
Alert logging status . . . . . . . . . . . . . . :   *NONE
Alert primary focal point  . . . . . . . . . . . :   *NO
Alert default focal point  . . . . . . . . . . . :   *NO
Alert backup focal point . . . . . . . . . . . . :
  Network ID . . . . . . . . . . . . . . . . . . :     *NONE
Alert focal point to request . . . . . . . . . . :
  Network ID . . . . . . . . . . . . . . . . . . :     *NONE
Alert controller description . . . . . . . . . . :   *NONE
Alert hold count . . . . . . . . . . . . . . . . :   0
Alert filter . . . . . . . . . . . . . . . . . . :   *NONE
  Library  . . . . . . . . . . . . . . . . . . . :
Message queue  . . . . . . . . . . . . . . . . . :   QSYSOPR
  Library  . . . . . . . . . . . . . . . . . . . :     QSYS
Output queue . . . . . . . . . . . . . . . . . . :   QPRINT
  Library  . . . . . . . . . . . . . . . . . . . :     QGPL
Job action . . . . . . . . . . . . . . . . . . . :   *FILE
Maximum hop count  . . . . . . . . . . . . . . . :   16
DDM request access . . . . . . . . . . . . . . . :   EXDDM
  Library  . . . . . . . . . . . . . . . . . . . :     RMTOBJ
Client request access  . . . . . . . . . . . . . :   *REGFAC
Default ISDN network type  . . . . . . . . . . . :
Default ISDN connection list . . . . . . . . . . :   QDCCNNLANY
Allow AnyNet support . . . . . . . . . . . . . . :   *NO
Network server domain  . . . . . . . . . . . . . :   IBMSYS01
Allow APPN virtual support . . . . . . . . . . . :   *NO
Allow HPR transport tower support  . . . . . . . :   *NO
Virtual controller autocreate APPC device limit  :   100
HPR path switch timers:
  Network priority . . . . . . . . . . . . . . . :   1
  High priority  . . . . . . . . . . . . . . . . :   2
  Medium priority  . . . . . . . . . . . . . . . :   4
  Low priority . . . . . . . . . . . . . . . . . :   8
Allow add to cluster . . . . . . . . . . . . . . :   *NONE
Modem country or region ID . . . . . . . . . . . :   CZ
```

Zdroj: Vlastní

3.4.2 Nastavení systémových hodnot (SYSVAL)

Systémové hodnoty ovlivňují způsob chování systému tj. řízení času, bezpečnost systému, regionální nastavení a další parametry. Systémové hodnoty lze zobrazit příkazem **WRKSYSVAL**. Kompletní seznam, nastavení hodnot a popis obsahuje Příloha č. 4.

3.4.3 Nastavení síťové bezpečnosti

Síťová bezpečnost se sestává ze zabezpečení komunikace pomocí SSL, použití exit pointů (exit programů), vypnutí nepoužívaných služeb a detekce napadení pomocí IDS viz 3.7.3 Intrusion Detection System (IDS).

- **Šifrování komunikace**

  Veškeré síťové služby na sytému IBM i podporují šifrování spojení pomocí SSL. U každé služby je možné nastavit parametr, má-li se startovat jen SSL, bez SSL nebo obě varianty. Ke každé službě, která má používat SSL je nutné přidělit serverový certifikát. Vygenerovat certifikát a přidělit ho konkrétní službě lze udělat pomocí DCM[19] (Digital Certificate Manager). V DCM je možné vygenerovat a spravovat certifikační autoritu (CA).

- **Exit pointy (exit programy)**

  Exit pointy jsou body v komunikačním programu. Pokud dojde k připojení klienta na server, je v určitý moment tento bod aktivován a je-li k němu přiřazen kontrolní tzv. exit program, pak podle seznamu dojde ke kontrole oprávněnosti přístupu na službu. Takto lze omezit přistup pro vyjmenované uživatele.

  Exit pointy lze využít nejen pro síťové servery, ale je pro ně i další použití uvnitř systému (pokud je spuštěn restart systému, je zavolán nějaký exit program). Lze používat i vlastní exit pointy a k nim napsat exit programy.

  Exit programy nejsou součástí vlastního systému, ale lze koupit kompletní řešení od externích dodavatelů. Jako zástupce uvádím produkt NetworkSecurity[20] od PowerTech Group Inc. nebo Bsafe/Enterprise Security[21] od Bsafe Information Systems Ltd.

3.4.4 Role uživatelských profilů

Na systému se provádějí různé činnosti, které lze rozdělit na několik skupin tzv. rolí, u těchto rolí, zejména administrátorských, je třeba dodržovat „princip neslučitelnosti rolí“, tzn. nemá je vykonávat tatáž osoba. Uživatelské role jsou následující[22]:

- **Systémový administrátor** (System administrator)

Jedná se o uživatelský profil s nejvyšším oprávněním v systému (kopie profilu QSECOFR – System Security Office), systémový administrátor má na zodpovědnost komplexní péči o systém (dozor, plánování, zálohování, konfigurace a řešení problémů). Systémový administrátor musí být nepřetržitě k dispozici (pracovní pohotovost).

- **Bezpečnostní auditor** (Security auditor (administrator))

Provádí dohled nad privilegovanými uživateli a kontroluje, jestli nedošlo k nepovolené změně některé z bezpečnostních částí systému.

[19] http://publib.boulder.ibm.com/infocenter/systems/scope/i5os/index.jsp?topic=/rzarl/rzarlpwdrules.htm
[20] http://www.powertech.com/powertech/PowerTech_Web_NetworkSecurity.asp
[21] http://www.bsafesolutions.com/bsafe_enterprise_security.html
[22] *http:/vse.boruvka.cz/01_Prez_200812_VSE_System_IBM_i_Sprava_systemu.ppt*

- **Databázový administrátor** (Database administrator)

Na systému IBM i je díky integrované databázi DB2 většinou totožný se systémovým administrátorem.

- **Aplikační administrátor**

Je zodpovědný za aplikaci, má přehled o její funkčnosti a aplikačních vazbách.

- **Administrátor uživatelských účtů** (User account administrator)

Provádí správu uživatelských profilů - jejich zakládání podle předdefinovaných šablon, jejich blokování, změnu hesel, vytváří seznam nepoužívaných uživatelských účtů k vymazání (rekonciliace).

- **Aplikační podpora**

Jedná se o zkušené zaměstnance dodavatele, kteří řeší aplikační chyby, které během provozování aplikace nastanou. Aplikační podpora musí být zajištěna i mimo pracovní dobu (pracovní pohotovost).

- **Technické účty**

Jsou speciální účty určené pro konkrétní aplikaci. Za tyto technické účty zodpovídá jejich vlastník. Technické účty se dělí na:

  - **Aktivní** – Status *Enabled, heslo nastaveno, neexpirující:
    Jedné se o přístupy z aplikačních serverů. Tyto profily mají přesně nadefinovaný přístup do systému, mnohdy jen k několik tabulkám, které potřebují ke své činnosti.
  - **Pasivní** – Status *Disabled, heslo *NONE:
    Jedná se o uživatelské profily, používané jen v rámci systému pro běh podpůrných částí systému nebo aplikací. Zejména jsou používány pro spouštění dávkových úloh.
  - **Bezpečnostní** – Status *Disabled, heslo *NONE:
    Jedná se o uživatelské profily, které se používají jako skupinové profily (group profile) nebo jako vlastníci objektů (object owners).

- **Systémové profily**

Jsou profily dodávané se systémem. Pokud není v dokumentaci uvedeno jinak, není doporučeno měnit jejich nastavení. Seznam systémových profilů obsahuje Příloha č. 3.

- **Operátor provozu**

Je to osoba, která spouští úlohy podle harmonogramu, provádí dozor a v případě problému kontaktuje osoby mající pracovní pohotovost.

- **Běžní uživatelé**

Jsou standardní uživatelé aplikace bez speciálních oprávnění, kteří mohou pracovat pouze v aplikaci a do systémového řádku nemají vůbec přístup. Pro běžné uživatele jsou vytvořené aplikační role (účetní, personalista, přepážkový pracovník, atd.). Aplikační role určují autorizaci uživatele do aplikace.

3.5 Nastavení oprávnění pro uživatelské knihovny

Uživatelské knihovny jsou nesystémové knihovny (*ALLUSR), v podstatě se jedná o programové a datové knihovny, které se používají pro jednotlivé aplikace.
Do systému IBM i je integrována databáze DB2 (více v 1.4 Databáze), všechny databáze jsou na stejné úrovni jako systémové knihovny (do systému se žádná další databáze neinstaluje) a pro přístup do této databáze se používají standardní uživatelské profily (*USRPRF), které se používají pro přihlášení do aplikace na systému umístěné. Pokud se jedná o aplikaci provozovanou přes textové rozhraní (emulace 5250) je třeba na programové a datové objekty potřeba nastavit příslušné oprávnění. Pro tyto aplikace zajišťuje autentizaci systém a pro autorizaci se používá bezpečnostní modul aplikace.

3.5.1 Programové knihovny

V programových knihovnách jsou umístěny programy pro vlastní uživatelskou funkčnost, programy pro dávkové zpracování a obrazovky používané uživateli. Na tyto objekty stačí běžným uživatelům přístup *USE.

3.5.2 Datové knihovny

V datových knihovnách jsou umístěna data vlastní aplikace (tabulky, datové oblasti, datové fronty, žurnály). Na tyto objekty potřebují běžní uživatelé přístup *CHANGE.

3.5.3 Žurnálové knihovny

Pro zajištění integrity dat, replikace dat a zpětného dohledání se používá logování databáze tzv. žurnálování. V datové knihovně jsou umístěny žurnály (*JRN), které odkazují na konkrétní žurnálové přijímače (*JRNRCV), ve kterých jsou žurnálovaná data umístěna.
Žurnálové přijímače je doporučeno umístit do jiné diskové oblasti, než je umístěna databáze a to ze dvou důvodů:

- Rozložení diskových operací (zápis probíhá na rozdílné disky).
- V případě úplného zničení diskové oblasti, na níž se databáze nachází je možné data pomocí poslední zálohy databáze a aplikace žurnálových změn zcela obnovit.

3.5.4 Bezpečnostní modul aplikace

Bezpečnostní modul zajišťuje autorizaci uživatelů přistupujících do aplikace, pro menší aplikace může být obsahem programových a datových knihoven. Tento modul je kritický z hlediska přímé modifikace pomocí databázové manipulace (např. SQL), a proto je vhodné citlivé pole šifrovat a nežádoucí modifikace eliminovat.

3.5.5 Integrovaný souborový systém (IFS)

IFS je aplikací využíváno pro generování výstupů v klasickém souborovém formátu, import nebo export dat mezi externími systémy. Při návrhu zabezpečení je třeba pamatovat i na tuto část, zejména bude-li umožněn přístup přes službu NetServer.

3.6 Revize nastavení systému a přidělených oprávnění

Po počátečním nastavení systému se většinou neprovádějí revize je-li nastavení systému v původním stavu a nedošlo tak k neschváleným změnám. Revize je třeba provádět i u uživatelských profilů, mají-li příslušná nastavení a nedošlo k neschválenému zvýšení oprávnění uživatelského profilů. Při vytváření nových uživatelských profilů je nezbytné zajistit, aby profily nedostávaly defaultní hesla (tj. stejná jako uživatelský profil) a aby byla generována rozdílná počáteční hesla. Defaultní hesla je třeba hlídat i pro systémové profily, jejich názvy lze nalézt v dokumentaci k systému a jsou-li defaultní je jen otázkou času kdy dojde k jejich zneužití (více v kapitole 3.7.1 Pokus o odhalení hesla).

Další oblastí revize jsou nepoužívané uživatelské profily, jak zaměstnanců, kteří odešli, tak zaměstnanců, kteří uživatelské profily dlouhodobě nepoužívají. Systém umožňuje automatické blokování uživatelů, kteří byly určitou dobu neaktivní (příkaz ANZPRFACT), profily které není žádoucí automaticky blokovat lze přidat do výjimek (příkazy DSPACTPRFL a CHGACTPRFL).

Na systému IBM i jsou veškeré příkazy umožňující bezpečnostní analýzy sdruženy do bezpečnostních nástrojů (Security Tools). Menu bezpečnostních nástrojů lze pustit pomocí **GO SECTOOLS**[23].

[23] i5/OS Diagnostic Tools for System Administrators, SG24-8253-01 (s. 135)

3.7 Prevence a detekce nekalých aktivit

Nedílnou součástí zabezpečení systému je detekce nekalých aktivit, to se týká zejména pokusu o odhadnutí hesla, pokusu o převzetí vyšších oprávnění a ochranu před dalšími útoky (zjišťování aktivních portů, DoS).

3.7.1 Pokus o odhalení hesla

Většinou se jedná o pokusy na známé uživatelské profily (QSECOFR, QSYSOPR, QUSER, QSYS, atd.) nebo na nějakým způsobem (pochybným) získaný seznam uživatelských profilů není-li u nějakého profilu použito defaultní heslo.

Pro nově vytvářené uživatelské profily je potřeba vždy generovat jiné unikátní počáteční heslo. Pokud se používají pro nové všechny profily stejné hesla, může snadno dojít ke zneužití a profil použije (zneužije) někdo jiný.

V tomto případě je třeba provádět alespoň detekci neplatných pokusů na systémové a privilegované uživatelské profily. Tyto aktivity jsou zaznamenávány do systémového auditního žurnálu QSYS/QAUDJRN.

Uživatelské profily s defaultním heslem lze vypsat pomocí příkazu **ANZDFTPWD** (Analyze Default Passwords), tímto příkazem je možné též provést expiraci hesel nebo tyto uživatelské profily zablokovat.[24]

3.7.2 Pokus o převzetí vyššího oprávnění

Prevencí této nekalé aktivity je nastavení adekvátního oprávnění na programy umožňují spuštění pod adoptovanou autoritou.

Každý program na systému IBM i umožňuje takové nastavení, aby mohl být zavolán s oprávněním vlastníka, pokud na tento program má volající uživatel oprávnění.

Pokud je volán program, který vlastní profil, mající speciální oprávnění *SECADM a *ALLOBJ a z toho programu je volán příkazový řádek, tak volající uživatel dostane příkazový řádek s plným oprávněním k systému. Z tohoto důvodu je třeba k takovýmto programům omezovat přístup nastavením veřejné autority na *EXCLUDE a hlídat nastavení privátních autorit.

Systém umožňuje vypsání programů používajících adoptované autority pomocí příkazu **DSPPGMADP**[25] (Display Program Adopt) případně **PRTADPOBJ**[26] (Print Adopting Objects). Ukázku obrazovky tohoto příkazu obsahuje Příloha č. 9

[24] http://publib.boulder.ibm.com/infocenter/systems/scope/i5os/index.jsp?topic=/cl/anzdftpwd.htm

Nastavení programu lze zobrazit pomocí příkazu **DSPPGM**[27], kde nás budou zajímat parametry:

- **Owner** (vlastník) – uživatelský profil pod nímž bude program spuštěn.
- **User profile** – může nabývat hodnot *USER (je spuštěn po uživatelem, který program volá) nebo *OWNER (je spuštěn po vlastníkem programu).
- **Use adopted authority** - může nabývat hodnot *YES nebo *NO.

3.7.3 Intrusion Detection System (IDS)

Od V5R4 byla do systému implementována funkčnost IDS, nastavení nebylo úplně jednoduché, protože konfigurace se prováděla editací textového souboru. Od V6R1 je IDS možné konfigurovat pomocí grafického rozhraní.

3.7.4 Změna úvodních zpráv

Pokud se uživatel přihlašuje do emulace 5250, tak pokud zadá neexistující profil, je napsáno, že tento profil neexistuje, když zadá neplatné heslo, je mu oznámeno, že zadal neplatné heslo. Tyto zprávy mohou být vodítkem, jaký uživatelský profil na systému existuje. Je proto doporučeno tyto zprávy upravit, aby jejich vypovídací hodnota byla omezená, avšak bylo sděleno, že je něco špatně.

3.7.5 Mazání nepoužívaných uživatelských profilů

Jako prevenci zneužití nepoužívaných účtů je vhodné uživatelské profily odešlých zaměstnanců pravidelně měsíčně mazat (reconciliace). Je možné je jen zablokovat, ale jejich úplné smazání ze systému je jistější a na systému se nehromadí uživatelské účty.

3.8 Prevence výpadku systému

K výpadku může dojít z mnoha příčin, od přetečení diskového prostoru (ASP), přes chybu obsluhy, až po hrubou chybu programu. V kapitole 2. Fyzická bezpečnost systému IBM i je pojednáno, co je třeba zajistit pro prevenci výpadku silové sítě, datové sítě, přehřátí systému a dalších příčin výpadků.

[25] http://publib.boulder.ibm.com/infocenter/systems/scope/i5os/index.jsp?topic=/cl/dsppgmadp.htm
[26] http://publib.boulder.ibm.com/infocenter/systems/scope/i5os/index.jsp?topic=/cl/prtadpobj.htm
[27] http://publib.boulder.ibm.com/infocenter/systems/scope/i5os/index.jsp?topic=/cl/dsppgm.htm

3.8.1 Přetečení diskového prostoru

Jedná se o nejčastější příčinu výpadku systému. Prevencí tohoto problému je monitorování zaplnění diskového prostoru pomocí externí aplikace, která při překročení určité prahové hodnoty vyhlásí poplach (zaslání kritické události do monitoringu se současným zasláním emailu či SMS zprávy osobě mající pracovní pohotovost).

Systém umožňuje nastavení prahů zaplnění diskového prostoru, jedná se o dva prahy, první provede pouze oznámení o přetečení první úrovně, druhý provede jednu z následujících akcí:

- Zašle zprávu do fronty systémového operátora (QSYSOPR)
- Zašle zprávu servisním uživatelům
- Uvede systém do restrikce
- Systém vypne nebo provede restart
- Provede se úloha na základě volání ukončovacích programů[28]

Dalším preventivním opatřením je držení určité hodnoty volného prostoru, která se odvíjí od celkové velikost diskového prostoru systému a tudíž je při rychlém nárůstu časová rezerva k nalezení příčiny.

Z důvodu rychlého vyčištění diskového prostoru, je třeba mít připraven seznam objektů, které je možno okamžitě vymazat. Tento seznam by všechny odpovědné osoby (systémoví administrátoři) měly znát nazpaměť, protože pokud tato situace nastane, není čas prohledávat dokumentaci, na rozhodnutí co smazat bývá mnohdy pár desítek sekund, které dělí systém od tvrdého pádu.

Častou příčinou této chyby je špatně nadefinovaný databázový dotaz, který začne vytvářet extrémně velkou výstupní tabulku, případně alokuje dočasnou diskovou paměť (current unprotected) zjistitelnou pomocí příkazu WRKSYSSTS. Další příčinou může být masivní vytváření tzv. tiskových dump spoolů, při nějaké programové chybě, která se opakuje v cyklu.

3.8.2 Hardwarový problém

V současné době je pro Power Systems zajištěna kompletní HW redundance a to i včetně procesorů a operační paměti. Důležité je provést výměnu vadného dílu v adekvátním času, neboť se vzrůstající dobou, po kterou není vadný díl vyměněn, roste riziko výpadku celého systému, což může mít, jde-li o chybu procesoru, paměti nebo servisního procesoru (FSP)

[28] http://publib.boulder.ibm.com/infocenter/systems/scope/i5os/index.jsp?topic=/rzakz/rzakzqstglowacn.htm

důsledek na všechny logické oblasti (LPAR) na systému provozované. Ostatní díly, jako disky a karty mají dopad pouze na systém, na kterém se chyba vyskytla.
Při výměně dílů mající dopad na funkčnost všech logických oblastí (procesor, operační paměť a servisní procesor) je potřeba po dobu výměny celý HW vypnout a odpojit od silového napájení.

3.8.3 Chyba obsluhy

Jedná se zejména o chybu privilegovaného uživatele, hlavně správce systému, který může omylem spustit příkaz pro vypnutí systému (PWRDWNSYS), uvedení systému do restriktovaného stavu (ENDSYS) a příkazy pro ukončení TCP/IP komunikace (ENDTCP, ENDTCPSVR), omylem ukončí důležitou úlohu nebo subsystém, případně udělá chybu v konfiguraci s dopadem na stabilitu systému.
Dále se může jednat o pochybení systémového operátora, které omylem spustí jinou operaci nebo nenahlásí problém systémovému administrátorovi držícímu pracovní pohotovost a následkem toho dojde k výpadku systému.
Je potřeba dát pozor při použití funkční klávesy F9 (listování použitých příkazů), aby privilegovaný uživatel v rychlosti nestisknul klávesu Enter a potencionálně rizikový příkaz (který předtím napsal na příkazový řádek, avšak nepotvrdil) se neprovedl. Pokud je takový příkaz vůbec na řádek napsán, je potřeba se odhlásit a neriskovat.

3.8.4 Hrubá chyba programu

Úlohy (běžící programy) na systému IBM i jsou od sebe izolované, tudíž nemohou přímo zapříčinit pád celého systému. Mezi nejčastější chyby patří:

- Při nastalé chybě dochází k vytváření velkého počtu dump tiskových spoolů nebo vytváření extrémně velké tabulky (viz 3.8.1 Přetečení diskového prostoru).
- Úloha při chybě začne spotřebovávat velké množství strojového času systému (to lze vyřešit snížením priorit úloh na minimum) a pak úlohu ukončit.
- Může se stát, že úlohu nelze standardně ukončit (ENDJOB), pak lze po uplynutí 10 minut od standardního ukončení úlohu ukončit abnormálně (ENDJOBABN). Pokud ani toto nepomůže, je možné počkat do konce provozní doby systému a pak provést restartování systému, jedná-li se však o kritickou úlohu, bez níž nemá provozování aplikace smysl je třeba provést restart systému okamžitě. Pro tyto nestandardní situace je třeba mít připravené provozní postupy (kdo rozhodne, koho informovat a co dělat).

Hrubá chyba programu může nastat z mnoha příčin:

- Často to bývá vstup nekorektních dat.
- Vnitřní zacyklení programu - program pracuje rutině korektně, ale je zavolán běžně nepoužívaný cyklus, ve kterém je chyba.

3.9 Aplikace programových fixů (PTF)

Nezbytnou součástí zabezpečení systémů je pravidelná aplikace programových fixů (PTF). Veškeré fixy je nutné před aplikací do produkčního prostředí ověřit v prostředí testovacím. Nové fixy je nutné aplikovat jako dočasné (temporary), všechny ověřené fixy, které jsou už delší dobu naaplikovány je vhodné před aplikací nových fixů naaplikovat jako trvalé (permanent). V případě problémů je možné dočasné fixy vyjmout.

3.9.1 Rozdělení PTF

PTF jsou pro sdružovány do sad, tím se zjednodušuje aplikace a fixy není potřeba získávat po jednom. Sady PTF se dále dělí na:

- **Cumulative PTF**

  Tato sada oprav je vydávána jednou za tři měsíce a obsahuje všechny důležité opravy za předešlé období.
- **HIPER PTF** (High impact or pervasive)

  Tyto PTF vycházejí týdně a obsahují souhrn nejdůležitějších PTF, které byly během týdne uvolněny.
- **Skupinové PTF** (Group PTF)

  Jde o fixy, které shrnují PTF pro konkrétní licenční program (např. 5761DG1) nebo část systému (databáze, bezpečnost, tisk). Skupinové PTF mají pořadové číslo tzv. úroveň (level).
- **Individuální PTF** (Individual PTF)

  Každý výše uvedený balíček, je složen ze samostatných fixů (PTF) a pokud je potřeba může být aplikován pouze jeden potřebný fix, při zachování určitých podmínek uvedených v popisu fixů tzv. PTF Cover Letters[29].

  PTF mohou být ve výše uvedených sadách obsaženy opakovaně. Aktuální informace o nových sadách oprav lze najít v Preventive Service Planning - PSP[30].

[29] http://www-912.ibm.com/a_dir/as4ptf.nsf/as4ptfhome
[30] http://www-912.ibm.com/s_dir/sline003.nsf/sline003hom

Většinu PTF je možné aplikovat bez restartu systému nebo je třeba pouze ukončit některé služby a ty po naaplikování zase hned nastartovat, tímto se minimalizuje výpadek systému.

V systému lze informace o jednotlivých PTF zobrazit příkazem DSPPTF, informace o sadách PTF lze zobrazit pomocí WRKPTFGRP. Všechny příkazy související s fixy lze získat pomocí příkazu GO PTF.

3.9.2 Doporučení pro aplikaci PTF

Důvod k aplikaci PTF je několik:

- Preventivní opatření: jsou aplikovány všechny sady fixů současně, frekvenci pro aplikaci všech sad PTF nelze jednoznačně stanovit, vždy záleží na použití konkrétního systému. Pro systémy s vysokou dostupností je aplikace doporučována jednou, maximálně dvakrát ročně a to během, dopředu plánovaného restartu (u těchto systému se restart provádí zhruba jednou až dvakrát do roka).
- Nastane akutní problém: ten je řešen konkrétním fixem. Po zhodnocení rizik, je možné tento fix aplikovat okamžitě.
- Mimořádná aplikace PTF: je třeba ji provést, pokud je vydána mimořádně kritická oprava, to se však nestává příliš často.

PTF lze získat na CD/DVD objednáním u lokální podpory IBM za manipulační poplatek, toto je však časově náročnější. Druhou možností je stažení PTF elektronickou cestou (Fix Central[31]), to lze provést prostřednictvím IBM ID. Obě služby jsou dostupné pokud si zákazník platí potřebné služby.
Elektronickou cestou lze PTF stáhnout během několika minut (záleží na velikosti) jako ISO image a pak pomocí image katalogu „Image Catalog“ připravit k aplikaci přes virtuální CD/DVD disk. S image katalogem lze pracovat příkazem WRKIMGCLG.

3.10 Všeobecná prevence

Základem všeobecné prevence je zvyšování povědomí mezi uživateli o zodpovědném přístupu k informační bezpečnosti, mezi hlavní body patří:

[31] http://www-933.ibm.com/support/fixcentral/

- Nesdělování citlivých informací (uživatelské profily, IP adresy, informace o aplikaci). Uživatelé musí být obezřetní, pokud po nich někdo požaduje různé informace, aniž sami předtím kontaktovali podporu kvůli nějakému problém.
- Nesdělování hesel - uživatelé musí vědět, že po nich nikdo nikdy nebude požadovat sdělení hesla.
- Zapisování hesel na nevhodná místa (monitory, šuplíky, spodní část klávesnice), uživatelům je vhodné poskytnout aplikaci pro bezpečné uchovávání hesel (např. KeePass Password Safe[32]). Možností je také použití řešení pro jednotné přihlášení uživatelů (SSO), kdy uživateli stačí pro všechny aplikace jeden uživatelský účet a jedno heslo.

Člověk (uživatel) je nejslabším článkem informačních systémů a s tím je třeba počítat. Seznamováním s pravidly a proškolováním uživatelů lze zamezit neúmyslnému úniku citlivých informací. Uživatelé informačních systémů si mnohdy nejsou vědomi ani nejzákladnějších pravidel a často podlehnou sociálnímu inženýrství, to je nutné změnit zvyšováním informační gramotnosti.

3.11 Organizační zajištění

Organizační zajištění se skládá z několika oblastí, jejichž existence je nezbytná pro optimální funkčnost systému.

3.11.1 Helpdesk (uživatelská podpora)

Helpdesk (uživatelská podpora) zajišťuje centrální podporu uživatelů a zabraňuje degradaci odborných pozic na řešitele opakujících se problémů. Pro Helpdesk je vhodné zavést jednotné telefonní číslo.

Helpdesk řeší opakující se problémy a udržuje jejich znalostní databázi (knowledge base).

3.11.2 Reset hesel (změna zapomenutého hesla)

Pro reset hesel je nutné stanovit jasná pravidla, není vhodné, aby ke změně hesla docházelo jen na základě telefonátu (výjimkou může být, pokud osobu dokážeme identifikovat hlasem a telefonním číslem). Pro reset hesel existuje několik způsobů:

- Email: požadavek na reset hesla je zaslán z emailové adresy žadatele, reset by neměl kvůli bezpečnosti provádět Helpdesk, ale administrátor uživatelských účtů nebo

[32] např. KeePass Password Safe, http://keepass.info/, jde o OpenSource správce hesel, dostupný včetně české lokalizace

druhotně systémový administrátor. Helpdesk by měl provádět hesel pouze do základních aplikací (doména windows, email), ale nikdy do kritických aplikací (např. bankovní systém, mzdový systém, apod.).

- Aplikace: uživatel, který zapomněl heslo, požádá zavoláním funkce o zaslání hesla, heslo je mu zasláno do jeho emailové schránky. Je nezbytné provádět křížovou kontrolu, je-li uživatel přihlášený ve Windows totožný s uživatelem aplikace. Tato varianta je použitelná zejména pro webové aplikace.
- Automatický systém: existuje jen jedna celopodniková aplikace pro reset hesel, ve které se velmi často používá propojení s LDAPem Windows domény ve spojení s návodnou otázkou.

3.11.3 Zastupitelnost

Vzájemná zastupitelnost je důležitá pro vlastní stabilitu a funkčnost systémů, je třeba počítat s tím, že správce musí mít dovolenou, může být nemocen atd.
Zastupitelnost není nikdy úplná, je dobré ji dělit podle různých oblastí systému (bezpečnost, komunikace, klientská aplikace, replikace, atd.) a tu si mezi sebou křížově rozdělit. U všech oblastí systému je zcela nezbytné mít aktuální dokumentaci.

3.11.4 Dokumentace

Dokumentace je nezbytnou součástí, která zajistí uchování znalostí a postupů i při nedostupnosti odpovědné osoby. Typy dokumentace můžeme rozdělit na:

- **Technická dokumentace**

Jedná se o dokumentaci při nasazování nové části systému, modulu či složitějším upgrade. V této dokumentaci má být popsáno: proč se to dělá, časový nástin, rámcový postup, podrobný postup a odkaz na použitou dokumentaci (interní, externí).

- **Provozní dokumentace**

Slouží jako návod k obsluze aplikace a bývá, jednak ve formě detailních návodek pro operátory provozu, jednak popisem pro administrátory provozu a může být součástí technické dokumentace.

- **Konfigurační dokumentace**

Jedná se o soupis konfigurace systému a jeho síťová rozhraní. HW konfiguraci lze velmi dobře vyčíst pomocí systémových příkazů (WRKHDWRSC) nebo v systémových nástrojích (STRSST – Start System Tools), takže to není nezbytné. Nutné je

dokumentování síťových vazeb, tj. do jaké zásuvky (patch panel) je síťová karta připojena a do jakého portu síťového zařízení (swich) je provedeno připojení na druhé straně.
Z konfigurační dokumentace lze ve finále velice jednoduše získat podklady pro tisk popisných štítků.
Popisné štítky slouží k označování kabelů, aby se zamezilo případnému omylu a odpojení jiné části systému. Velmi vhodné je také označování počítačových systémů identifikačními štítky (jméno systému, IP adresa, použití, atd.).

- **Plán obnovy a havarijní plán**

Tyto dva plány jsou důležité pro případ nečekaných událostí, určují jak se při nich chovat a jak co nejrychleji obnovit činnost systémů. Zároveň se při přípravě těchto plánů zjistí případné nedostatky a slabá místa. Je důležité tyto plány pravidelně testovat a aktualizovat.

- **Systémový deník**

Do tohoto deníku jsou zaznamenávány veškeré změny a události týkající se systému. Minimálně by měl obsahovat jméno systému, datum změny, popis změny, kdo ji provedl a kdo ji schválil.

3.11.5 Uživatelské role

Role určuje jaká přístupová oprávnění (autorizace) do aplikace budou uživateli přidělena, jedná se o šablony uživatelských profilů a určení přístupu k jednotlivým funkcím (sadě funkcí) v aplikaci. Role eliminují případné dohady, jaká kdo má mít přístupová oprávnění, vše co je nad rámec rolí schvaluje delegovaný vlastník dat.

3.11.6 Vlastník dat

Oddělení IT spravuje vše okolo systémů a aplikací, reálně je však vlastníkem dat obchodní oddělení, které data využívá a je s ním třeba zásadní změny konzultovat. Delegovaní zástupci oddělení, by měli odsouhlasit veškeré přístupy k datům, které nejsou stanoveny v předdefinovaných rolích.

3.12 Shrnutí kapitoly

Tato kapitola poskytuje přehled o zabezpečení systému IBM i a dává vodítko, co je třeba zajistit, jak systémově, tak organizačně, aby byl systém bezpečný.

4 Zálohování, obnova a replikace systému IBM i

Systém může být sebelépe zabezpečen, avšak při chybě obsluhy (privilegovaný uživatel, operátor DC) může dojít ke smazání systémových, případně aplikačních objektů.
Problém může také nastat při poškození objektu, případně nutnosti srovnání starších objektů.
Speciálním případem zálohování je archivace, kdy zálohovaná data z důvodu pozdějšího použití (dohledání chybných transakcí, legislativní důvody) uchováváme po delší časové období.
Po skončení životnosti médií je třeba tyto paměťové nosiče bezpečně zlikvidovat a zamezit případnému úniku citlivých dat. (Likvidací dat se např. zabývá společnost REISSWOLF likvidace dokumentů a dat, s.r.o.[33]) .

4.1 Zálohování a obnova

Zálohování (backup) je pravidelná a soustavná činnost probíhající převážně každodenně, obnova (restore) probíhá na vyžádání a to v mnohem menší míře než zálohování. Zálohování je cyklické, tzn. media se používají opakovaně v určitých cyklech (14 dní, měsíc).
Pro zálohování a obnovu na systému IBM i se používá licenční program Backup Recovery and Media Services (5761-BR1)[34], který umožňuje kompletní správu záloh a médií.

4.1.1 Servisní zálohování

Pod servisním zálohováním si můžeme představit pravidelné denní zálohování systému - konfigurace systému, zabezpečení, ale i programových knihoven. Ze servisních záloh jsou vyjmuty databáze (datové knihovny), které zaujímají převážnou část diskové kapacity systému a jsou zálohovány samostatně viz 4.1.2 „Zálohování databáze“. Jednou týdně probíhá úplně zálohování (zpravidla o víkendu) a denně přírůstkové (zálohují se pouze změněné objekty, ne celé knihovny). Servisní zálohy jsou drženy nejdéle několik týdnů (2-8 týdnů) a poté se média opětovně použijí a nepotřebné zálohy přepíší.

[33] http://www.reisswolf.cz/sluzby/likvidace-dat/
[34] http://publib.boulder.ibm.com/infocenter/systems/scope/i5os/index.jsp?topic=/rzai8/rzai8overview.htm

4.1.2 Zálohování databáze

Zálohování databází (datových knihoven) se zpravidla provádí před zpracováním a po zpracování (vždy se jedná o úplné zálohování) z důvodu uvedení databáze do původního stavu pro případ opětovného spuštění zpracování, z důvodu chyby v programu, kdy se databáze může dostat do nekonzistentního stavu.

4.1.3 Křížové zálohování

Křížové zálohování je nahrávání záloh z produkčního systému na zařízení umístěná na záložní lokalitě, obráceně je to také možné. Křížové zálohování je použitelné, pokud jsou na záložní lokalitu dostatečně propustné přenosové linky.

4.2 Archivace

Archivace je speciální případ zálohování, kdy zálohovaná data jsou uchovávána po delší časové období od 6 měsíců déle. Pro speciální případy se používá trvalá (permanentní) doba uchování (expirace).

Doba archivace je dána, jednak interními předpisy společnosti, jednak legislativně. Při archivaci, je třeba dbát na to, že data na médiích musí být dostupná do doby expirace a počítat s tím při obměně technologie, zda-li dokáže starší média číst a pokud ne, je třeba archivní média přetočit. Lze také držet původní HW pro zálohování, avšak po delší době jsou problémy se servisem a případné servisní poplatky, držení staršího HW prodražují.

Pokud se při zálohování dat používá šifrování médií, je nezbytné počítat s dostupností certifikátů po celou dobu života média.

4.3 Replikace

Replikace je přenos dat v reálném čase z jednoho systému na druhý systém, který je převážně umístěn v jiné lokalitě (DRC).

Replikace se provádí pro případ výpadku primárního (produkčního) systému z důvodu větší poruchy HW nebo jiných příčin o nichž pojednává kapitola 2. „Fyzická bezpečnost systému IBM i“.

Replikace se dělí na dvě části objektovou a databázovou. Objektová replikace je přenos celého objektu, případně jeho parametru (např. pokud u uživatelského profilu dojde ke změně hesla, je přeneseno jen heslo).

Databázová replikace se používá pro replikování datových objektů:

- Tabulek (*FILE PF-DTA)
- Datových oblastí (*DTAARA)
- Datových front (*DTAQ)

Na objekt, který je třeba datově replikovat se musí nastartovat žurnálování do příslušného aplikačního žurnálu. Aplikačních žurnálů bývá několik, dělených podle aplikace, modulu nebo režimu pro žurnálování.

V replikačním SW jsou pak jednotlivé žurnály vidět jako samostatné nezávislé kanály. Na záložním systému se synchronně vytváří aplikační žurnál a změny jsou z něj aplikovány na replikovanou databázi v reálném čase s minimálním zpožděním (zpoždění je závislé na šířce přenosového pásma).

Pokud je pro databázi použité samostatné ASP, lze provádět replikaci na binární úrovni.

Jako příklad aplikace zajišťující vysokou dostupnost lze uvést produkt **MIMIX HA for i5/OS**[35] od společnost Vision Solutions, Inc., který obsahuje nejen modul pro replikaci dat, ale i modul pro přepnutí (switch) systémů.

4.4 Shrnutí kapitoly

Zálohování, obnova, archivace a replikace jsou nedílnou součástí zabezpečení počítačových systémů, do doby než se něco stane to může vypadat jako zbytečné opatření zvyšující náklady, pokud se něco stane jsou výše uvedená opatření neocenitelná.

[35] http://www.visionsolutions.com//Products/High-Availability-MIMIX.aspx

Závěry a doporučení

Pokud nejsou dodržovány základní principy bezpečnosti informačních systémů, a to zejména ze strany uživatelů, tak i ten nejbezpečnější systém, je snadno kompromitovatelný.

Musíme si uvědomit, že v každém systému existuje alespoň jedna bezpečnostní „díra“ a je s tím třeba při návrhu preventivních kontrol počítat.

Největší důraz je třeba klást při zabezpečení systémů připojených přímo do globální počítačové sítě – internetu, z které hrozí největší riziko napadení.

Je důležité si uvědomit, že bezpečnost není cíl, ale cesta ...

Seznam použité literatury

Tištěná literatura

1. **Kolektiv IBM**. Jak začít pracovat s AS/400 2. vyd. Praha : IBM, 1998. SC09-3597-01
2. **SOLTIS G., Frank**. Systém AS/400 zevnitř, 1. vyd. Praha : Computer Press, 1997. s. 147-160. ISBN 80-7226-012-X
3. **ŽUPKA, Vladimír; kolektiv IBM**. Základy AS/400. 1. vyd. Praha : IBM, 1995.

Elektronické zdroje

1. **IBM** : System i – operační systém, [cit. 2009-03-31]
   Dostupný z WWW: <http://www-03.ibm.com/systems/cz/i/software/os/>
2. **IBM i5/OS V6R1** : System's help and a system's menus
3. **IBM i (i5/OS) software**, [cit. 2009-03-31]
   Dostupný z WWW: <http://www-03.ibm.com/systems/i/software/>
4. **IBM Systems Information Center** : IBM i5/OS information, [cit. 2009-03-31]
   Dostupný z WWW:
   <http://publib.boulder.ibm.com/infocenter/systems/scope/i5os/index.jsp>
5. **MUNSON, Randall; System i Network** : They Say It's Your Birthday, [cit. 2009-03-31]. Dostupný z WWW:
   <http://systeminetwork.com/article/they-say-it%E2%80%99s-your-birthday>
6. **POWERS, Susan; MATETIC, Andrei; ROY, Mark;** i5/OS Diagnostic Tools for System Administrators. Second Edition. IBM March 2008, SG24-8253-01 s. 57, 91-103, 135. ISBN 0738486779
   Dostupný z WWW: <http://www.redbooks.ibm.com/abstracts/sg248253.html>
7. **BORŮVKA, Filip.** Přednáška VŠE – IT Management : Správa systémů v praxi pro studenty VŠE, 11.12.2008, [cit. 2009-03-31]
   Dostupný z WWW: <http://www.boruvka.cz/VSE>

Tato práce je elektronicky dostupná na WWW: http://bivs.boruvka.cz/BP

Seznam použitých zkratek a vysvětlení pojmů

Zkratka	Význam	Vysvětlení (význam v překladu)
ASP	Auxiliary Storage Pool	Diskový prostor systému rozdělený na systémové ASP1 a uživatelská od ASP2 výše. Jedná se o na sobě nezávislé diskové prostory (ASP1 je povinné).
CL	Control Language	Příkazový řádek včetně jeho rozšíření (vyšší skriptovací jazyk)
CPF	Control Program Facility	Název operačního systému pro System/38
CPU	Central Processing Unit	Systémový procesor
DB	DataBase	Databáze
DDM	Distributed Data Management	Umožňuje přistupovat na datové soubory mezi systémy, zejména IBM i
DC	Data Center	Datové centrum též počítačový sál
DR	Disaster Recovery	Obnova po katastrofě
DRDA	Distributed Relational Database Architecture	Protokol pro databázovou komunikaci
FSP	Flexible Service Processor	Část systému zajišťující funkčnost dělení na logické části (LPAR) a přidělování zdrojů.
FTP	File Transfer Protocol	Protokol pro přenos souborů
HW	Hardware	Technické vybavení
IBM	International Business Machines	Přední světová společnost v ICT
IDS	Intrusion Detection System	Dokáže detekovat a oznámit pokus o napadení
IFS	Integrated File system	Souborový systém
LDAP	Lightweight Directory Access Protocol	Stále častěji je používán adresářová služba pro internetové i neinternetové aplikace
LPAR	Logical PARtition	Rozdělení HW na více systémů
MAC	Media Access Control	Zajišťuje řízení přístupu k mediu na nižších vrstvách ISO/OSI, obsahuje jedinečnou adresu – MAC adresa
NTP	Network Time Protocol	Protokol pro synchronizaci času
OS	Operating System	Operační systém
OSPF	Open Shortest Path First	Síťový směrovací protokol
PASE	Portable Application Solutions Environment	Umožňuje provozovat UNIX/Linux aplikace na systému IBM i
PTF	Program Temporary Fix	Softwarové fixy systému IBM i
RIP	Routing Information Protocol	Nejstarší protokol pro výměnu směrovacích informací v síti
RPG	Report Program Generator	Programovací jazyk systému IBM i
SMB	Server Message Block	Protokol pro výměnu a sdílení souborů (tiskáren) používaný zejména v Microsoft Windows
SMTP	Simple Mail Transfer Protocol	Slouží pro přenos elektronické pošty
SNA	System Network Architecture	Původní protokol pro komunikaci mezi systémy IBM, dnes je nahrazován TCP/IP protokolem
SNMP	Simple Network Management Protocol	Umožňuje monitorování, řízení a konfigurování vzdálených zařízení
SNTP	Simple Network Time Protocol	Protokol pro synchronizaci času
SSO	Single Sign-On	Uživatel má přístup k více než jednomu systému nebo aplikaci zadáním jediného uživatelského ID a hesla
SQL	Structured Query Language	Umožňuje definovat data, manipulovat s nimi, vytvářet dotazy a řídit přístup k datům
SSL	Secure Sockets Layer	Dokáže zabezpečit síťovou komunikaci
TCP/IP	Transmission Control Protocol/Internet Protocol	Sada síťových protokolů umožňující výměnu informací mezi počítači
UDP	User Datagram Protocol	Slouží k přenášení datagramů v síti bez potvrzování příjmu
UPS	Uninterruptible Power Supply	Zdroj nepřerušitelného napájení

Seznam použitých tabulek, obrázků a příloh

Seznam použitých tabulek:

Seznam použitých obrázků:

Seznam použitých příloh:

Příloha č. 1

Použité systémové příkazy (význam zkratky a stručný popis použití)

Příkaz	Význam	Oblast	Popis
ANZDFTPWD	Analyze Default Passwords	Bezpečnost	Provede analýzu defaultních hesel s možností nastavení vypršení hesla nebo zablokování uživatelského profilu. Výstup příkazu je do tiskového souboru.
ANZPRFACT	Analyze Profile Activity	Bezpečnost	Provede analýzu nepoužívaných profilů a ty uvede do stavu *DISABLED
CFGTCP	Configure TCP/IP	Komunikace	Příkaz zobrazí menu pro konfiguraci TCP/IP.
DSPACTPRFL	Display Active Profile List	Bezpečnost	Zobrazí seznam profilů, které mají výjimku a nejsou blokovány
DSPAUDJRNE	Display Audit Journal Entries	Bezpečnost	Umožňuje vygenerovat bezpečnostní žurnál audit report (do tiskového výstupu nebo na obrazovku)
DSPJRN	Display Journal	Bezpečnost	Umožňuje zkonvertovat záznamy z libovolného žurnálu do fyzického soboru, tiskového výstupu nebo přímo na obrazovku
DSPLOG	Display Log		Příkaz zobrazí informace o aktivitách prováděných na systému.
DSPMSG	Display Messages		Zobrazení zpráv v různých frontách zpráv (*MSGQ)
DSPNETA	Display Network Attributes		Zobrazí nastavení síťových atributů systému
DSPPGMADP	Display Program Adopt	Bezpečnost	Zobrazí seznam objektů, na kterých je adoptivní oprávnění pro konkrétní profil
DSPPTF	Display Program Temporary Fix		Zobrazení programových fixů
ENDJOB	End Job	Řízení činnosti	Provede ukončení zadané úlohy
ENDJOBABN	End Job Abnormal	Řízení činnosti	Není-li úloha ukončena do 10 minut, je možné ji ukončit hrubší metodou
ENDTCP	End TCP/IP	Komunikace	Ukončení TCP/IP pro celý systém
ENDTCPSVR	End TCP/IP Server	Komunikace	Ukončení jednotlivého komunikačního serveru
CHGACTPRFL	Change Active Profile List	Bezpečnost	Nastavení výjimek profilů, které nemají být automaticky blokovány při použití ANZPRFACT
CHGNETA	Change Network Attributes	Konfigurace	Umožní změnit nastavení síťových atributů
CHGNTPA	Change SNTP Attributes	Konfigurace	Změna parametrů NTP protokolu
CHGUSRPRF	Change User Profile	Bezpečnost	Umožní změnit parametry profilu
PRTADPOBJ	Print Adopting Objects	Bezpečnost	Vytvoří seznam objektů majících adoptované oprávnění
PWRDWNSYS	Power Down System	Řízení činnosti	Provede tzv. IPL – vypnutí/restart systému
STRSST	Start System Service Tools	Konfigurace	Umožňuje provádět konfiguraci a analýzy na nižší úrovni
WRKACTJOB	Work with Active Jobs	Řízení činnosti	Umožňuje komplexní práci s aktivními úlohami
WRKAUTL	Work with Authorization Lists	Bezpečnost	Práce s autorizačními listy
WRKHDWRSC	Work with Hardware Resources	Konfigurace	Lze detailně zobrazovat HW konfigurací systému, pracovat s ní lze v SST
WRKIMGCLG	Work with Image Catalogs		Práce se soubory v ISO formátu
WRKPTFGRP	Work with PTF Groups		Práce se sadami PTF
WRKSHRPOOL	Work with Shared Storage Pools	Řízení činnosti	Umožňuje konfigurovat přidělení a nastavení operační paměti pro jednotlivé subsystémy
WRKSYSSTS	Work with System Status	Řízení činnosti	Příkaz zobrazí aktuální stav operační a diskové paměti a spotřebu výkonu
WRKSYSVAL	Work with System Value	Konfigurace	Práce se systémovými hodnotami
WRKUSRPRF	Work with User Profiles	Bezpečnost	Práce s uživatelskými profily

Zdroj: Vlastní

Příloha č. 2

Typy záznamů v žurnálu (QAUDJRN)

Typ záznamu	Popis
AD	Monitorování změn
AF	Selhání oprávnění
AP	Získání adoptovaného oprávnění
AU	Změny atributů
CA	Změny oprávnění
CD	Monitorování příkazových řetězců
CO	Vytvoření objektu
CP	Změna, vytvoření nebo obnova uživatelského profilu
CQ	Změna objektu *CRQD
CU	Operace s klastry
CV	Ověření spojení
CY	Konfigurace šifrování
DI	Adresářový server
DO	Vymazání objektu
DS	Resetování hesla pro zabezpečení DST
EV	Systémové proměnné
GR	Generický záznam
GS	Popis soketů byl předán jiné úloze
IM	Monitor narušení
IP	Komunikace mezi procesy
IR	Akce pravidel IP
IS	Správa zabezpečení Internetu
JD	Změna parametru USER popisu úlohy
JS	Akce ovlivňující úlohy
KF	Soubor klíčového řetězce
LD	Záznam adresáře - vytvoření či odstranění propojení nebo vyhledání
ML	Poštovní akce kancelářských služeb
NA	Změna atributu sítě
ND	Narušení filtru pro vyhledávání v adresáři APPN
NE	Narušení filtru koncových bodů APPN
OM	Přesunutí nebo přejmenování objektu
OR	Obnova objektu
OW	Změna vlastnictví objektů
O1	(Přístup k optickému zařízení) Jediný soubor nebo adresář
O2	(Přístup k optickému zařízení) Dvojí soubor nebo adresář
O3	(Přístup k optickému zařízení) Nosič
PA	Program byl změněn, aby adoptoval oprávnění
PG	Změna primární skupiny objektu
PO	Tiskový výstup
PS	Výměna profilu
PW	Neplatné heslo
RA	Změna oprávnění během obnovy
RJ	Obnovení popisu úlohy se zadaným uživatelským profilem
RO	Změna vlastníka objektu během obnovy
RP	Obnovení programu adoptovaného oprávnění
RQ	Obnovení objektu *CRQD
RU	Obnovení oprávnění uživatelského profilu

RZ	Změna primární skupiny během obnovy
SD	Změny systémového distribučního adresáře
SE	Změna záznamu směrování subsystému
SF	Akce se soubory pro souběžný tisk
SG	Asynchronní signály
SK	Zabezpečená připojení pomocí soketů
SM	Změny správy systému
SO	Akce s uživatelskými informacemi zabezpečení serveru
ST	Použití servisních nástrojů
SV	Změna systémové hodnoty
VA	Změna přístupového seznamu
VC	Spuštění nebo ukončení spojení
VF	Zavření souborů na serveru
VL	Překročení limitu účtu
VN	Síť - přihlášení nebo odhlášení
VO	Akce ověřovacích seznamů
VP	Chyba síťového hesla
VR	Přístup k síťovému prostředku
VS	Spuštění nebo ukončení relace serveru
VU	Změna síťového profilu
VV	Změna stavu služby
X0	Síťová autentizace
X1	Identifikace tokenu
XD	Rozšíření adresářového serveru
YC	Přístup k objektu DLO (změna)
YR	Přístup k objektu DLO (čtení)
ZC	Přístup k objektu (změna)
ZR	Přístup k objektu (čtení)

Zdroj: http://publib.boulder.ibm.com/infocenter/systems/scope/i5os/index.jsp?topic=/rzarl/rzarlf04.htm

Příloha č. 3

Uživatelské profily dodané IBM

Uživatelský profil [1]	Uživatelská třída	Status	Heslo je *NONE	Text [2]	Speciální autorita	Popis [3]
QANZAGENT	*SYSOPR	*ENABLED	*YES	Trace Analyzer Agent Server	*NONE	
QAUTPROF	*USER	*ENABLED	*YES	IBM-supplied User Profile	*NONE	Uživatelský profil oprávnění IBM
QBRMS	*USER	*ENABLED	*YES	IBM-supplied User Profile	*NONE	Uživatelský profil BRM
QCLUMGT	*USER	*DISABLED	*YES	IBM-supplied User Profile	*NONE	Profil správy klastrů
QCLUSTER	*USER	*ENABLED	*YES	IBM-supplied User Profile	*IOSYSCFG	Profil klastru vysoké dostupnosti
QCOLSRV	*USER	*ENABLED	*YES	IBM-supplied User Profile	*NONE	Uživatelský profil služby shromažďování Centrální správy
QDBSHR	*USER	*ENABLED	*YES	Internal Data Base User Profile	*NONE	Profil sdílení databáze
QDBSHRDO	*USER	*ENABLED	*YES	Internal Data Base User Profile	*NONE	Profil sdílení databáze
QDESADM	*USER	*ENABLED	*YES	DB2 TEXT EXTENDER ADMINISTRATOR	*NONE	
QDESUSR	*USER	*ENABLED	*YES	DB2 TEXT EXTENDER USER	*NONE	
QDFTOWN	*USER	*ENABLED	*YES	Default Owner for System Objects	*NONE	Profil předvoleného vlastníka
QDIRSRV	*USER	*ENABLED	*YES	System Directory Services Server User Profile	*NONE	
QDLFM	*USER	*ENABLED	*YES	IBM-supplied User Profile	*NONE	Správce souborů datového spoje
QDOC	*USER	*ENABLED	*YES	Internal Document User Profile	*NONE	
QDSNX	*USER	*ENABLED	*YES	IBM-supplied User Profile	*NONE	Profil řídicího programu uzlu distribuovaných systémů
QEJB	*USER	*ENABLED	*YES	IBM-supplied User Profile	*NONE	Uživatelský profil Enterprise Java
QEJBSVR	*USER	*ENABLED	*YES	IBM-supplied User Profile	*NONE	Uživatelský profil aplikačního serveru WebSphere
QFNC	*USER	*ENABLED	*YES	IBM-supplied User Profile	*NONE	Profil financí
QGATE	*USER	*ENABLED	*YES	IBM-supplied User Profile	*NONE	Profil mostu VM/MVS
QIBMHELP	*SYSOPR	*ENABLED	*YES	IBM Eclipse Online Help	*NONE	
QIPP	*USER	*ENABLED	*YES	IBM-supplied User Profile	*NONE	Profil internetového tisku
QLPAUTO	*SYSOPR	*ENABLED	*YES	IBM-supplied User Profile	*ALLOBJ *IOSYSCFG *JOBCTL *SAVSYS *SECADM	Profil automatické instalace licencovaného programu
QLPINSTALL	*SYSOPR	*ENABLED	*YES	IBM-supplied User Profile	*ALLOBJ *IOSYSCFG *JOBCTL *SAVSYS *SECADM	Profil instalace licencovaného programu
QLWISVR	*USER	*DISABLED	*YES		*NONE	
QMGTC	*USER	*ENABLED	*YES	IBM-supplied User Profile	*NONE	Profil Centrální správy
QMQM [4]	*USER	*ENABLED	*YES	MQ PROFILE	*JOBCTL	Technický profil pro WebSphere MQ
QMQMADM [4]	*USER	*ENABLED	*YES	MQ GROUP PROFILE	*NONE	Skupinový profil pro WebSphere MQ

QMSF	*USER	*ENABLED	*YES	Mail Server Framework Profile	*NONE	Profil funkce poštovního serveru
QNETSPLF	*USER	*ENABLED	*YES	Internal Spool Network Profile	*NONE	Profil souběžného tisku v síti
QNFSANON	*USER	*ENABLED	*YES	IBM-supplied User Profile	*NONE	Uživatelský profil NFS
QNTP	*USER	*ENABLED	*YES	IBM-supplied User Profile	*NONE	Technický profil pro synchronizaci času
QPEX	*USER	*ENABLED	*YES	IBM-supplied User Profile	*NONE	Uživatelský profil průzkumníka výkonnosti
QPGMR	*PGMR	*ENABLED	*YES	Programmer and Batch User	*JOBCTL *SAVSYS	
QPM400	*USER	*ENABLED	*YES	IBM-supplied User Profile	*IOSYSCFG *JOBCTL	IBM Performance Management pro IBM i
QRJE	*PGMR	*ENABLED	*YES	IBM-supplied User Profile	*JOBCTL	Profil dálkového vstupu prací
QSECOFR	*SECOFR	*ENABLED	*NO	Security Officer	*ALLOBJ *AUDIT *IOSYSCFG *JOBCTL *SAVSYS *SECADM *SERVICE *SPLCTL	Správce systému (podobně jako u UNIX/Linux Root a ve Windows Administrator)
QSNADS	*USER	*ENABLED	*YES	IBM-supplied User Profile	*NONE	Profil distribučních služeb SNA
QSPL	*USER	*ENABLED	*YES	Internal Spool User Profile	*NONE	Profil souběžného tisku
QSPLJOB	*USER	*ENABLED	*YES	Internal Spool User Profile	*NONE	Profil úlohy souběžného tisku
QSRV	*PGMR	*ENABLED	*YES	Service User Profile	*JOBCTL *SERVICE	Servisní uživatelský profil
QSRVAGT	*SYSOPR	*ENABLED	*YES	IBM-supplied User Profile	*IOSYSCFG *JOBCTL *SERVICE	Uživatelský profil agenta služby
QSRVBAS	*PGMR	*ENABLED	*YES	Basic Service User Profile	*JOBCTL	Profil pro základní služby
QSVCCS	*SYSOPR	*ENABLED	*YES	CC Server User Profile	*JOBCTL	Uživatelský profil serveru CC
QSVSM	*SYSOPR	*DISABLED	*YES	SystemView System Manager User Profile	*JOBCTL	Uživatelský profil ECS
QSYS	*SECOFR	*ENABLED	*YES	Internal System User Profile	*ALLOBJ *AUDIT *IOSYSCFG *JOBCTL *SAVSYS *SECADM *SERVICE *SPLCTL	Profil systému
QSYSOPR	*SYSOPR	*ENABLED	*YES	System Operator	*JOBCTL *SAVSYS	Profil systémového operátora
QTCM	*USER	*DISABLED	*YES	IBM-supplied User Profile	*NONE	Profil Triggered Cache Manager
QTCP	*SYSOPR	*ENABLED	*YES	Internal TCP/IP User Profile	*JOBCTL	
QTFTP	*USER	*ENABLED	*YES	IBM-supplied User Profile	*NONE	TFTP (Trivial File Transfer Protocol)
QTMHHTP1	*USER	*ENABLED	*YES	HTTP Server CGI User Profile	*NONE	Uživatelský profil HTML Workstation Gateway Profile
QTMHHTTP	*USER	*ENABLED	*YES	HTTP Server User Profile	*NONE	
QTMPLPD	*USER	*ENABLED	*YES	ALLOW REMOTE LPR REQUESTERS	*NONE	
QTSTRQS	*USER	*ENABLED	*YES	Test Request User Profile	*NONE	Profil testovacího požadavku

QUMB	*USER	*ENABLED	*YES	ULTIMEDIA SYSTEM FACILITIES	*NONE	
QUSER	*USER	*ENABLED	*YES	Work Station User	*NONE	
QWEBQRYADM	*USER	*ENABLED	*NO	IBM DB2 WEB QUERY ADMINISTRATOR	*IOSYSCFG *JOBCTL *SAVSYS	
QWSERVICE	*USER	*DISABLED	*YES		*NONE	
QYCMCIMOM	*USER	*ENABLED	*YES	IBM-supplied User Profile	*NONE	Uživatelský profil serveru
QYPSJSVR	*USER	*ENABLED	*YES	IBM-supplied User Profile	*NONE	Profil serveru Centrální správy Java
QZRDLP	*USER	*DISABLED	*YES	LPAR Toolkit Owner Profile	*IOSYSCFG *SECADM *SERVICE	

Zdroj: Vlastní

[1] Buďte opatrní při odebírání oprávnění, která mají profily dodané IBM k objektům dodaným s operačním systémem. Některé profily dodané IBM mají soukromá oprávnění k objektům dodaným s operačním systémem. Odebráním jakýchkoliv těchto oprávnění můžete způsobit selhání systémových funkcí.

[2] Originální popis uživatelských profilů použitý v systému IBM i V6R1

[3] http://publib.boulder.ibm.com/infocenter/systems/scope/i5os/index.jsp?topic=/rzarl/rzarlibmsppl.htm

[4] Profil je v systému jen pokud je nainstalován produkt IBM WebSphere MQ for iSeries (5724H72)

Příloha č. 4

Systémové hodnoty (dodávané a doporučené nastavení)

Jméno hodnoty	Doporučená hodnota [1]	Dodávaná hodnota	Description	Popis	Poznámky
QABNORMSW	0	0	Previous end of system indicator	Indikátor předchozího ukončení systému	0=Normální, 1=Abnormální
QACGLVL	> *JOB	*NONE	Accounting level	Účtovací úroveň	
QACTJOB	> 1500	200	Initial number of active jobs	Počáteční počet aktivních úloh	
QADLACTJ	> 50	30	Additional number of active jobs	Přídavný počet aktivních úloh	
QADLSPLA	2048	2048	Spooling control block additional storage	Přídavná paměť řídicího bloku souběžného tisku	
QADLTOTJ	> 100	30	Additional number of total jobs	Celkový počet přídavných úloh	
QALWJOBITP	0	0	Allow jobs to be interrupted	Povolit přerušení úloh	
QALWOBJRST	*ALL	*ALL	Allow object restore option	Povolit obnovu objektů	
QALWUSRDMN	*ALL	*ALL	Allow user domain objects in libraries	Povolit objekty uživatelské domény v knihovnách	
QASTLVL	> *INTERMED	*BASIC	User assistance level	Asistenční úroveň uživatele	*BASIC, *INTERMED, *ADVANCED
QATNPGM	*ASSIST	*ASSIST	Attention program	Program klávesy Attention	
QAUDCTL	> *OBJAUD	*NONE	Auditing control	Řízení auditování	
	*AUDLVL				
	*NOTEMP				
QAUDENDACN	*NOTIFY	*NOTIFY	Auditing end action	Akce po ukončení auditování	*NOTIFY, *PWRDWNSYS
QAUDFRCLVL	*SYS	*SYS	Force auditing data	Údaje o vynucení auditování	
QAUDLVL	> *AUTFAIL	*NONE	Security auditing level	Úroveň auditování zabezpečení	
	*CREATE	' '			
	*DELETE	' '			
	*OBJMGT	' '			
	*JOBDTA	' '			
	*OFCSRV	' '			
	*OPTICAL	' '			
	*PGMFAIL	' '			
	*PRTDTA	' '			
	*SAVRST	' '			
	*SECURITY	' '			
	*SERVICE	' '			
	*SYSMGT	' '			
	*NETCMN	' '			
QAUDLVL2	*NONE	*NONE	Security auditing level extension	Rozšíření úrovně auditování zabezpečení	
QAUTOCFG	1	1	Autoconfigure devices	Automatická konfigurace zařízení	0=Vypnuto, 1=Zapnuto
QAUTORMT	1	1	Autoconfigure of remote controllers	Automatická konfigurace vzdálených řadičů	
QAUTOSPRPT	0	0	Automatic system disabled reporting	Automatické hlášení problémů systému	

QAUTOVRT	> 32767	0	Autoconfigure virtual devices	Automatická konfigurace virtuálních zařízení	
QBASACTLVL	> 399	6	Base storage pool activity level	Úroveň aktivity základní společné oblasti paměti	
QBASPOOL	> 1199200	2000	Base storage pool minimum size	Min. velikost základní společné oblasti paměti	
QBOOKPATH	/QDLS/QBKBOOKS/BOOKS	/QDLS/QBKBOOKS/BOOKS	Book and bookshelf search path	Vyhledávací cesta knih a jejich umístění	
QCCSID	> 870	65535	Coded character set identifier	Identifikátor kódované znakové sady	
QCENTURY	1	' '	Century	Století	0=1928 - 1999, 1=2000 - 2062
QCFGMSGQ	QSYS/ QSYSOPR	QSYS/QSYSOPR	Configuration message queue	Fronta zpráv pro konfigurační objekty	
QCHRID	> 959 870	697 37	Graphic character set and code page	Grafická znaková sada a kódová stránka	
QCHRIDCTL	*DEVD	*DEVD	Character identifier control	Řízení identifikátoru znaků	
QCMNARB	*CALC	*CALC	Communication arbiters	Komunikační arbitry	
QCMNRCYLMT	> 0 0	0 0	Communications recovery limits	Limit obnovy komunikací	
QCNTRYID	> CZ	US	Country or region identifier	Identifikátor země nebo oblasti	
QCONSOLE	> DSP01	QCONSOLE	Console name	Jméno konzole	
QCRTAUT	*CHANGE	*CHANGE	Create default public authority	Výchozí oprávnění při vytváření	
QCRTOBJAUD	> *CHANGE	*NONE	Create object auditing	Auditování vytváření objektů	
QCTLSBSD	> QSYS/QCTL	QSYS/QBASE	Controlling subsystem	Řídicí podsystém	
QCURSYM	$	$	Currency symbol	Symbol měny	
QDATE	01.01.2009	' '	System date	Systémové datum	
QDATETIME	01/01/2009 00:00:00.000000	' '	System date and time	Systémový datum a čas	
QDATFMT	> DMY	MDY	Date format	Formát data	
QDATSEP	/	/	Date separator	Oddělovač data	
QDAY	01	' '	Day	Den	
QDAYOFWEEK	*SUN	' '	Day of week	Den v týdnu	
QDBFSTCCOL	*ALL	*ALL	Database file statistics collection	Kolekce statistik databázového souboru	
QDBRCVYWT	0	0	Database recovery wait indicator	Indikátor čekání na obnovu databáze	
QDECFMT		' '	Decimal format	Formát zápisu desetinných míst	
QDEVNAMING	*NORMAL	*NORMAL	Device naming conventions	Konvence pojmenování zařízení	
QDEVRCYACN	*DSCMSG	*DSCMSG	Device I/O error action	Akce při I/O chybě zařízení	
QDSCJOBITV	> 60	240	Time interval before disconnected jobs end	Časový interval před ukončením odpojených úloh	
QDSPSGNINF	> 1	0	Sign-on display information control	Nastavení informací o přihlášení	
QDYNPTYADJ	1	1	Dynamic priority adjustment	Dynamické nastavení priorit	
QDYNPTYSCD	1	1	Dynamic priority scheduler	Dynamický plánovač priorit	

QENDJOBLMT	120	120	Time limit during immediate ending of a job	Časový limit pro okamžité ukončení úlohy	
QFRCCVNRST	1	1	Force conversion on restore	Vynucení konverze při obnově	
QHOUR	0	' '	Hour of the day	Hodina ze dne	
QHSTLOGSIZ	> 32767	5000	Maximum history log records	Maximum záznamů v protokolu událostí	
QIGC	1	1	DBCS version installed indicator	Indikátor nainstalování verze DBCS	
QIGCCDEFNT	*NONE	*NONE	Double byte code font	Dvoubajtově kódovaný font	
QIGCFNTSIZ	*NONE	*NONE	Coded font size	Velikost bodu kódovaného fontu	
QINACTITV	> 60	*NONE	Inactive job time-out	Časový limit neaktivní úlohy	
QINACTMSGQ	> *DSCJOB	*ENDJOB	Inactive job message queue	Fronta zpráv neaktivní úlohy	
QIPLDATTIM	*NONE	*NONE	Date and time to automatically IPL	Datum a čas automatického IPL	
QIPLSTS	> 2	0	IPL status indicator	Indikátor stavu IPL	
QIPLTYPE	0	0	Type of IPL to perform	Typ IPL, který se má provést	
QJOBMSGQFL	> *PRTWRAP	*NOWRAP	Job message queue full action	Akce při zaplnění fronty zpráv úlohy	
QJOBMSGQMX	16	16	Maximum size of job message queue	Maximální velikost fronty zpráv úlohy	
QJOBMSGQSZ	16	16	Job message queue initial size	Počáteční velikost fronty zpráv úlohy	
QJOBMSGQTL	24	24	Job message queue maximum initial size	Maximální počáteční velikost fronty zpráv úlohy	
QJOBSPLA	3516	3516	Spooling control block initial size	Počáteční velikost řídicího bloku souběžného tisku	
QKBDBUF	*TYPEAHEAD	*TYPEAHEAD	Type ahead and/or attention key option	Zápis napřed a/nebo klávesa Attention	
QKBDTYPE	> CSB	USB	Keyboard language character set	Znaková sada jazyka klávesnice	
QLANGID	> CSY	ENU	Language identifier	Identifikátor jazyka	
QLEAPADJ	0	0	Leap year adjustment	Nastavení přestupného roku	
QLIBLCKLVL	1	1	Library locking level	Úroveň uzamykání knihoven	
QLMTDEVSSN	> 1	0	Limit device sessions	Omezení relací pro zařízení	
QLMTSECOFR	> 0	1	Limit security officer device access	Omezení přístupu správce systému k zařízení	
QLOCALE	> *NONE	' '	Locale path name	Jméno cesty k lokalitě	
QLOGOUTPUT	*JOBEND	*JOBEND	Job log output	Výstup logu úloh	
QMAXACTLVL	*NOMAX	*NOMAX	Maximum activity level of system	Maximální úroveň aktivity systému	
QMAXJOB	245280	163520	Maximum number of jobs	Maximální počet úloh	
QMAXSGNACN	> 2	3	Action to take for failed signon attempts	Akce po neúspěšném přihlášení	1=Vypnuto zařízení, 2=Zablokován profil, 3=Zablokován profil a vypnuto zařízení
QMAXSIGN	3	3	Maximum sign-on attempts allowed	Maximální povolený počet pokusů o přihlášení	
QMAXSPLF	9999	9999	Maximum spooled files	Maximální počet souborů pro souběžný tisk	

QMCHPOOL	> 2894364	20000	Machine storage pool size	Velikost společné oblasti paměti počítače	
QMINUTE	0	' '	Minute of the hour	Minuta z hodiny	
QMLTTHDACN	0	2	Multithreaded job action	Akce úlohy s více vlákny	
QMODEL	570	' '	System model number	Číslo modelu systému	
QMONTH	01	' '	Month of the year	Měsíc v roce	
QPASTHRSVR	*CALC	*CALC	Pass-through servers	Přechodové servery	
QPFRADJ	> 3	2	Performance adjustment	Přizpůsobení výkonu	0=Žádné, 1=Při IPL, 2=Při IPL a automatické nastavení, 3=Automatické nastavení
QPRBFTR	> QSRVAGT /QS9FILTER	*NONE	Problem log filter	Filtr protokolu problémů	
QPRBHLDITV	> 0	30	Problem log hold interval	Interval zadržení v protokolu problémů	
QPRCFEAT	7748	' '	Processor feature	Označení (typ) procesoru	
QPRCMLTTSK	> 1	2	Processor multi tasking	Souběžné zpracování úloh procesorem	0=Vypnuto, 1=Zapnuto, 2=Řízeno systémem
QPRTDEV	PRT01	PRT01	Printer device description	Výchozí systémová tiskárna	
QPRTKEYFMT	*PRTHDR	*PRTHDR	Print header and/or border information	Tisk hlavičky a/nebo okraje	
QPRTTXT		' '	Print text	Tištěný text	
QPWDCHGBLK	> 24	*NONE	Block password change	Blokování změny hesla	
QPWDEXPITV	> 30	*NOMAX	Password expiration interval	Interval platnosti hesla	
QPWDEXPWRN	7	7	Password expiration warning	Varování vypršení platnosti hesla	
QPWDLMTAJC	0	0	Limit adjacent digits in password	Omezit sousední číslice v hesle	
QPWDLMTCHR	*NONE	*NONE	Limit characters in password	Omezit znaky v hesle	
QPWDLMTREP	> 2	0	Limit repeating characters in password	Omezit opakující se znaky v hesle	
QPWDLVL	> 3	0	Password level	Úroveň hesla	
QPWDMAXLEN	> 128	8	Maximum password length	Maximální délka hesla	
QPWDMINLEN	> 8	6	Minimum password length	Minimální délka hesla	
QPWDPOSDIF	0	0	Limit password character positions	Omezit umístění znaků v hesle	
QPWDRQDDGT	> 1	0	Require digit in password	Požadování číslic v hesle	
QPWDRQDDIF	> 5	0	Duplicate password control	Možnost opakování hesla	
QPWDRULES	*PWDSYSVAL	*PWDSYSVAL	Password rules	Pravidla pro hesla	*PWDSYSVAL=Použití hodnot QPWD*
QPWDVLDPGM	*NONE	*NONE	Password validation program	Program pro ověření hesla	
QPWRDWNLMT	900	900	Maximum time for PWRDWNSYS *IMMED	Maximální čas pro PWRDWNSYS *IMMED	
QPWRRSTIPL	0	0	Automatic IPL after power restored	Automatický IPL po obnově dodávky proudu	0=Nelze, 1=Lze
QQRYDEGREE	> *OPTIMIZE	*NONE	Parallel processing degree	Úroveň paralelního zpracování	*NONE, *IO,*OPTIMIZE, *MAX
QQRYTIMLMT	*NOMAX	*NOMAX	Query processing time limit	Časový limit pro zpracování dotazu	

QRCLSPLSTG	8	8	Reclaim spool storage	Náprava paměti určené pro souběžný tisk	
QRETSVRSEC	> 1	0	Retain server security data	Uchovávat data zabezpečení serveru	
QRMTIPL	0	0	Remote power on and IPL	Vzdálené zapnutí a IPL	
QRMTSIGN	*FRCSIGNON	*FRCSIGNON	Remote sign-on control	Vzdálené přihlášení	
QRMTSRVATR	0	0	Remote service attribute	Atribut vzdálených služeb	
QSAVACCPTH	1	1	Save access paths	Ukládat přístupové cesty	
QSCANFS	*ROOTOPNUD	*ROOTOPNUD	Scan file systems	Skenování systému souborů	
QSCANFSCTL	*NONE	*NONE	Scan file systems control	Nastavení skenování systému souborů	
QSCPFCONS	1	1	IPL action with console problem	Akce IPL při problému konzole	
QSECOND	0	' '	Second of the minute	Sekunda z minuty	
QSECURITY	40	40	System security level	Úroveň zabezpečení systému	
QSETJOBATR	*NONE	*NONE	Set job attributes from locale	Nastavit atributy úlohy z lokality	
QSFWERRLOG	*LOG	*LOG	Software error logging	Protokolování chyb softwaru	
QSHRMEMCTL	1	1	Shared memory control	Řízení sdílené paměti	
QSPCENV	*NONE	*NONE	Special environment	Speciální prostředí	
QSPLFACN	*KEEP	*KEEP	Spooled file action	Akce souboru pro souběžný tisk	*KEEP, *DETACH
QSRLNBR	65XXXXX	' '	System serial number	Sériové číslo systému	
QSRTSEQ	*HEX	*HEX	Sort sequence	Třídicí posloupnost	
QSRVDMP	*DMPUSRJOB	*DMPUSRJOB	Service dump control	Nastavení servisního výpisu	
QSSLCSL	*RSA_AES_128_CBC_SHA	*RSA_AES_128_CBC_SHA	Secure sockets layer cipher specification list	Seznam specifikací šifer SSL	
	*RSA_RC4_128_SHA	*RSA_RC4_128_SHA			
	*RSA_RC4_128_MD5	*RSA_RC4_128_MD5			
	*RSA_AES_256_CBC_SHA	*RSA_AES_256_CBC_SHA			
	*RSA_3DES_EDE_CBC_SHA	*RSA_3DES_EDE_CBC_SHA			
	*RSA_DES_CBC_SHA	*RSA_DES_CBC_SHA			
	*RSA_EXPORT_RC4_40_MD5	*RSA_EXPORT_RC4_40_MD5			
	*RSA_EXPORT_RC2_CBC_40_MD5	*RSA_EXPORT_RC2_CBC_40_MD5			
	*RSA_NULL_SHA	*RSA_NULL_SHA			
	*RSA_NULL_MD5	*RSA_NULL_MD5			
QSSLCSLCTL	*OPSYS	*OPSYS	Secure sockets layer cipher control	Řízení šifer SSL	
QSSLPCL	*OPSYS	*OPSYS	Secure sockets layer protocols	Protokoly SSL	
QSTGLOWACN	*MSG	*MSG	Auxiliary storage lower limit action	Akce při dolním limitu pomocné paměti	
QSTGLOWLMT	5.0000	5.0000	Auxiliary storage lower limit	Spodní limit pomocné paměti	

QSTRPRTWTR	1	1	Start print writers at IPL	Spustit tiskové služby při IPL	
QSTRUPPGM	> MODSYSLIB/ QSTRUP	QSYS/QSTRUP	Startup program	Program aktivovaný po spuštění systému	
QSTSMSG	*NORMAL	*NORMAL	Display status messages	Zobrazení stavových zpráv	
QSVRAUTITV	2880	2880	Server authentication interval	Interval autentizace serveru	
QSYSLIBL	> MODSYSLIB	QSYS	System part of the library list	Systémová část seznamu knihoven	
	QSYS	QSYS2			
	QSYS2	QHLPSYS			
	QHLPSYS	QUSRSYS			
	QUSRSYS	' '			
QTHDRSCADJ	1	1	Thread resources adjustment	Nastavení prostředků vláken	
QTHDRSCAFN	*NOGROUP *NORMAL	*NOGROUP *NORMAL	Thread resources affinity	Afinita prostředků vláken	
QTIMADJ	*NONE	*NONE	Time adjustment	Nastavení času	
QTIME	00:00:00	' '	Time of day	Čas ze dne	
QTIMSEP	:	:	Time separator	Oddělovač času	
QTIMZON	> QP0100CET2	' '	Time zone	Časová zóna	
QTOTJOB	> 25000	200	Initial total number of jobs	Celkový Počáteční počet úloh	
QTSEPOOL	*NONE	*NONE	Time slice end pool	Oblast na konci přiděleného času	
QUPSDLYTIM	> 0 0	200	Uninterruptible power supply delay time	Doba prodlevy UPS	
QUPSMSGQ	QSYS/ QSYSOPR	QSYS/QSYSOPR	Uninterruptible power supply message queue	Fronta zpráv UPS	
QUSEADPAUT	*NONE	*NONE	Use adopted authority	Použití adoptovaného oprávnění	
QUSRLIBL	> MODUTIL	QGPL	User part of the library list	Uživatelská část seznamu knihoven	
	USRTOOL	QTEMP			
	QGPL	' '			
	QTEMP	' '			
QUTCOFFSET	> +0100	0	Coordinated universal time offset	Posun vůči univerzálnímu času	
QVFYOBJRST	3	3	Verify object on restore	Ověřování objektů při obnově	
QYEAR	9	' '	Year	Rok	

Zdroj: Vlastní

[1] > znamená doporučená hodnota je rozdílná od předvolené (po instalaci OS)

Příloha č. 5

Možné hodnoty pro systémovou hodnotu QAUDLVL (úroveň auditování)

***NONE**	Nejsou protokolovány žádné události řízené systémovou hodnotou QAUDLVL nebo QAUDLVL2. Pro jednotlivé uživatele jsou protokolovány události na základě hodnot AUDLVL v uživatelských profilech.
***NOTAVL**	Zobrazení této hodnoty indikuje, že systémová hodnota není uživateli k dispozici, protože uživatel nemá speciální oprávnění *AUDIT nebo *ALLOBJ. Systémovou hodnotu nelze nastavit na tuto hodnotu.
***AUDLVL2**	K určení operací týkajících se zabezpečení, které se mají auditovat, jsou použity obě systémové hodnoty QAUDLVL a QAUDLVL2.
***ATNEVT**	Události upozornění jsou zaznamenány.
***AUTFAIL**	Jsou protokolovány události selhání oprávnění.
***CREATE**	Jsou protokolovány operace vytvoření objektů.
***DELETE**	Jsou protokolovány operace vymazání objektů.
***JOBBAS**	Jsou auditovaný základní funkce úloh.
***JOBCHGUSR**	Jsou auditovaný změny aktivního uživatelského profilu podprocesu nebo příslušných skupinových profilů.
***JOBDTA**	Jsou protokolovány operace ovlivňující úlohu. Hodnota *JOBDTA je složena ze dvou hodnot (*JOBBAS a *JOBCHGUSR), které umožňují lépe přizpůsobit auditování. Jsou-li zadány obě hodnoty, získáte stejné auditování, jako by bylo zadáno pouze *JOBDTA.
***NETBAS**	Jsou auditovány základní funkce sítě.
***NETCLU**	Jsou auditovány operace týkající se klastrů a skupiny klastrového zdroje.
***NETCMN**	Jsou auditovány funkce sítě a komunikační funkce. Hodnota *NETCMN se skládá z několika hodnot, aby bylo možné auditování lépe přizpůsobit potřebám uživatele. Hodnota *NETCMN se skládá z následujících položek: *NETBAS, *NETCLU, *NETFAIL, *NETSCK
***NETFAIL**	Jsou auditovaná selhání sítě.
***NETSCK**	Jsou auditovány úlohy soketů.
***OBJMGT**	Jsou protokolovány operace přejmenování a přesunu objektů.
***OFCSRV**	Jsou protokolovány změny systémového distribučního adresáře a kancelářské poštovní operace.
***OPTICAL**	Je protokolováno použití optických nosičů.
***PGMADP**	Je protokolováno získání oprávnění od programu, který oprávnění adoptuje.
***PGMFAIL**	Jsou protokolována narušení integrity systému.
***PRTDTA**	Jsou protokolovány činnosti: tisk souboru pro souběžný tisk, přímé odeslání výstupu do tiskárny a odeslání výstupu do vzdálené tiskárny.
***SAVRST**	Jsou protokolovány operace uložení a obnovy.
***SECCFG**	Je auditovaná konfigurace zabezpečení.
***SECDIRSRV**	Jsou auditovány změny a aktualizace prováděné funkcemi adresářové služby.
***SECIPC**	Jsou auditovány změny komunikace mezi procesy.
***SECNAS**	Jsou auditovány operace síťové autentizační služby.
***SECRUN**	Jsou auditovány funkce zabezpečení týkající se doby provádění.
***SECSCKD**	Jsou auditovány deskriptory soketů.
***SECURITY**	Jsou protokolovány funkce související se zabezpečením. Hodnota *SECURITY se skládá z několika hodnot, pomocí kterých lze auditování lépe přizpůsobit. Hodnota *SECURITY se skládá z následujících položek: *SECCFG, *SECDIRSRV, *SECIPC, *SECNAS, *SECRUN, *SECSCKD, *SECVFY, *SECVLDL
***SECVFY**	Je auditováno použití verifikačních funkcí.
***SECVLDL**	Jsou auditovány změny objektů ověřovacího seznamu.
***SERVICE**	Je protokolováno použití servisních nástrojů.
***SPLFDTA**	Jsou protokolovány operace provedené se soubory pro souběžný tisk.
***SYSMGT**	Je protokolováno použití funkcí správy systému.

Zdroj: http://publib.boulder.ibm.com/infocenter/systems/scope/i5os/index.jsp?topic=/rzarl/rzarlaudlev.htm

Příloha č. 6

Zobrazení uživatelského profilu QSECOFR (**DSPUSRPRF QSECOFR**)

(Jsou zobrazeny všechny parametry uživatelského profilu – tyto parametry mají všechny profily v systému.)

```
User Profile . . . . . :   QSECOFR
Previous sign-on . . . . . :   15/01/09  15:59:02
Password verifications not valid . . . . . :   0
Status . . . . . :   *ENABLED
Date password last changed . . . . . :   15/01/09  15:58:39
Password is *NONE  . . . . . :   *NO
Password expiration interval . . . . . :   *NOMAX
Password set expired by command  . . . . . :   *NO
Block password change  . . . . . :   *SYSVAL[1]
Local password management  . . . . . :   *YES
User class . . . . . :   *SECOFR
Creation date/time . . . . . :   08/07/08  11:02:22
Change date/time . . . . . :   15/01/09  08:53:13
Last used date . . . . . :   15/01/09
Restore date/time  . . . . . :   08/07/08  13:43:59
Special authority  . . . . . :   *ALLOBJ
                                 *AUDIT
                                 *IOSYSCFG
                                 *JOBCTL
                                 *SAVSYS
                                 *SECADM
                                 *SERVICE
                                 *SPLCTL
Group profile  . . . . . :   *NONE
Owner  . . . . . :   *USRPRF
Group authority  . . . . . :   *NONE
Group authority type . . . . . :   *PRIVATE
Supplemental groups  . . . . . :   *NONE
Assistance level . . . . . :   *SYSVAL
Current library  . . . . . :   *CRTDFT
Initial program  . . . . . :   *NONE
  Library  . . . . . :
Initial menu . . . . . :   MAIN
  Library  . . . . . :     *LIBL
Limit capabilities . . . . . :   *NO
Text . . . . . :   Security Officer
Display sign-on information  . . . . . :   *SYSVAL
Limit device sessions  . . . . . :   *NO
Keyboard buffering . . . . . :   *SYSVAL
Storage information:
  Maximum storage allowed  . . . . . :   *NOMAX
  Storage used . . . . . :   9166364
  Storage used on independent ASP  . . . . :   *NO
Highest scheduling priority  . . . . . :   0
Job description  . . . . . :   QDFTJOBD
  Library  . . . . . :     QGPL
Accounting code  . . . . . :
Message queue  . . . . . :   QSECOFR
  Library  . . . . . :     QUSRSYS
Message queue delivery . . . . . :   *NOTIFY
Message queue severity . . . . . :   00
Output queue . . . . . :   *WRKSTN
  Library  . . . . . :
Printer device . . . . . :   *WRKSTN
Special environment  . . . . . :   *SYSVAL
User Profile . . . . . :   QSECOFR
Attention program  . . . . . :   *SYSVAL
  Library  . . . . . :
Sort sequence  . . . . . :   *SYSVAL
  Library  . . . . . :
```

```
Language identifier  . . . . . :   *SYSVAL
Country or region identifier . . . . . :   *SYSVAL
Coded character set identifier . . . . . :   *SYSVAL
Character identifier control . . . . . :   *SYSVAL
Locale job attributes  . . . . . :   *SYSVAL
Locale . . . . . :   *NONE
User options . . . . . :   *NONE
Object auditing value  . . . . . :   *NONE
Action auditing values . . . . . :   *NONE
User ID number . . . . . :   0
Group ID number  . . . . . :   *NONE
User entitlement required  . . . . . :   NO
Home directory . . . . . :   /HOME/QSECOFR
```

Zdroj: Vlastní

[1] Hodnota *SYSVAL znamená, použití systémové hodnoty - o kterou se jedná lze zjistit klávesou F1 stisknutou nad konkrétní položkou

Parametry příkazu **DSPJRN**

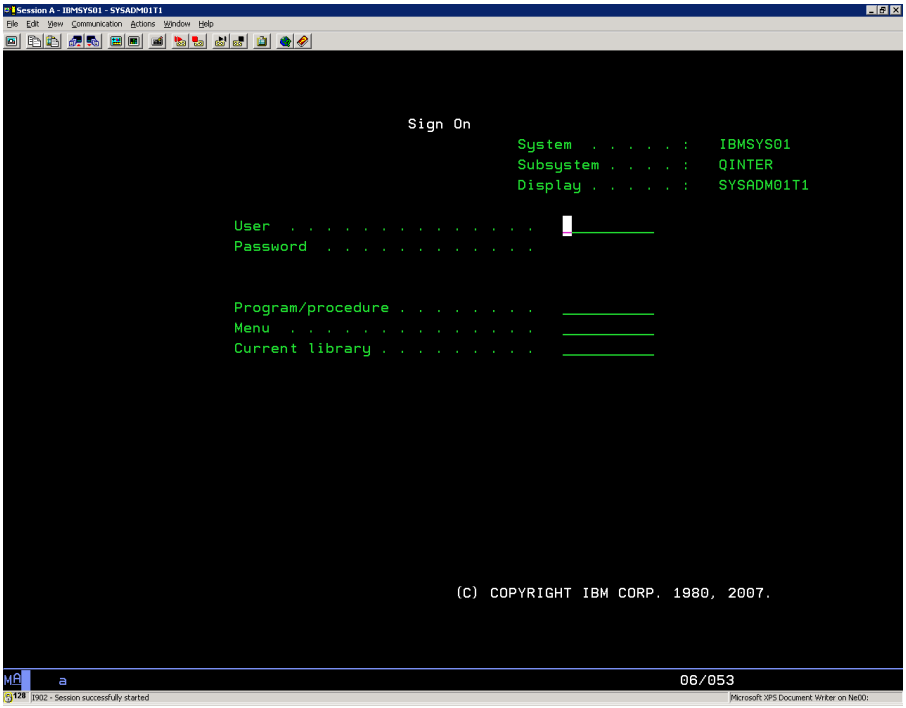
```
                        Display Journal (DSPJRN)

Type choices, press Enter.

Journal  . . . . . . . . . . . . > QAUDJRN       Name, *INTSYSJRN
  Library  . . . . . . . . . . .     *LIBL       Name, *LIBL, *CURLIB
Journaled file:
  File . . . . . . . . . . . . .                 Name, *ALLFILE, *ALL
    Library  . . . . . . . . . .     *LIBL       Name, *LIBL, *CURLIB
  Member . . . . . . . . . . . .   *FIRST        Name, *FIRST, *ALL,
*NONE
               + for more values
Objects:
  Object . . . . . . . . . . . .                 Name, *ALL
    Library  . . . . . . . . . .     *LIBL       Name, *LIBL, *CURLIB
  Object type  . . . . . . . . .                 *FILE, *DTAARA, *DTAQ,
*LIB
  Member, if data base file  . .   *FIRST        Name, *FIRST, *ALL,
*NONE
               + for more values
 Objects:
   Name . . . . . . . . . . . . .

   Include or omit  . . . . . .   *INCLUDE      *INCLUDE, *OMIT
                + for more values
 Directory subtree  . . . . . .   *NONE         *NONE, *ALL
 Name pattern:
   Pattern  . . . . . . . . . .   *

                                                                      ...
   Include or omit  . . . . . .   *INCLUDE      *INCLUDE, *OMIT
                + for more values
Range of journal receivers:
  Starting journal receiver  . . > *CURCHAIN     Name, *CURRENT,
*CURCHAIN
    Library  . . . . . . . . . .                 Name, *LIBL, *CURLIB
  Ending journal receiver  . . .                 Name, *CURRENT
    Library  . . . . . . . . . .                 Name, *LIBL, *CURLIB
Starting large sequence number     *FIRST
Starting date and time:
  Starting date  . . . . . . . . > 150109        Date
  Starting time  . . . . . . . . > 140000        Time
Ending large sequence number . .   *LAST
Ending date and time:
  Ending date  . . . . . . . . . > 150109        Date
  Ending time  . . . . . . . . . > 143000        Time
Number of journal entries  . . .   *ALL          Number, *ALL
Journal codes:
  Journal code value . . . . . . > T             *ALL, *CTL, A, B, C, D,
E...
  Journal code selection . . . .   *ALLSLT       *ALLSLT, *IGNFILSLT...
               + for more values
Journal entry types  . . . . . . > AF            Character value, *ALL,
*RCD
               + for more values
Job name . . . . . . . . . . . .   *ALL          Name, *ALL
  User . . . . . . . . . . . . .                 Name
  Number . . . . . . . . . . . .                 000000-999999
Program  . . . . . . . . . . . .   *ALL          Name, *ALL
User profile . . . . . . . . . .   *ALL          Name, *ALL
Commit cycle large identifier  .   *ALL
Dependent entries  . . . . . . .   *ALL          *ALL, *NONE
Output format  . . . . . . . . .   *CHAR         *CHAR, *HEX
Journal identification number  .                 Character value
```

```
Include hidden entries . . . . .   *NO            *NO, *YES
File identifier  . . . . . .
               + for more values
Object journal identifier  . . .
               + for more values
Output . . . . . . . . . . . . . > *OUTFILE      *, *PRINT, *OUTFILE
Outfile format . . . . . . . . . > *TYPE5        *TYPE1, *TYPE2,
*TYPE3...
File to receive output . . . . . > JRNOUT19      Name
  Library  . . . . . .             *LIBL         Name, *LIBL, *CURLIB
Output member options:
  Member to receive output . . .   *FIRST        Name, *FIRST
  Replace or add records . . . .   *REPLACE      *REPLACE, *ADD
Entry data length:
  Field data format  . . . . . > *CALC          Number, *VARLEN
  Variable length field length                  Number, *CALC
  Allocated length . . . . . .                  Number, *FLDLEN
Null value indicators length:
  Field data format  . . . . . .   *OUTFILFMT    1-8000, *VARLEN
  Variable length field length                  1-8000, *CALC
  Allocated length . . . . . .                  1-8000, *FLDLEN

                          Additional Parameters

Include entries  . . . . . .   *CONFIRMED    *CONFIRMED, *ALL
Starting sequence number . . . .   *FIRST
Ending sequence number . . . . .   *LAST
Commit cycle identifier  . . . .   *ALL
ASP device . . . . . .   *             Name, *
```

Zdroj: Vlastní

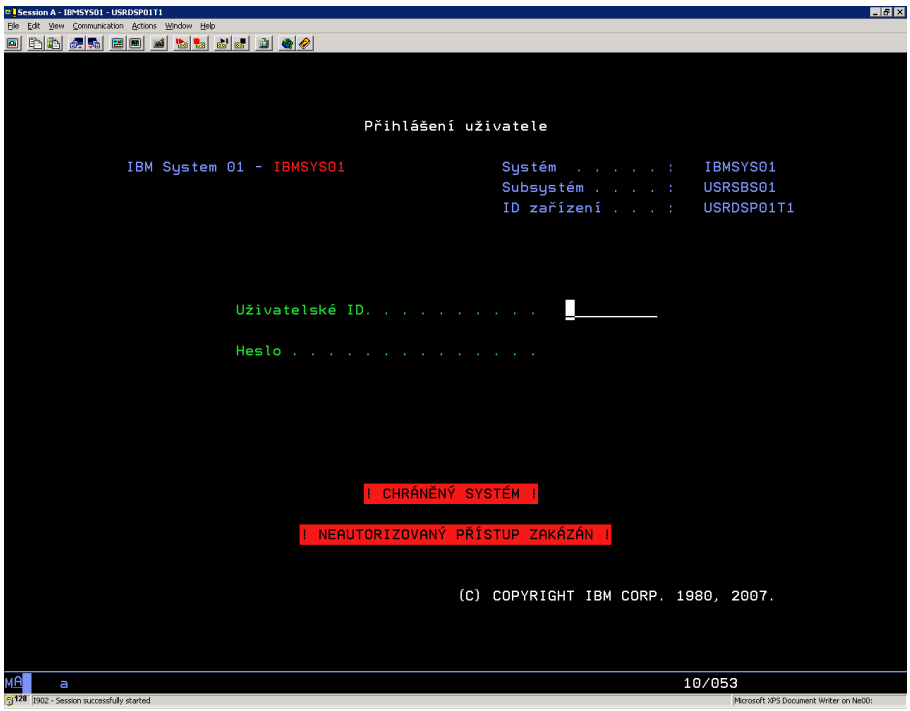
Přihlašovací obrazovky – emulace 5250

Obrázek 7 - Základní přihlašovací obrazovka (Subsystém QINTER)



Zdroj: Vlastní

Obrázek 8 – Uživatelská přihlašovací obrazovka



Zdroj: Vlastní

Příloha č. 9

Vstupy a výstupy vybraných příkazů

Příkaz **WRKUSRPRF, CHGUSRPRF**

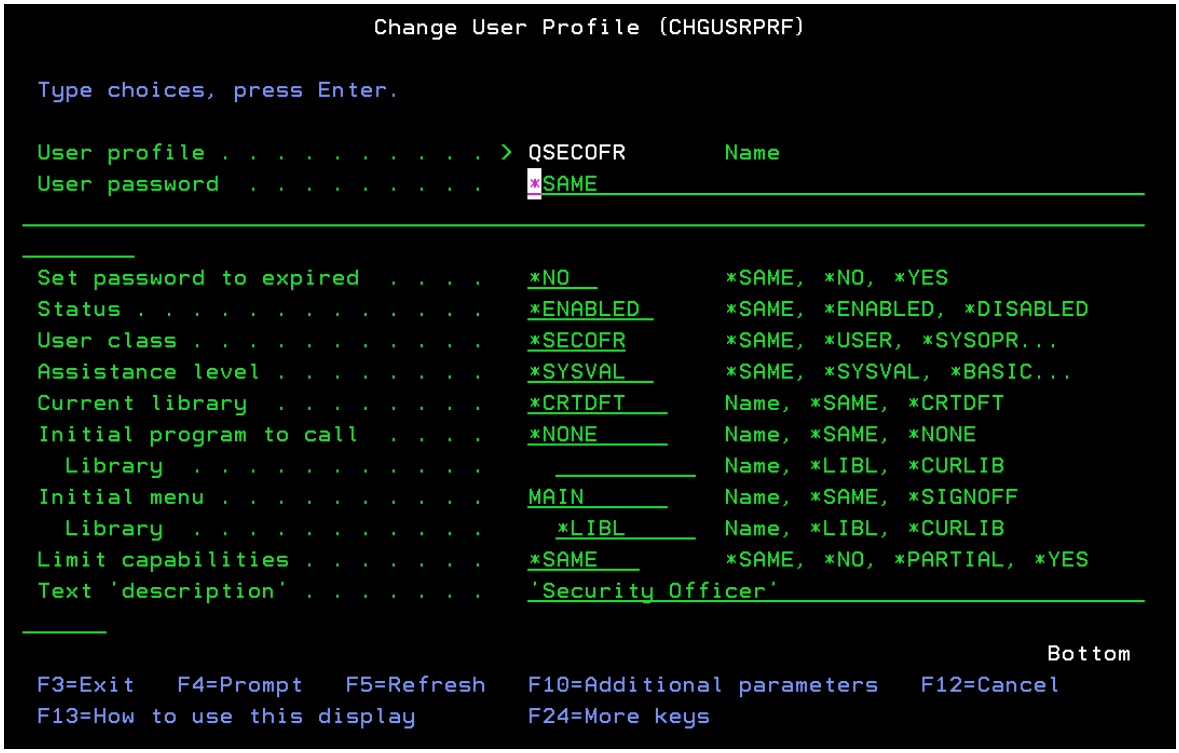
Obrázek 9 - Příkaz WRKUSRPRF QS*

Zdroj: Vlastní

Obrázek 10 - Výstup příkazu WRKUSRPRF QS*

Zdroj: Vlastní

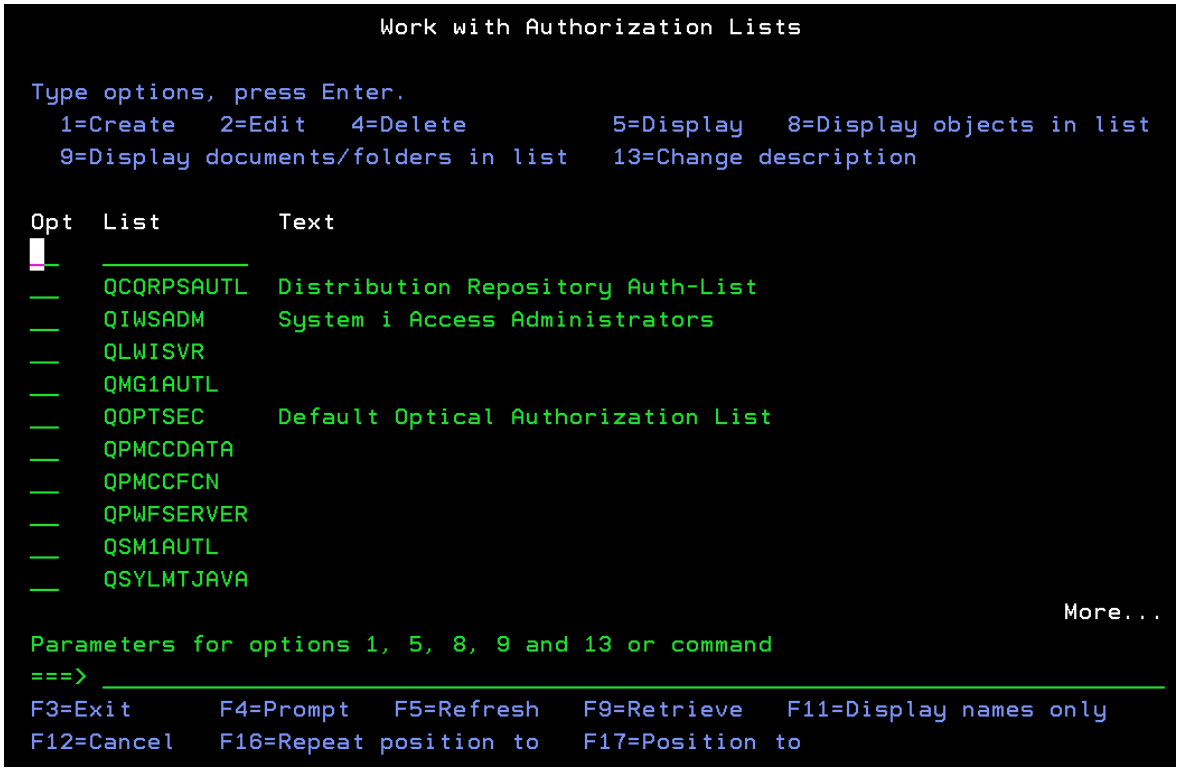
Obrázek 11 - Příkaz CHGUSRPRF QSECOFR



Zdroj: Vlastní

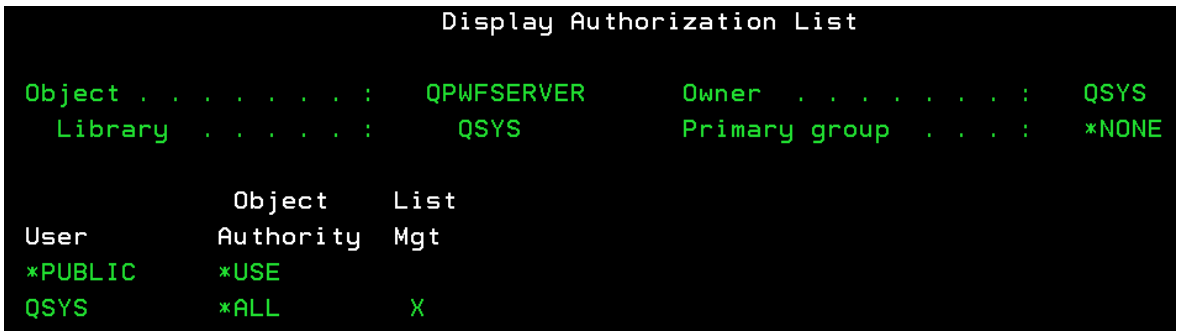
Příkaz **WRKAUTL, DSPAUTL**

Obrázek 12 - Příkaz WRKAUTL Q*



Zdroj: Vlastní

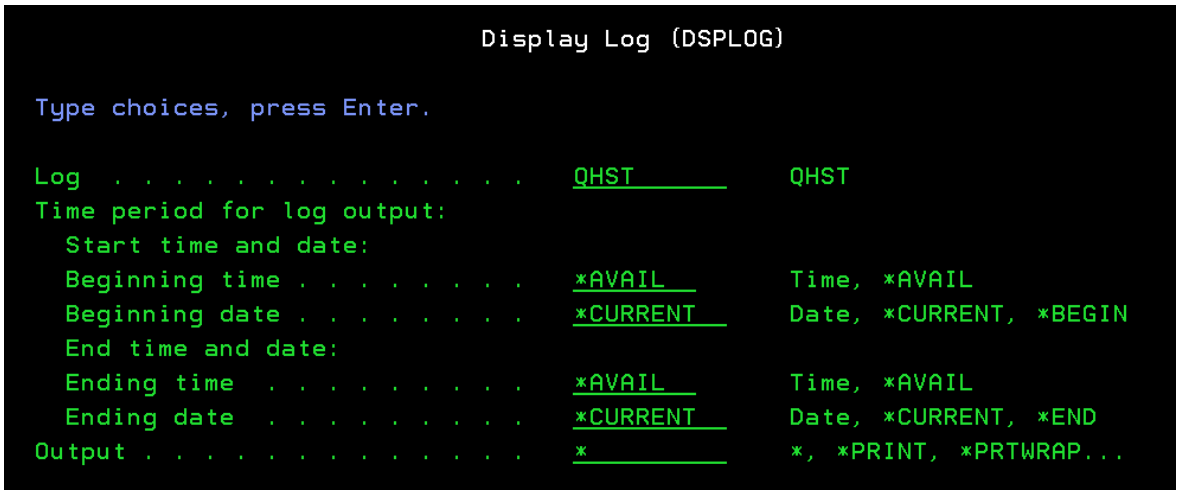
Obrázek 13 - Příkaz DSPAUTL QPWFSERVER



Zdroj: Vlastní

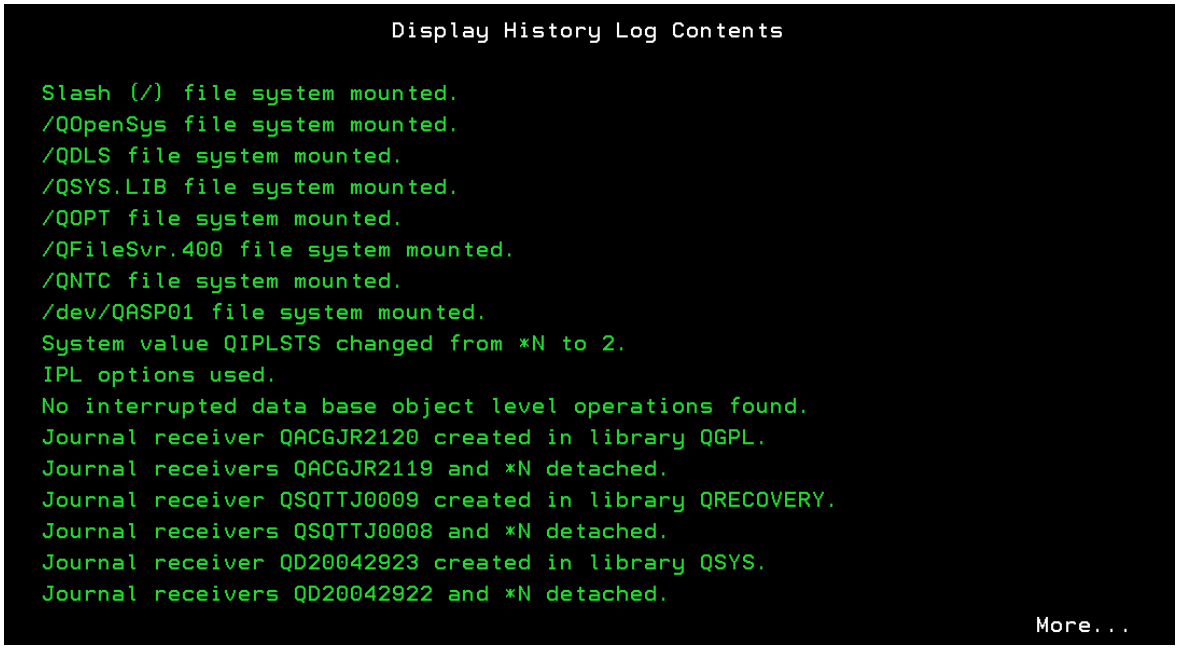
Příkaz **DSPLOG**

Obrázek 14 - Příkaz DSPLOG



Zdroj: Vlastní

Obrázek 15 - Výstup příkazu DSPLOG



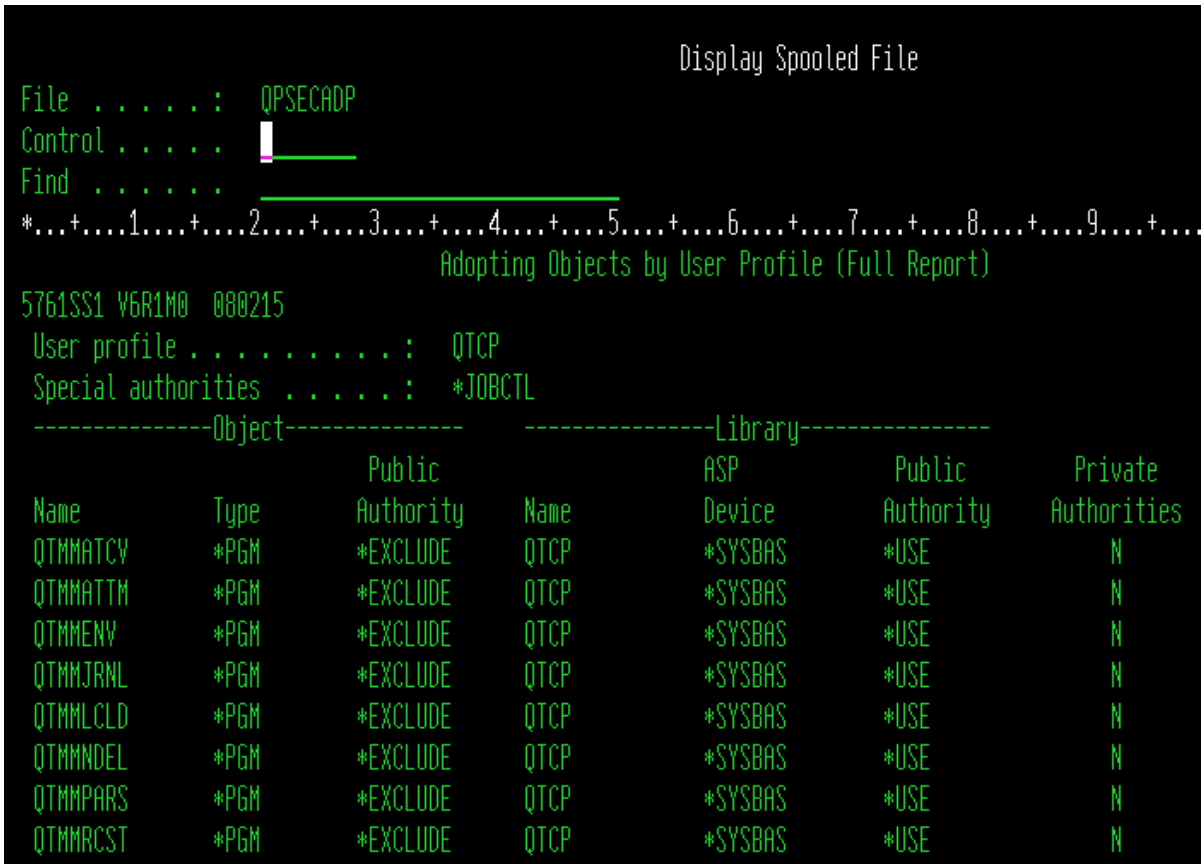
Zdroj: Vlastní

Příkaz **PRTADPOBJ**

Obrázek 16 - Příkaz PRTADPOBJ

Zdroj: Vlastní

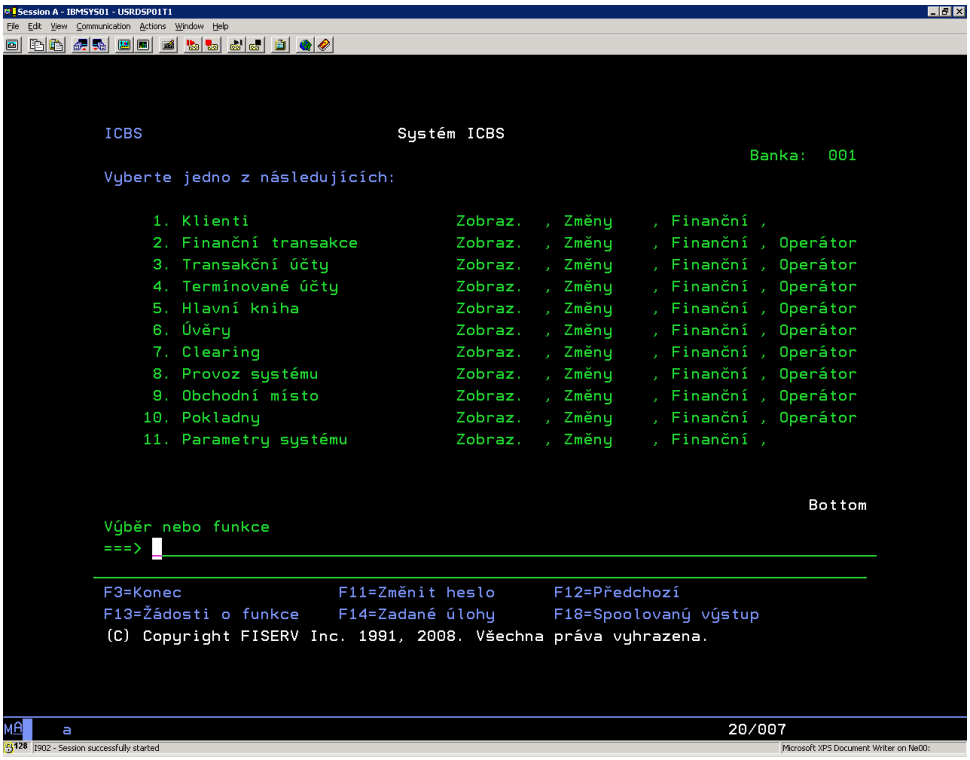
Obrázek 17 - Výstup příkazu PRTADPOBJ

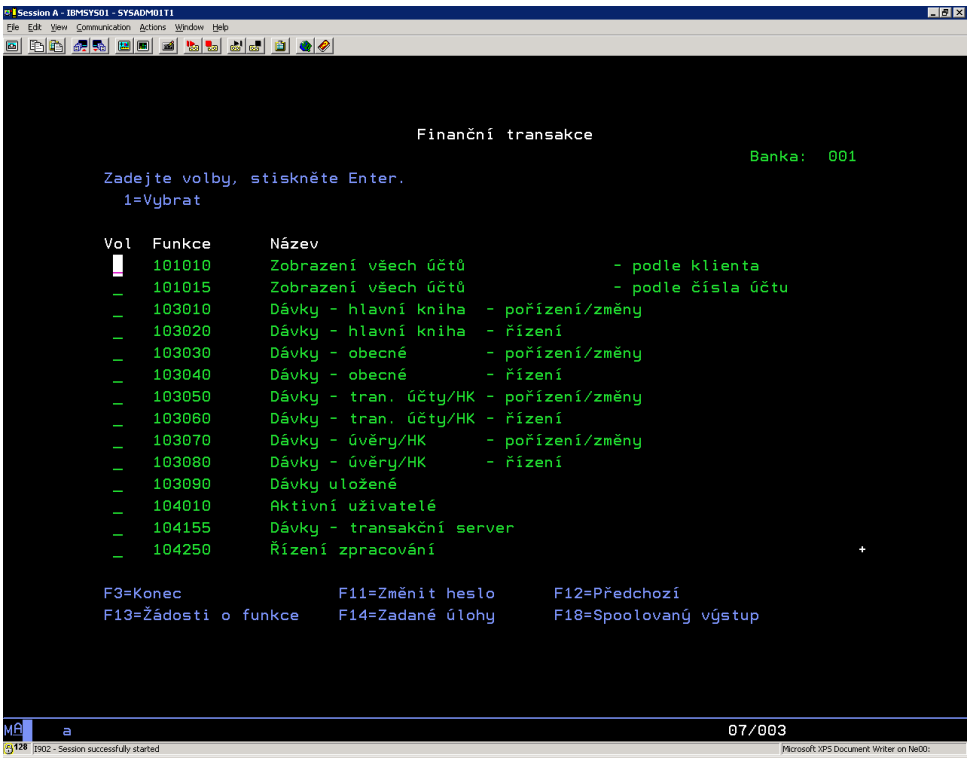


Zdroj: Vlastní

Ukázky aplikačních obrazovek – emulace 5250

Aplikace ICBS: Core bankovní systém, Terminálový provoz, FISERV Inc.[36] - USA

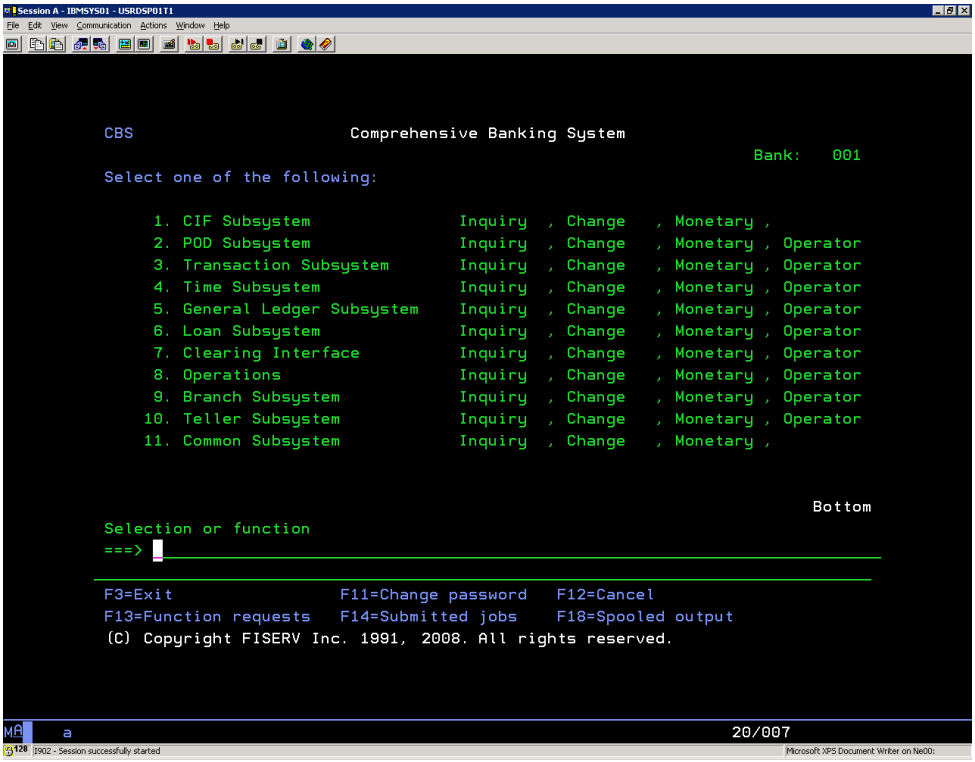




Zdroj: Vlastní

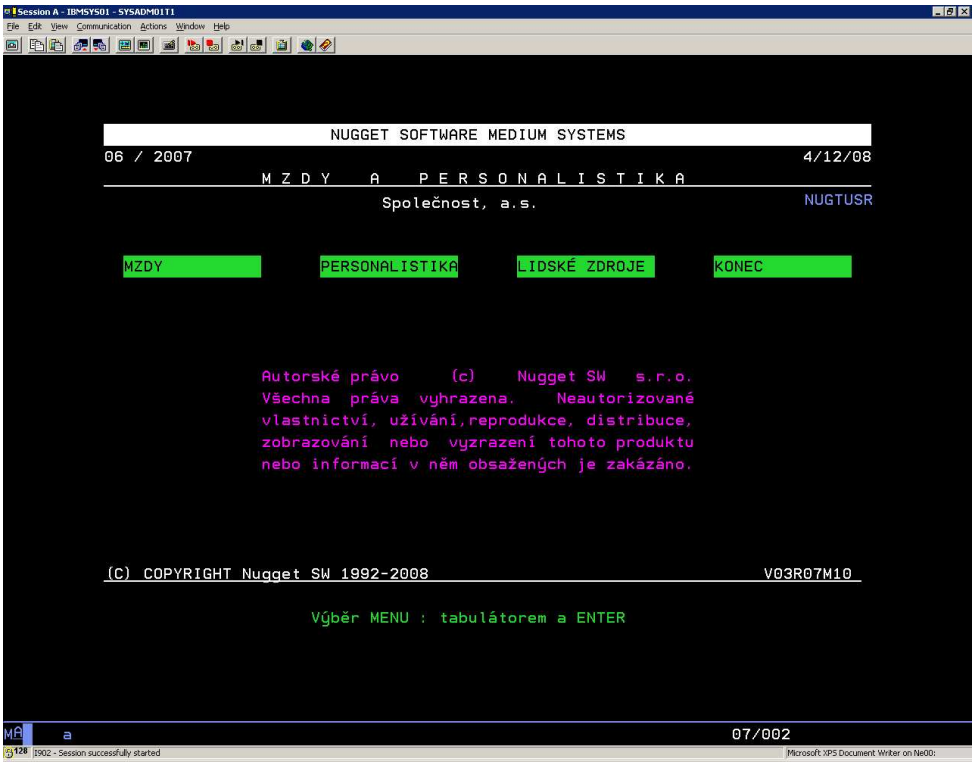
[36] http://www.fiserv.com/

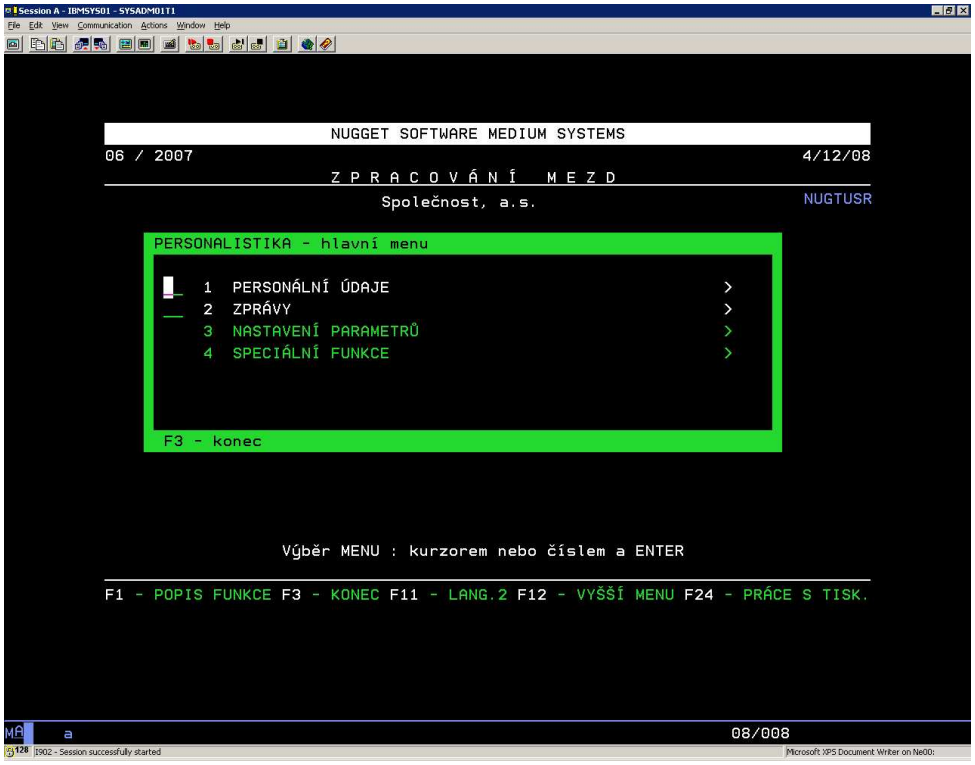
Aplikace ICBS: Anglická verze



Zdroj: Vlastní

Aplikace Nugget: Mzdy a personalistika, terminálový provoz, Nugget SW, s.r.o. - ČR[37], existuje verze pro i5/OS a Windows





Zdroj: Vlastní

[37] http://www.nuggetsw.cz/

Příloha č. 11

Referenční použití systému IBM i v ČR[38]

Tabulka 9 - Rozložení IBM i podle segmentů

Segment	Bankovnictví	Průmysl	Státní instituce	Ostatní	Celkem
Počet severů	39	18	15	216	288

Zdroj: Sales department, IBM ČR

Příklady nasazení systému IBM i v praxi:

- **AMATI - Denak, s.r.o. (Kraslice)**

  Dechové hudební nástroje

  – EVIS/400 (ERP systém)

- **BCPP - Burza cenných papírů Praha, a.s.**

  Organizátor trhu s cennými papíry v ČR

  – Hlavní obchodní aplikace (investiční obchody)

- **ČSOB - Československá obchodní banka, a. s.**

  Bankovnictví

  – IBIS (Bankovní systém pro Corporate)

- **GE Money Bank, a.s.**

  Bankovnictví

  – ICBS (Core bankovní systém)

  – Nugget (Mzdy a personalistka)

- **GPE s.r.o. (dříve Muzo)**

  Bezhotovostní platby

  – Bezhotovostní platby pro banky a finanční instituce v ČR a po celém světě

[38] *http://www.boruvka.cz/vse/01_Prez_200812_VSE_System_IBM_i_Sprava_systemu.ppt*

- **KB - Komerční banka, a.s.**

  Bankovnictví

  - Karetní systém

- **OLMA, a.s.**

  Potravinářství (mléčné výrobky)

  - Řízení technologií

- **Strojimport, a.s.**

  Export a import strojírenských výrobků a zařízení

  - SPECTRUM/400 (ERP systém)

- **Vysoká škola báňská – Technická univerzita Ostrava**
  - Interní informační systém
  - Vědeckovýzkumné aktivity
  - RNDr. Ivo Martiník, Ph.D. (ivo.martinik at vsb.cz)