



INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ

Operační systémy II

Lenka Závodná, Ing.

**Zlepšování podmínek pro využívání ICT ve výuce
a rozvoj výuky angličtiny
na SPŠei Ostrava**

č. projektu CZ.1.07/1.1.07/03.0089

Ostrava 2011

Obor: Informační technologie (18-20-M/01)

Předmět: Operační systémy

Ročník: čtvrtý

Autor: Lenka Závodná, Ing.

Doporučená literatura:

VYCHODIL, Vilém. *Operační systém Linux: příručka českého uživatele*. 1. vyd. Brno: Computer Press, 2003, 260 s. ISBN 80-722-6333-1.

SHAH, Steve. *Administrace systému Linux: jak porozumět svému počítači : podrobný průvodce začínajícího administrátora*. 2. vyd. Praha: Grada, 2003, 533 s. ISBN 80-247-0641-5.

© Lenka Závodná

© Střední průmyslová škola elektrotechniky a informatiky, Ostrava,
příspěvková organizace

OBSAH

Úvod.....	9
1 Správa síťových operačních systémů	10
1.1 Úkoly správce systému.....	10
1.2 Oprávnění správce systému	11
1.3 Nástroje správy	12
2 Rizika práce v síti a jejich minimalizace	14
2.1 Bezpečnostní hrozby a rizika	14
2.2 Bezpečnostní incidenty.....	15
2.3 Bezpečnostní politika, zásady zabezpečení.....	16
2.4 Obecná struktura dokumentu se zásadami zabezpečení.....	17
2.5 Příklad některých typů zásad.....	18
3 SW možnosti zabezpečení	20
3.1 Možnosti zabezpečení.....	20
3.2 Bezpečnostní software	21
3.3 Firewall.....	21
3.4 Některé bezpečnostní technologie používané v síti	22
4 HW možnosti zabezpečení.....	24
4.1 Fyzické zabezpečení	24
4.2 Přepěťové ochrany	24
4.3 Záložní zdroje energie	26
4.4 Zabezpečení dat proti selhání pevného disku RAID	27
5 Virtualizace.....	32
5.1 Co je to virtualizace a její možnosti.....	32
5.2 Vývoj virtualizace.....	33
5.3 Typy virtualizace.....	34
5.4 Výhody virtualizace.....	38
6 Serverová virtualizace	44
6.1 Virtuální počítač.....	44
6.2 Modely serverové virtualizace.....	46
6.3 Hlavní výrobci produktů pro serverovou virtualizaci	47
6.4 Hardwarová náročnost virtualizace serverů	48
7 Synchronizace času v síti	51

7.1	Důvody pro synchronizaci času	51
7.2	NTP (Network Time Protocol)	52
7.3	Konfigurace času	54
8	Proces bootování a inicializace OS.....	59
8.1	Proces bootování systému	59
8.2	Zaváděcí sektor, MBR	60
8.3	BIOS.....	61
8.4	Zavaděč, boot loader	62
8.5	Bootování z jiného média	63
9	Linux: start a konfigurace zavaděče	65
9.1	Start systému	65
9.2	Zavaděče v Linuxu	66
9.3	GRUB Legacy	67
9.4	GRUB 2.....	69
10	Linux: inicializace systému	73
10.1	Proces init.....	73
10.2	Konfigurační soubor /init/tab	73
10.3	Proces init a start systému.....	74
10.4	Run level 1	77
10.5	Run level 0, 6	77
10.6	Startovací skripty: rc skripty	77
11	MS Windows: start systému.....	80
11.1	Před bootovací sekvence	80
11.2	Bootovací sekvence	81
11.3	Bootovací sekvence ve Windows XP.....	82
11.4	Bootovací proces ve Windows Vista, Windows 7, Windows Server 2008	82
11.5	Co se děje po spuštění ntoskrnl.exe	85
11.6	Přihlašovací sekvence, Winlogon.exe.....	85
12	Linux: Konfigurace OS	89
12.1	Skripty	89
12.2	Konfigurace příkazového interpretu bash	90
12.3	Adresář /etc	91
12.4	Adresář /dev	92
12.5	Souborový systém /proc	92

13	MS Windows: Registry	96
13.1	Co je to registr	96
13.2	Struktura registru	97
13.3	Zabezpečení registru	100
14	Windows: práce s registry	102
14.1	Editor registrů	102
14.2	Funkce regedit	103
14.3	Řízení přístupu k registru	104
14.4	Další nástroje pro práci s registry	105
15	Konfigurace síťového rozhraní, sítě	108
15.1	Síťové rozhraní	108
15.2	IP adresy	109
15.3	Subnetting	111
15.4	Adresy rezervované pro privátní sítě	112
15.5	Konfigurace sítě	113
16	Linux: konfigurace síťového rozhraní	116
16.1	Detekce ovladače pro síťovou kartu	116
16.2	Konfigurace sítě	117
16.3	Nastavení sítě pomocí nástroje ip	119
16.4	Konfigurační soubory (Gentoo)	120
17	MS Windows: konfigurace síťového rozhraní	123
17.1	Konfigurace síťové karty v MS Windows	123
17.2	Nastavení síťového rozhraní	123
17.3	Síťové rozhraní a příkazová řádka	127
18	Autentizace a autorizace uživatele	130
18.1	Autentizace na základě hesla	130
18.2	Bezpečné heslo	131
18.3	Jiné způsoby autentizace	133
18.4	Pokročilé způsoby identifikace a ověřování	133
18.5	Autorizace uživatele	134
19	Linux: proces přihlašování, organizace a správa účtů,	137
19.1	Přihlášení uživatele	137
19.2	Uživatelský účet	138
19.3	Vytvoření a modifikace účtu	140

19.4	Heslo v Linuxu	141
19.5	Logování přihlašování uživatele.....	142
20	Linux: přístupová práva	144
20.1	Základní přístupová práva	144
20.2	Speciální přístupová práva: t-bit a s-bit.....	146
20.3	Umask	147
20.4	ACC: access list, rozšířená práva	147
21	OS Windows: Organizace a správa účtů.....	152
21.1	Pracovní skupiny a domácí skupiny, domény	152
21.2	Místní a doménové uživatelské účty	153
21.3	Uživatelské účty a účty počítačů v doméně	155
21.4	Výchozí uživatelské účty.....	155
21.5	Vytvoření místního uživatelského účtu.....	156
22	OS Windows: Skupiny a zvláštní identity	160
22.1	Uživatelské skupiny lokální a doménové	160
22.2	Postup tvorby skupin	162
22.3	Výchozí skupiny.....	162
22.4	Místní (lokální) skupiny	163
22.5	Doménové skupiny	164
22.6	Zvláštní identity	165
23	OS Windows: Práva a oprávnění	169
23.1	Práva a oprávnění	169
23.2	Oprávnění k souborům a složkám	169
23.3	Dědičnost	171
23.4	Řízení uživatelských účtů – UAC.....	171
24	MS Windows: profily uživatelů.....	175
24.1	Uživatelské profily, funkce, rozdělení.....	175
24.2	Vytvoření a aktualizace cestovního profilu	176
24.3	Povinný cestovní profil – Mandatory Profil	177
25	Správa souborových systémů	179
25.1	Logická struktura disku.....	179
25.2	LVM (Logical Volume Management).....	180
25.3	Co je to souborový systém	181
25.4	Zabezpečení dat.....	181

25.5	Kvóty (anglicky <i>quota</i>)	182
25.6	Co je úkolem správy FS.....	182
26	OS Linux: Správa FS.....	184
26.1	Disk, diskové oddíly v Linuxu.....	184
26.2	Programy pro práci s diskovými oddíly	185
26.3	Připojování a odpojování FS.....	187
26.4	Utility pro práci s oddíly.....	188
26.5	Přístup na linuxové disky z Windows.....	188
27	MS Windows: Správa FS	194
27.1	Správa sdílených složek: Nástroj Sdílené složky	194
27.2	Správa disků a svazků.....	194
27.3	Správce prostředků souborového serveru	197
27.4	Zálohování serveru.....	197
28	Instalace OS, aplikací (MS Windows, Linux).....	199
28.1	Instalace SW	199
28.2	Instalace OS.....	201
28.3	Způsoby instalace.....	202
28.4	Instalace OS Linux	203
28.5	Instalace OS Windows.....	204
28.6	Novell SUSE LINUX Enterprise Server: HW požadavky	204
29	Linux: síťové služby, konfigurace	207
29.1	Spuštění služeb	207
29.2	Superserver inetd, xinetd.....	207
29.3	Konfigurace inetd.....	208
29.4	Kontrola přístupu ke službám pomocí tcp_wrappers.....	210
29.5	Konfigurace xinetd.....	211
29.6	Kontrola přístupu ke službám	212
29.7	Soubory services a protocols.....	213
30	MS Windows: Správa počítače, služby	217
30.1	Služby Windows Server.....	217
30.2	Služby systému Windows 7	219
30.3	Spuštění a zastavení služby	222
30.4	Služby v OS Windows a příkazový řádek	223
31	Adresářové služby, LDAP	225

31.1	Adresářová služba	225
31.2	LDAP: Protokol pro adresářové služby	226
31.3	Informační model	227
31.4	Jmenný model	228
31.5	Funkční model	229
31.6	Bezpečnostní model	229
32	MS Windows: Active Directory	232
32.1	Active Directory	232
32.2	Logická struktura	233
32.3	Fyzická struktura	235
32.4	Globální katalog GC	236
33	MS Windows: Politiky, zásady zabezpečení	239
33.1	Zásady zabezpečení (politiky/ policy)	239
33.2	Doménové politiky, Group Policy	240
33.3	Politika hesel (Password Policy)	241
34	OS Novell NetWare/NOES: eDirectory	245
34.1	Od NDS k eDirectory	245
34.2	Základní vlastnosti eDirectory	245
34.3	Instalace	246
34.4	Správa eDirectory	247
34.5	Nástroje pro správu	248
34.6	Objekty v eDirectory	249
35	Licenční politiky v OS	252
35.1	Co je to licence?	252
35.2	Některé licence pro „svobodný“ software	253
35.3	Licenční politika Microsoft	254
35.4	Krabicový produkt FPP (<i>Full Package Product</i>)	254
35.5	OEM licence	254
35.6	Multilicenční programy	255
35.7	Licenční politika pro produkty Novell	256

Vysvětlivky k používaným symbolům



Obsah hodiny – popisuje náplň hodiny



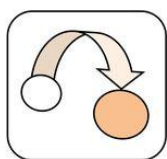
Cíl hodiny – specifikace dovedností a znalostí, které si studující osvojí během hodiny



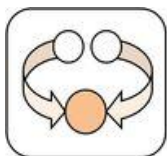
Klíčová slova – nové pojmy, specifické termíny či cizí slova, jejichž význam je v textu vysvětlen



Definice – definování a vysvětlení nového pojmu či jevu



Příklad – objasnění nebo konkretizování problematiky na příkladu ze života, z praxe, ze společenské reality apod.



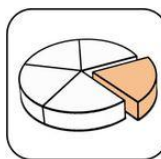
Shrnutí – shrnutí probrané látky, shrnutí kapitoly



Kontrolní otázky a úkoly – prověřují, do jaké míry studující text a problematiku pochopil, zapamatoval si podstatné a důležité informace a zda je dokáže aplikovat při řešení problémů



Otázky k zamyšlení - úkoly rozšiřující úroveň základních znalostí



Literatura – literatura a zdroje pro doplnění a rozšíření poznatků kapitoly

Úvod

Výukový modul Operační systémy II je zaměřen na seznámení s problematikou operačních systémů (dále OS) v rozsahu předmětu Operační systémy (dále jen OPS) čtvrtého ročníku oboru Informační technologie.

Učivo OPS 4. ročníku je zaměřeno na to, aby se studující seznámili s operačními systémy z pozice správců. Cílem výuky je zvládnout základy správy a konfigurace nejrozšířenějších síťových operačních systémů (MS Linux, MS Windows, Novell NetWare), a jejich základních síťových služeb. Výukový modul Operační systémy II je výukovou oporou pro teoretickou část výuky.

Učivo navazuje na znalosti a dovednosti, které žáci získali v předmětu OPS ve třetím ročníku a je dále provázáno s předměty Počítačové sítě (POS) ve třetím a čtvrtém ročníku.

Studující se v tomto modulu seznámí se základními pojmy z oblasti instalace, konfigurace operačních systémů, správy uživatelů, souborových systémů vytváření účtů, síťových služeb (charakteristika, instalace, konfigurace).

1 Správa síťových operačních systémů

Obsah hodiny



Obsahem této hodiny je vysvětlení významu správce síťových OS a jeho povinnosti.

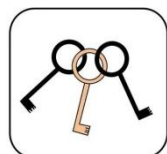
Cíl hodiny



Po prostudování budete schopni:

- vysvětlit význam a funkci správce OS,
- specifikovat povinnosti správce OS,
- charakterizovat účty pro správu v jednotlivých OS,
- vysvětlit používání příkazů su a sudo v unixových systémech.

Klíčová slova



Administrace, Administrátor, Oprávnění, Uživatel root, system, admin, administrator, Příkazy su, sudo

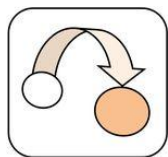
1.1 Úkoly správce systému

„Úlohou správného správce systému a sítě je pouze mít nohy na stole a sledovat, jak je vše správně nastaveno a nakonfigurováno, sledovat hladce běží provoz.“

Teď si asi řeknete: „Super. To je přesně to, co chci dělat!“ Jenže tomuto ideálnímu stavu předchází spousta práce.

Aby operační systém bezchybně pracovat, musí být vše správně nainstalováno, nakonfigurováno. Pro pravidelné činnosti vytvořeny skripty tak, aby systém vyžadoval co nejméně „ruční práce“ správce. Počítače navíc nepracují samy, používají je lidé, kteří většinou o nich nic neví. A i když správce vytvoří řadu směrnic, důkladně uživatele vyškolí, je víc než pravděpodobné, že dříve nebo později (většinou dříve), budou potřebovat jeho pomoc.

Encyklopedie profesí definuje pozici „Správce operačních systémů a sítí“ poněkud seriózněji:



„Správce operačních systémů a sítí nastavuje parametry operačních systémů počítačů a počítačových sítí. Má za úkol zajistit funkčnost a bezpečnost během provozu celého výpočetního systému nebo sítě. Přebírá, ověřuje, uvádí do provozu a nastavuje parametry operačních systémů a počítačových sítí. Monitoruje a diagnostikuje provoz operačních systémů i počítačových sítí. Optimalizuje využívání operačních systémů, zajišťuje antivirovou ochranu a kompletní zálohování. Implementuje firemní a systémové aplikace. Detekuje chyby a vady sítí a jejich jednotlivých systémů. Součástí jeho práce je i vedení podrobné dokumentace.“

Správa systému (administrace) tedy zahrnuje řadu činností jako je:

- analýza a návrh hardware a software pro použití v malé organizaci,
- instalace operačního systému a jeho konfigurace,
- instalace a správa klientského software,
- implementace firemních a systémových aplikací,
- instalace periférií a jejich konfigurace,
- správa uživatelských účtů a monitorování činnosti uživatelů,
- správa a údržba souborových systémů, archivace, zálohování,
- správa a konfigurace síťových služeb a síťových připojení,
- monitorování provozu OS, jejich diagnostika, optimalizace výkonu,
- detekování chyb a vad sítí a jejich jednotlivých systémů,
- zabezpečení dat před zneužitím,
- ochrana dat před zničením,
- vedení provozní dokumentace o využívaném software za účelem dodržování autorských práv v této oblasti,
- definování problémů uživatelů a jejich řešení,
- formulování zásad bezpečnosti zabezpečení, kontrola jejich dodržování,
- školení uživatelů v oblasti využívání informačních systémů a bezpečnosti.

1.2 Oprávnění správce systému

Pro správce systému nejsou v OS nastavena oprávnění a jiná omezení, která jsou jinak pro běžné uživatele limitující. V některých případech však může být i správce omezen, ale tato omezení může jednoduše zrušit.

V systémech Windows jsou tato omezení oproti Unixovým OS ve větším rozsahu. Například správce (*Administrator*) nemůže přistupovat do adresáře, do kterého nemá nastavena oprávnění, musí nejprve převzít vlastnictví a oprávnění si pak může přidělit.

V Unixových systémech je účet správce nazván *root*. Jeho vlastnické identifikátory *UID* i *GID*¹ jsou 0 (nula). Omezení oprávnění je jen ve speciálních případech, například *root* nemůže manipulovat se souborem, který má nastaven atribut *immutable bit* (pomocí příkazu *chattr*).

Protože *root* má v podstatě neomezený přístup do systému, doporučuje se a je běžné, že řadu činností provádí přes dočasné oprávnění. Správce jako uživatel má možnost získat dočasně *root* oprávnění pomocí příkazů ***sudo*** nebo ***su***. V moderních distribucích Linuxu bývá dokonce znemožněno se přihlásit pod účtem *root* (z důvodu bezpečnosti).

Příkaz *su* (*Substitute User identity*) slouží v Unixových systémech k přepnutí uživatele na jiného uživatele. Pro zajištění své činnosti využívá speciální oprávnění *SUID*.

Příkaz *sudo* (*substitute user do*) je užívaný v Unixových OS k vykonání operace s oprávněními jiného uživatele. Převážně je tím uživatelem *root*. Při přístupu přes účet jiného uživatele příkazem *sudo*, je vyžadována autorizace, tj. dotazování na vlastní heslo. Lze však nastavit dotazování na heslo uživatele, jehož oprávnění se bude používat, nebo aby se nemuselo zadávat heslo vůbec, což není z bezpečnostních důvodů vhodné.

Příkazy *su* a *sudo* se používají v příkazovém řádku, existují ale i podobné příkazy pro grafické rozhraní: *kdesu* pro prostředí *KDE* a *gksudo* pro prostředí *GNOME*.

V OS řady Windows NT (tj. Windows XP, Windows 7 a výše) je správcem systému účet *Administrator*. Existuje ještě skrytý uživatel pojmenovaný *SYSTEM*, který může provádět mnoho operací navíc přímo bez varovných hlášek. Správce může získat maximální oprávnění utilitou třetí strany zvanou *psexec*. Výsledek se blíží Unixovému *rootu*.

V systému Novell NetWare byl účet správce systému pojmenován, *admin* s právem *S supervisor*, což znamená nejvyšší oprávnění.

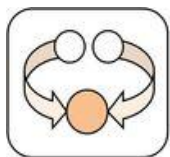
1.3 Nástroje správy

Úkoly správy lze provádět pomocí jednoho, dvou nebo všech tří následujících typů nástrojů pro správu:

- nástrojů založených na grafickém uživatelském rozhraní (GUI),
- nástrojů založených na příkazovém řádku,
- skriptů nebo nástrojů založených na skriptech.

¹ *UID* je identifikační číslo uživatele, *GID* je identifikační číslo základní skupiny uživatele, jsou uvedeny v */etc/passwd*

Shrnutí kapitoly



Správce (administrátor) OS musí provádět řadu činností (administrace systému), aby počítačový systém zůstal v provozuschopném stavu.

V každém OS má správce zřízený účet, který disponuje oprávněním, které odstraňuje omezení běžných uživatelů. V OS Unixových disponuje správce účtem root (UID, GID = 0) s minimálním omezením, proto řadu činností provádí přes dočasné oprávnění pomocí příkazů **sudo** nebo **su**.

V systémech Windows je účet správce *Administrator* více omezen, ale může si chybějící oprávnění podle potřeby přidělit. Menší omezení má pak skrytý uživatel *SYSTEM*.

V systému Novell NetWare má účet správce systému admin s právem *S supervisor*.

Kontrolní otázky a úkoly



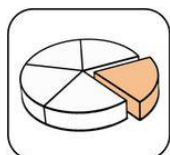
- 1) Co je cílem správce OS?
- 2) Jak byste charakterizovali účet správce OS v jednotlivých systémech?
- 3) Jaké povinnosti má správce OS
- 4) Jaký význam mají příkazy su sudo v unixových systémech?

Otázky k zamyšlení



- 1) Co je bezpečnostním rizikem neomezeného účtu?

Použitá literatura a jiné zdroje:



- [1] Správce operačních systémů pro malé a střední organizace: Odborná způsobilost. MINISTERSTVO PRŮMYSLU A OBCHODU. www.narodni-kvalifikace.cz [online]. 31.3.2011 [cit. 2012-01-29]. Dostupné z: <http://www.narodni-kvalifikace.cz/detailKvalifikacnihoStandardu.aspx?id=365>
- [2] Správce operačních systémů a sítí: Encyklopedie profesí. Prace.cz [online]. 1996 - 2012 [cit. 2012-01-29]. Dostupné z: <http://www.prace.cz/poradna/encyklopedie-profesi/s/spravce-operacnich-systemu-a-siti/>

2 Rizika práce v síti a jejich minimalizace

Obsah hodiny



Obsahem této hodiny je problematika bezpečnostních rizik v informačních systémech a jejich minimalizace vytvořením bezpečnostní politiky organizace.

Cíl hodiny



Po prostudování budete schopni:

- identifikovat bezpečnostní hrozby a rizika,
- popsat proces tvorby bezpečnostní politiky firmy,
- charakterizovat strukturu dokumentu se zásadami zabezpečení,
- orientovat se v nejběžněji používaných zásadách zabezpečení.

Klíčová slova



Bezpečnostní hrozba, riziko, incident, Analýza rizik, Bezpečnostní politika, Certifikační audit

2.1 Bezpečnostní hrozby a rizika

Informace mají svoji cenu. Je třeba je zabezpečit před zneužitím a ochránit před poškozením, zničením.

Hrozby lze dělit na:

- **Objektivní:**
 - Přírodní, fyzické jako např. požár, povodeň, výpadek napětí, poruchy. Jejich prevence obtížná, řeší se spíše možnost minimalizace dopadů a obnovy prostřednictvím havarijního plánu.
 - Fyzikální: např. elektromagnetické vyzařování.
 - Technické: chyby HW, SW, krádež, resp. zničení paměťového média, nebo nedokonalé zrušení informace na něm.
- **Subjektivní:** tj. hrozby plynoucí z lidského faktoru:
 - **Neúmyslné:** např. působení nevyškoleného uživatele či správce IS.

- **Úmyslné:** vnější útočníci (např. špióni, teroristé, konkurenti, hackeři) nebo vnitřní útočníci (propuštění, rozzlobení, vydírání, chamtiví zaměstnanci).

Při zavádění a provozu počítačové sítě a informačního systému je nutné analyzovat rizika, tj. definovat a identifikovat potencionální hrozby, odhalit zranitelná místa.

Analýza rizik je tedy aktivitou v procesu řešení bezpečnosti. Musí poskytnout odpověď na následující tři základní otázky:

- Co se stane, když nebudou informace chráněny?
- Jak může být porušena bezpečnost informací?
- S jakou pravděpodobností se to stane?

Výstupem je dokument „Analýza rizik“ obsahující popis systému a výsledky analýzy. Tedy úroveň hrozeb, zjištěné zranitelnosti, úroveň stávajících ochranných opatření.

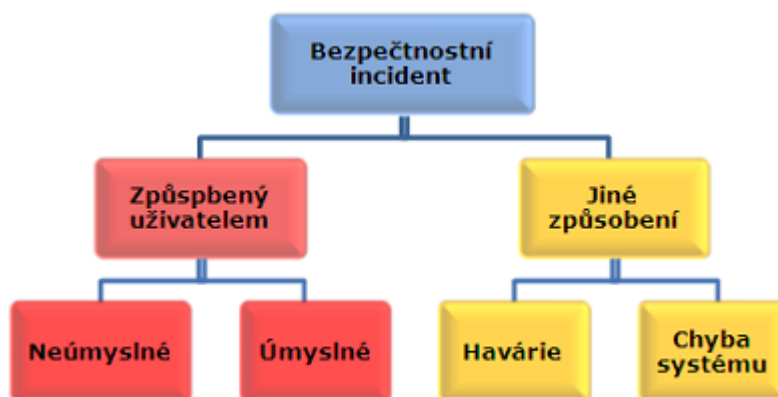
Na základě analýzy rizik je možno vytvořit souhrn doporučených protiopatření k jejich minimalizaci, zpracovat bezpečnostní politiku organizace.

Ochrana proti rizikům je i otázkou peněz. Čím vyšší míra zabezpečení, tím jsou vyšší náklady. Při návrhu vhodných protiopatření je třeba stanovit, zda náklady nejsou vyšší než rizika. Velkou roli tady hraje cena informací, dat, která potřebujeme chránit. Je třeba dosáhnout takové úrovně zabezpečení, aby vynaložené náklady nepřevýšily možné ztráty, ke kterým může v důsledku uskutečnění hrozby dojít.

Při hodnocení možných následků (ztrát) je třeba zvážit přímé ztráty v materiální i duchovní podobě (např. vyzrazení obchodních záměrů, výsledků výzkumu, náklady na obnovení ztracených informací či obnovení výroby). A je třeba vzít do úvahy i ztráty nepřímé, týkající se například ztráty dobrého jména podniku, nedodržení závazků termínů, atd.

2.2 Bezpečnostní incidenty

Bezpečnostní incident je situace, kdy už dojde k poškození či ztrátě datových souborů, vyřazení systému z provozu, rozšíření počítačových virů v síti nebo průniku do IS.



Obrázek 2-1: Bezpečnostní incidenty

Pokud bezpečnostnímu incidentu dojde, je třeba

- vyšetřit jeho příčinu,
- podrobně analyzovat,
- odstranit nebo alespoň minimalizovat důsledky a
- uskutečnit opatření zamezující možnosti opakování.

2.3 Bezpečnostní politika, zásady zabezpečení

Bezpečnost nelze omezit pouze na řešení technologické úrovně jako je nasazení bezpečnostních technologií včetně jejich konfigurace. Je třeba pamatovat na to, že jedním z největších rizik je člověk a řešit bezpečnost na úrovni organizační. Zformulovat a zavést řadu pravidel a zásad, vysvětlit je uživatelům a dbát na jejich dodržování. Za tím účelem se vytváří dokument popisující zásady zabezpečení.

Je to dokument vytvořený na základě „Analýzy rizik“ schválený nejvyšším vedením organizace a závazný pro celou organizaci. Jsou v něm deklarovány zásady zabezpečení v oblasti informační bezpečnosti.

„Zásady zabezpečení“ určují jaké chování je a není uvnitř a vně sítě přípustné.

- Musí mít písemnou formu.
- Musí být závazná v celé organizaci, platit pro všechny úseky, zaměstnance a vedoucí pracovníky.
- Musí být známá všem, kterých se týká.
- Musí být schválena na úrovni vrcholového managementu organizace.
- Plnění musí být vynutitelné, jinak nemá smysl.

Existují dva přístupy k formulaci politiky informační bezpečnosti organizace

- Stručná bezpečnostní politika,
- Detailní bezpečnostní politika.

Stručná bezpečnostní politika (3-5 stran) obsahuje pouze základní zásady, a to:

- vysvětlení pojmu „informační bezpečnost“,
- deklaraci, že vedení organizace politiku informační bezpečnosti, podporuje a vyžaduje od všech její plnění,
- stanovení organizační a odpovědnostní struktury informační bezpečnosti a definování povinností,
- způsob řízení, kontroly a dokumentace informační bezpečnosti.

Detailní bezpečnostní politika (desítky stran) obsahuje jednotlivá bezpečnostní opatření platná pro celou organizaci. Detailní politika by měla ve zvolené míře podrobnosti obsáhnout celý systém řízení a správy informační bezpečnosti.

Nejdůležitější je samozřejmě zavedení bezpečnostní politiky (všech pravidel a standardů) do praxe. Dále je nutno průběžně monitorovat stav jejich plnění.

Jednorázově se provádí **audit** (jednorázové hodnocení). Jedná se o analýzu požadavků, rizik a hodnocení současného stavu zabezpečení. Obvykle jej provádí nezávislá specializovaná firma.

Pokud je úspěšně vybudován a provozován systém řízení informační bezpečnosti, lze přistoupit k jeho certifikaci (**certifikační audit**). Certifikace představuje zhodnocení systému řízení informační bezpečnosti (ISMS - Information Security Management System) nezávislou organizací, která má k této činnosti náležitá oprávnění. Certifikát se vydává na tři roky. Celý proces certifikace se řídí normou ISO/IEC 27001.

2.4 Obecná struktura dokumentu se zásadami zabezpečení

- Oddíl 1 Celkový přehled (důvod a vymezení rizik)
- Oddíl 2 Účel dokumentu (účelem je stanovit pravidla přípustného využívání počítačového vybavení z důvodu ochrany firmy, zaměstnanců před ...)
- Oddíl 3 Působnost (pro jaké skupiny zaměstnanců, zařízení: zaměstnance, dodavatele, konzultanta, dočasného pracovníka, ..., pro zařízení ve vlastnictví firmy, pronajatá zařízení, ...)
- Oddíl 4 Vlastní zásady (jednotlivá pravidla, vysvětlení ilustrace)
- Oddíl 5 Uskutečňování zásad (postihy za porušení)

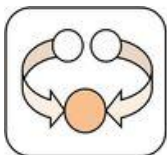
- Oddíl 6 Definice pojmů
- Oddíl 7 Historie revizí (datum, popis a důvod každé provedené změny)

2.5 Příklad některých typů zásad

Přehled nejdůležitějších a nejběžněji používaných zásad, jejich definování je k dispozici na <http://www.sans.org/security-resources/policies/>.

- Zásady přípustného užívání:
 - přípustné šifrování,
 - přípustné užívání – osoby, které smí používat počítače firmy,
 - přípustné využívání telefonních linek.
- Požadavky na poskytovatele aplikačních služeb.
- Oprávnění vykonávat audit a monitorování systému.
- Požadavky na přístupové informace:
 - ukládání a načítání uživatelských jmen a hesel,
 - standardy pro vytvoření silného hesla,
 - ochrana hesla,
 - frekvence změn hesla.
- Pravidla pro vzdálený přístup.
- Určuje citlivost informací.
- Antivirová ochrana.
- Zabezpečení:
 - směrovačů a prepínačů,
 - serverů,
 - VPN,
 - bezdrátové komunikace.

Shrnutí kapitoly



Informace mají svoji cenu. Je třeba je zabezpečit před zneužitím, ochránit před poškozením, zničením.

Hrozby lze rozdělit objektivní (přírodní, fyzické, fyzikální, technické) a subjektivní (lidský faktor), úmyslné a neúmyslné. Pokud dojde k bezpečnostnímu incidentu, je třeba minimalizovat jeho důsledky a postarat se o to, aby se neopakoval.

Při zavádění a provozu počítačové sítě a informačního systému je nutné analyzovat rizika a vytvořit bezpečnostní politiku organizace, dbát o její zavedení do praxe a dodržování. K tomu slouží monitorování a audity.

Systém řízení informační bezpečnosti lze na tři roky certifikovat - ISM certifikát.

Kontrolní otázky a úkoly



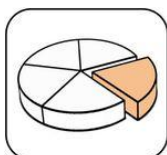
- 1) Jak dělíme bezpečnostní hrozby?
- 2) Jak se hodnotí systém řízení informační bezpečnosti?
- 3) Co je to analýza rizik?
- 4) Jaké jsou následky porušení bezpečnosti?
- 5) Co je to bezpečnostní incident?
- 6) Jaká je struktura dokumentu se zásadami zabezpečení?
- 7) Jaké zásady se definují v rámci bezpečnostní politiky?

Otázky k zamyšlení



- 1) Jakou roli v bezpečnosti má lidský faktor?

Použitá literatura a jiné zdroje:



- [1] MINISTR, Jan. STŘEDNÍ ODBORNÁ ŠKOLA OCHRANY OSOB A MAJETKU S.R.O. Informační bezpečnost [online]. Karviná, 2011 [cit. 2012-02-03]. Dostupné z: <http://www.ivosoom.cz/aktivity4.php>
- [2] M. THOMAS, Thomas. Zabezpečení počítačových sítí bez předchozích znalostí. první. Brno: CP Books, a.s., 2005. ISBN 80-251-0417-6.

3 SW možnosti zabezpečení

Obsah hodiny



Obsahem této hodiny je nástin možností SW zabezpečení počítačů a serverů v síti, síťového provozu.

Cíl hodiny



Po prostudování budete schopni:

- orientovat se v možnostech SW zabezpečení,
- orientovat se v technologiích zabezpečení síťového provozu.

Klíčová slova



Firewall, Antimalware, Filtrování paketů, obsahů, NAT, Proxy, Technologie AAA

3.1 Možnosti zabezpečení

Pro ochranu počítačových sítí se používá řada bezpečnostních technologií a produktů. Patří mezi ně především:

- antivirový a další bezpečnostní sw,
- síťové bezpečnostní technologie,
- používání VPN (Virtuální privátní síť),
- firewall, stínící směrovač, proxy server,
- biometrické snímače.

Bezpečnost jsou nejen různé bezpečnostní technologie a produkty, ale je to především řada procesů, činností, např.:

- Správná konfigurace operačního systému, software, síťových služeb, firewallu.
- Aktualizace operačního systému (záplaty), aplikací, antivirových programů.
- Pravidelné zálohování, archivace dat.
- Školení uživatelů.
- Kontrola dodržování bezpečnostní politiky.

3.2 Bezpečnostní software

Základní ochranu jednotlivých počítačů zajišťuje bezpečnostní software. Jsou to programy a aplikace umožňující ochranu počítače. Na každém počítači by neměly chybět dva základní typy:

- firewall,
- antimalware.

Nainstalovaný a dobře nakonfigurovaný firewall (fw) představuje bariéru (zeď) mezi počítačem a sítí, ke které se chcete připojit. Poskytuje ochranu před útokem „zvenčí“, zabraňuje průchodu nechtěných přenosů. Primárním úkolem fw detekovat a blokovat. Je nutná jeho správná konfigurace.

Komplexním SW, který primárně chrání váš počítač před malware, jsou antivirové systémy. Disponují řadou nástrojů pro detekci a identifikaci malware (nejen virů). Je opět nutná správná konfigurace a pravidelná aktualizace.

3.3 Firewall

Firewall může být řešen hardwarově nebo softwarově. Poskytuje pravidla pro filtrování příchozích a odchozích paketů a rozhoduje (na základě pravidel nastavených systémovým administrátorem), zdali může paket propustit na cílovou adresu.

Firewall je obvykle umístěn na síťové bráně, což je místo, kde je jedna síť propojena s další sítí.

Tři základní typy filtrování, prováděného firewallem:

- filtrování paketů,
- filtrování spojení,
- filtrování aplikací.

Filtrování paketů filtruje přenášené datové pakety podle informací v jejich hlavičce podle použitého přenosového protokolu (IP, TCP/UDP a ICMP). Filtrováním paketů lze uvolnit nebo zablokovat specifické IP adresy nebo čísla portů.

Filtrování spojení je založeno na filtrování spojení souvisejících s již navázaným spojením. Pokud paket není součástí navázaného spojení, nebude propuštěn skrze firewall.

Filtrování aplikací filtruje protokoly odpovídající určitým aplikacím. Například zablokovat Java applety nebo skripty jazyka Visual Basic.

Hardwarovým firewall je vyhrazené zařízení, na kterém běží vlastní operační systém. Tyto počítače fungují pouze jako firewall a proto jsou

rychlejší a stabilnější než počítače, na kterých běží softwarový firewall a na kterých se souběžně pracuje.

3.4 Některé bezpečnostní technologie používané v síti

Filtrování paketů v přístupových seznamech (ACL)

Paketové filtry na směrovači tvoří první obrannou linii. Po provedení kontroly paketu se na něj aplikují určitá pravidla a podle nich se paketu povolí nebo zakáže průchod. Pravidla se zapisují do ACL (Access Control List), přeloženo to znamená přístupový seznam. Jedná se vlastně o seznam zakázaných (deny) nebo povolených (permit) IP adres. Právě podle těchto IP adres se provádí filtrování paketů.

ACL se zpracovává shora dolů. Jako první se uvádí pravidla zmítavá, vždy musí být nějaká pravidla povolovací, jinak neprojde nic, protože na konci seznamu musí být implicitní zamítavé pravidlo: nic jiného nepouštěj.

Překlady síťových adres – NAT

Smyslem NAT mechanismu je převedení IP adresy privátní na veřejnou. Zavádí se na firewallu, směrovači nebo počítači, který je mezi privátní a veřejnou sítí.

Proxy a ochrana na úrovni aplikací

Proxy firewallly a proxy servery vstupují do komunikace jako prostředníci, kontrolují každé spojení. Proxy zkontroluje paket, označí spojení za povolené, a otevře nové spojení a odešle paket. Provoz je filtrován podle stanovených aplikačních pravidel

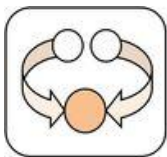
Filtrování obsahu

Jedná se o filtrování nad síťovým připojením. Používá se pro omezení přístupu na stránky s nevhodným obsahem, při kontrole elektronické pošty. Pomocí obsahového filtru lze detekovat spamy, kontrolovat přílohy na přítomnost virů apod.

Technologie AAA: Autentizace - Autorizace – Účtování (Accounting)

Přístup ke službám je umožněn na základě Autentizace, tj. ověření totožnosti na základě přihlašovacího jména a hesla. Po přihlášení následuje Autorizace – stanovení oprávnění, na základě přístupových práv a poslední A znamená sběr informací – Účtování (Accounting). O přihlášeném uživateli se zaznamenávají informace o jím prováděných operacích.

Shrnutí kapitoly



Pro ochranu počítačových sítí se používá nejen řada bezpečnostních technologií a produktů, ale především řada procesů, činností:

Základní ochranu počítačů zajišťuje bezpečnostní software:

- firewall,
- antimalware.

Některé bezpečnostní technologie používané v síti

- filtrování paketů v přístupových seznamech (ACL),
- překlady síťových adres – NAT,
- proxy a ochrana na úrovni aplikací,
- filtrování obsahu,
- technologie AAA: Autentizace - Autorizace – Účtování (Accounting).

Kontrolní otázky a úkoly



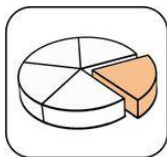
- 1) Jmenujte nejčastěji používané bezpečnostní technologie a produkty?
- 2) Co je základním bezpečnostním softwarem?
- 3) Charakterizujte firewall a jeho možnosti?
- 4) Jaké bezpečnostní technologie se používají v síti?

Otázky k zamyšlení



- 1) Jakou roli v bezpečnosti má lidský faktor?

Použitá literatura a jiné zdroje:



- [1] M. THOMAS, Thomas. Zabezpečení počítačových sítí bez předchozích znalostí. Brno: CP Books, a.s., 2005. ISBN 80-251-0417-6.

4 HW možnosti zabezpečení

Obsah hodiny



Obsahem této hodiny je nástin možností HW zabezpečení počítačů a serverů v síti, síťového provozu.

Cíl hodiny



Po prostudování budete schopni:

- orientovat se v možnostech HW zabezpečení,
- popsat technologii RAID.

Klíčová slova



Přepětové ochrany, UPS, RAID

4.1 Fyzické zabezpečení

Ve vysoce zabezpečeném prostředí by měly být:

- Servery a přípojná zařízení uchovávána za zamčenými dveřmi.
- Pracovní stanice v nezabezpečených prostorách by měly mít nainstalovaný kontrolní software, který by v případě nutnosti zabránil v přístupu k citlivým datům na síti.
- Síťová kabeláž by měla být vedena pevnými instalačními lištami nebo rourami, aby nebylo možné se na ni napíchnout.
- Bezpečná likvidace datových nosičů.

4.2 Přepětové ochrany

Každým rokem dochází z velké části ke ztrátám nebo poškození dat z důvodu přepětí v elektrorozvodné síti nebo z důvodu výpadku proudu.

Přepětí je napětí, které přesahuje nejvyšší hodnotu provozního napětí v elektrickém obvodu.

Vzniká přímo, působením silného elektromagnetického pole např. při přímém nebo blízkém úderu blesku², v blízkém okolí silných vysílačů nebo radiolokátorů, při explozi nukleárních náloží nebo nepřímo, souběhem s jinými vodiči a kabelem, ke kterým jsou připojeny tzv. zdroje rušení³.

Mezi nejvýraznější a nejškodlivější patří pulzní přepětí. Jedná se o krátkodobé přepětí, trvající řádově nanosekundy až milisekundy. Ohrožuje zvláště elektronická zařízení obsahující polovodičové součásti.

Pulzní přepětí tak podle původu rozlišujeme na:

- atmosférická přepětí (LEMP – Lighting ElektroMagnetic Pulse),
- přepětí způsobená nukleárními výbuchy (NEMP–Nuclear ElektroMagnetic Pulse).
- spínací přepětí (SEMP – Switching ElektroMagnetic Pulse),
- přepětí vzniklá při výbojích statické elektřiny (ESD – ElektroStatic Discharge),

Kvalitní ochranu elektronických a elektrických zařízení proti účinkům nebezpečného pulzního přepětí poskytuje systém přepětiových ochran. Instalace přepětiových ochran je prevencí proti možným škodám.

Zdánlivě nemalé náklady na přepětiové ochrany bývají mnohdy pouze zlomkem procenta pořizovací hodnoty chráněné techniky a nepatrnou částkou k možným škodám zaviněným výpadky a zničením technologického zařízení.

Přepětiové ochranné zařízení (SPD – Surge Protective Device) zamezuje nebo omezuje vznik přepětí, nebo vzniklé přepětí a jeho účinky snižuje na míru bezpečnou pro chráněné zařízení.

Přepětiová ochranná zařízení se rozdělují do tří stupňů. Aby ochrana byla dostatečně účinná, doporučuje se používat všechny tři stupně.

SPD T1, (1. stupeň, třída B), hrubá ochrana, tj. svodiče bleskového proudu při přímých úderech blesku. (např.bleskojistky, jiskřiště) Tyto

² Při přímém úderu blesku do elektrovedného (silového) kabelu cca 50% bleskového proudu odečte z místa úderu proraženou izolací kabelu do země. Zbylých 50% bleskového proudu se přibližně rovnoměrně rozdělí na dva proudy, tekoucí z místa úderu blesku na obě strany, tj. cca 25% ke každému konci zasaženého kabelu.

V místě vniku bleskového proudu do sdělovacího (výjimkou silových kabelů) kabelu dojde k podobnému rozdělení zbytkového proudu jako u silového kabelu s tím rozdílem, že žil ve sdělovacím kabelu je podstatně více než v silovém kabelu. Tím se celková hodnota bleskového proudu tekoucího ke chráněným přístrojům rozdělí na n dílů (n =počet žil v zasaženém kabelu).

³ Elektrické přístroje, které kromě svojí řádné činnosti vytvářejí "navíc" ve vodičích, ke kterým jsou připojeny rušivé vlny napětí a proudů (špatné připojení, zhoršení technických parametrů)

ochrany zachytí největší díl přepěťové vlny, instalují se buď do hlavních přípojných skříní (HPS) na venkovní straně obvodové zdi nebo do hlavního rozvaděče uvnitř objektu.

SPD T2, (2. stupeň, třída C), střední ochrana: svodiče přepětí konstruované na bázi varistorů schopné svádět pulzní přepětí. Obvykle se instalují do podružných rozvaděčů, případně do hlavního (spolu s SPD T1).

SPD T3, (3. stupeň, třída D), jemná ochrana: svodiče sloužící k ochraně jednotlivých spotřebičů nebo skupin spotřebičů před pulzním přepětím a připojované k zásuvkám. Základním prvkem jemné ochrany jsou varistory a speciální polovodičové diody. Pro méně náročné aplikace se používá jednoduchá přepěťová ochrana vestavěná do zásuvky, prodlužovacího přívodu, elektroinstalačních krabic nebo elektrokanálů. Pro náročnější aplikace je tato přepěťová ochrana doplněna o vysokofrekvenční filtr. Tato kombinovaná ochrana je často umístěna do zásuvkových adaptérů.

4.3 Záložní zdroje energie

Pro případ výpadku proudu je nutný záložní zdroj energie – UPS (Uninterruptible Power Supplies).

UPS je akumulátorový typ záložního zdroje, který může dodávat jen omezené množství nashromážděné energie. Počítače tak po výpadku elektřiny mohou ještě nějakou dobu pracovat. Tato doba stačí na to, aby bylo možné uložit rozdělanou práci, pozavírat aplikace a bezpečně ukončit operační systém.

Typický záložní zdroj zvládne dodávat elektrickou energii nejméně 5 až 20 minut, dokud se nevybíje akumulátor.

UPS jsou připojeny do elektrické zásuvky na zdi. Při běžném provozu se záložní zdroj trvale dobíjí. Počítač je připojen k UPS. Většina dnešních UPS má na výstupu několik elektrických zásuvek, takže k ní můžete připojit více počítačů najednou.

Při výpadku elektrického proudu to UPS rozpozná, některé UPS mohou být nakonfigurovány tak, že upozornění uživatele při výpadku proudu. Uživatel je upozorněn zvukovým signálem (pípáním), nebo pomocí software, který na určitý uživatelský účet odešle zprávu s upozorněním. Program je možné také nastavit pro automatické započetí procesu vypínání připojeného počítače, pokud je UPS v režimu napájení z baterií.

Další možností jsou generátory. Vyrábí elektřinu pomocí motoru, spalujícího benzín, petrolej, naftu nebo další palivo. Díky generátoru je možné s veškerým vybavením (včetně počítačů) dál pracovat po celou dobu výpadku elektrické energie.

4.4 Zabezpečení dat proti selhání pevného disku RAID

RAID (Redundant Array of Inexpensive/Independent Disks) je vícenásobné diskové pole nezávislých disků. Jedná se o technologii řadičů, která koordinovaně řídí přístup ke dvěma nebo více diskům současně. Účelem je zvýšení kapacity, bezpečnosti nebo rychlostí (případně vše).

V principu jde o spojení několika disků do jednoho svazku, který se navenek tváří jako jeden pevný disk. Technické řešení diskových polí je dvojí, hardwarové a softwarové. V prvním případě se o spojení disků stará hardwarový řadič, v druhém totéž zajistí jádro operačního systému.

Řešení postavená na hardwarovém řadiči jsou nákladnější. V nejlepším a nejdražším případě jde o samostatné skříně, které obsahují řadič s velkou vyrovnávací pamětí a šuplíky s pevnými disky, obvykle v hot-swapovém provedení⁴. Při poruše jednoho disku obsluha za provozu disk vyjme a vloží nový. Bez jakékoli ztráty dat či provozního výpadku a bez citelné ztráty výkonu pole.

Pro menší servery a náročnější stanice je určen řadič RAID v podobě přídatné karty. V nejjednodušším provedení určeném většinou pro disky s rozhraním SATA jej obsahují i některé lépe vybavené základní desky. Jednodušší řadiče mají především tu nevýhodu, že podstatná část jejich funkcionality je tvořena softwarovým ovladačem. Nevýhodou softwarového řešení jsou oproti hardwarovému vždy o něco vyšší nároky na systémové prostředky.

RAID umožňuje zabezpečení dat proti selhání pevného disku. Data se ukládají na více nezávislých disků. Pokud dojde k selhání některého z disků, nedojde ke ztrátě dat. (Nezaměňovat se zálohováním).

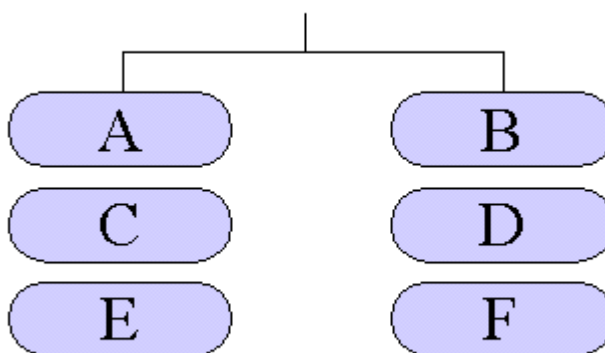
Úroveň zabezpečení se liší podle zvoleného typu RAID, které je označováno čísly (nejčastěji RAID 0, RAID 1, RAID 5 či nověji RAID 6). RAID je často používán na serverech.

RAID 0 Striping, prokládání

Data jsou rozložena do menších bloků a ty se střídavě ukládají na různé disky. Výhodou je rychlost a 100% využití kapacity disků, neboť se pracuje se všemi disky současně. Ale při selhání jednoho disku z pole dojde ke ztrátě všech dat.

K použití se toto pole hodí spíše v softwarové podobě pro vysoce zatížené stanice nebo též pro hardwarová řešení, kde se RAID 0 kombinuje s jiným typem pole (např. RAID 1 + RAID 0 = RAID 10).

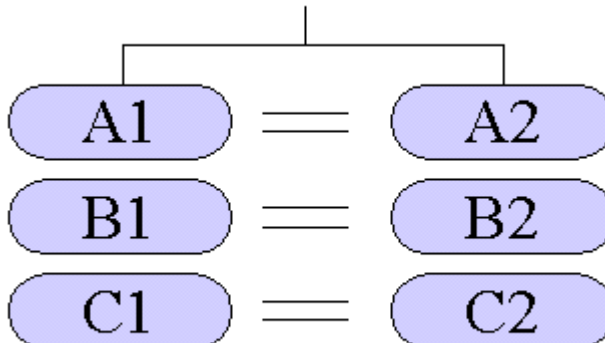
⁴ Hot-swap - výměna komponent za horka, tedy za chodu. Pokud je diskové pole označováno jako hot-swap, při havárii nebo nutnosti rozšířit diskovou kapacitu může operátor disk vyměnit (případně přidat) bez zastavení systému.



Obrázek 4-1: RAID 0 Striping, prokládání

RAID 1 Zrcadlení disku

Vyžaduje dva fyzické pevné disky, nejlépe o stejné kapacitě. Všechna data na jednom disku jsou zrcadlena na druhém. Na druhém disku se tak nachází přesně stejná kopie všech souborů. Pokud jeden disk selže, druhý jej nahradí, buď automaticky, nebo příkazem operačního systému. Po výpadku jednoho disku v plném provozu se může server nechat běžet po nezbytně dlouhou dobu pouze s jedním diskem



Obrázek 4-2: Zrcadlení disků

U větších polí je možné vytvořit několik dvojic disků, které se vzájemně zrcadlí. Asi jedinou nevýhodou RAID 1 je, že kapacita pole je poloviční. Pro svou jednoduchost a relativní bezproblémovost jde o velice oblíbený typ diskového pole u malých serverů, a to jak v softwarové, tak v hardwarové podobě a je asi nejvhodnější pro použití na domácí stanici.

RAID 1 Dvojité disky

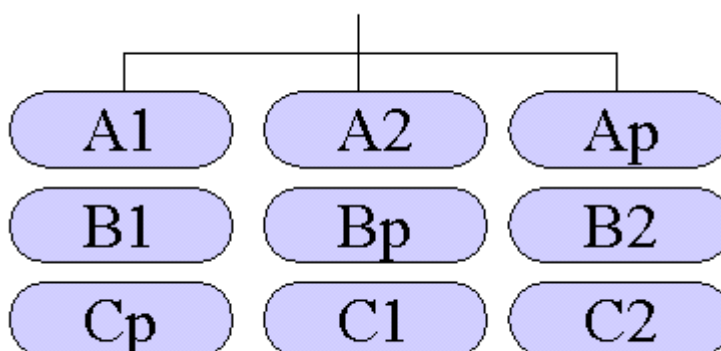
Pracují stejně jako zrcadlení disku jen s tím rozdílem, že dva fyzické disky jsou připojeny k různým diskovým řadičům. Při selhání jednoho řadiče může nadále pracovat druhý disk, připojený k jinému řadiči.

RAID 0+1 prokládání a zrcadlení

Jedná se kombinace RAID 0 a RAID 1. Používají se čtyři disky. Data se nejprve ukládají prokládaně (RAID 0) na dva disky A a B, poté se to samé děje s dalšími dvěma disky C a D. Ve výsledku získáme dvě dvojice zrcadlených disků AB a CD. Při výpadku některého z disků sice dojde ke ztrátě redundantnosti dat, ale data se po chybě dokážou snadno opravit.

Přidat RAID 5

K jeho realizaci jsou nezbytné nejméně tři pevné disky. Data jsou opět rozdělena do bloků a jsou zapisována střídavě na všechny disky. K nim je dopočítávána parita, která je na disky rovnoměrně rozložena.



Obrázek 4-3: RAID 5

Pole je odolné proti výpadku disku (v případě pole ze tří disků je možný výpadek jednoho). Předností je dobrý výkon, zejména při čtení velkých souborů. Kapacita pole složeného ze tří disků bývá odhadována na dvě třetiny součtu kapacity zapojených disků. Jde o oblíbený RAID pro servery, a to jak v softwarové, tak v hardwarové podobě.

RAID 6

Minimem jsou čtyři disky. RAID 6 je podobný RAIDu 5 s tím, že paritní blok není jeden, ale dva, takže pole, které má kapacitu $n-2$ disků, unese selhání kterýchkoliv dvou z nich. Výkon RAIDu 6 je podobný jako výkon RAIDu 5, náročnost na výpočetní výkon je ovšem o něco vyšší (počítají se dva paritní bloky).

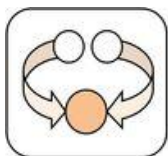
RAID 10

RAID 10 je kombinací RAIDu 1 a 0 v tomto pořadí. Tj. nejprve se vytvoří dvě RAID 1 pole, a poté se nad nimi postaví RAID 0. Výhodou je dobrý poměr mezi odolností a výkonem.

RAID 15 (nebo RAID 51)

RAID 15 (nebo RAID 51) je kombinací RAIDu 1 a 5. Bývá označován jako RAID pro paranoidní, neb poskytuje poměrně velkou odolnost, za kterou se ovšem platí drastickým úbytkem kapacity.

Shrnutí kapitoly



Ve vysoce zabezpečeném prostředí by měl být fyzicky zabezpečen přístup k serveru, síťovým zdrojům, datovým nosičům.

Počítače a všechna síťová zařízení by měla být chráněna proti přepětí (přepěťové ochrany) a proti výpadku proudu (UPS, generátory).

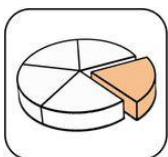
Dalším kritickým místem jsou samotné disky jakožto nosiče dat. Pro jejich vyšší zabezpečení se používá technologie RAID.

Kontrolní otázky a úkoly



- 1) Jak lze fyzicky zabezpečit server?
- 2) Co je to přepětí a jak vzniká?
- 3) Jak chráníme elektroniku proti přepětí?
- 4) Jak chráníme počítačovou síť proti výpadku proudu?
- 5) Jaká je funkce UPS?
- 6) Charakterizujte technologie RAID.

Použitá literatura a jiné zdroje:



- [1] MINISTR, Jan. STŘEDNÍ ODBORNÁ ŠKOLA OCHRANY OSOB A MAJETKU S.R.O. Informační bezpečnost [online]. Karviná, 2011 [cit. 2012-02-03]. Dostupné z: <http://www.ivsoso.com.cz/aktivity4.php>.
- [2] KOUDELKA, Ctirad a Václav VRÁNA. Ochrana před přepětím. VŠB, FEI Katedra obecné elektrotechniky. [online]. prosinec 2006 [cit. 2012-04-15]. Dostupné z: http://fei1.vsb.cz/kat420/vyuka/BC_FBI/Prednasky/ochrana%20pred%20prepetim.pdf.
- [3] ČEVELA, Lubomír. Když se řekne RAID... LinuxExpres [online]. 12. srpen 2005 [cit. 2012-04-15]. Dostupné z: <http://www.linuxexpres.cz/praxe/sprava-linuxoveho-serveru-raid-teoreticky>.

- [4] DOČEKAL, Michal. Správa Linuxového serveru: RAID teoreticky. *LinuxExpres* [online]. 3. prosinec 2009 [cit. 2012-04-15]. Dostupné z: <http://www.linuxexpres.cz/praxe/sprava-linuxoveho-serveru-raid-teoreticky>.

5 Virtualizace

Obsah hodiny



Obsahem této hodiny je vysvětlení pojmu virtualizace a výhod virtualizace, popis různých typů virtualizace.

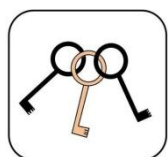
Cíl hodiny



Po prostudování budete schopni:

- vysvětlit pojem virtualizace,
- orientovat se v různých typech virtualizace,
- popsat výhody virtualizace.

Klíčová slova



Virtualizace, Softwarová a hardwarová virtualizace, Virtualizační vrstva, Plná virtualizace, Hypervisor, Částečná virtualizace, Paravirtualizace, Vserver, Aplikační virtualizace

5.1 Co je to virtualizace a její možnosti

Jedna z definic říká: “Virtualizace je abstrakce technických prostředků od jejich použití.” Jedná se o oddělení zdrojů (CPU, operační paměť, ...) od fyzických komponent. Tato abstrakce je základní myšlenkou virtualizace.

Virtualizace v podstatě představuje iluzi, v níž je nějaký zdroj (např. paměť, procesor, disk a další periferie) zmnožen – vytvořením řady kopií a každý uživatel dostane jednu nebo více z těchto kopií k dispozici. Kopie vznikají pouze jako koncepty, tedy jako fyzicky neexistující virtuální objekty (virtuální paměť, virtuální disk, virtuální procesor). Takto může být z virtuálních komponent vytvořen celý virtuální počítač. Uživatel má tak pocit naprosté kontroly (vlastnictví), ale reálně sdílí konkrétní fyzické zdroje s dalšími uživateli.

Virtualizace se realizuje na virtualizační vrstvě, kterou vytváří virtualizační SW. Virtualizační vrstva přizpůsobuje architektonickou vrstvu počítače, nad kterou je vystavěna, a poskytuje vhodné prostředí pro běh programů, které jsou nad virtualizační vrstvou provozovány. Pomocí

virtualizační vrstvy, která emuluje hardware počítače nebo jeho určitou část (využitím skutečných HW prostředků počítače) je možné provozovat na daném fyzickém systému programy, které jsou jinak s HW prostředky daného počítače neslučitelné. Při virtualizaci celé potřebné škály HW prostředků je možné nad stávajícím operačním systémem nejenom provozovat některé „nenativní“ programy, ale i celé virtuální operační systémy.

Virtualizovat lze na různých úrovních, od celého počítače (tzv. virtuální stroj), po jeho jednotlivé hardwarové komponenty (např. virtuální procesory, virtuální paměť, virtualizace vzdálených úložných zařízení atd.), případně pouze softwarové prostředí (virtualizace OS).

Prostředí, které provádí virtualizaci kompletní sady fyzického hardwaru a které se jeví programům, které nad ním běží, jako skutečné hardwarové prostředí, se označuje jako virtuálním strojem, virtuální počítač.

Existuje tedy několik základních vrstev virtualizace:

- **Virtualizace desktopů**
- **Serverová virtualizace**
 - *Softwarová*: spouští virtualizovaný OS nad softwarovou virtualizační platformou přímo na existujícím OS
 - *Hardwarová*: spouští virtualizovaný OS nad softwarovou virtualizační platformou přímo nad hardwarem, bez existujícího OS. Kód hypervizoru (představující virtualizační vrstvu) je přímo integrován do hardware.
- **Virtualizace úložišť**: sloučení fyzického úložiště z různých zařízení tak, aby se jevílo jako jeden fond úložišť (virtuální disky).
- **Virtualizace sítí** (např. VLAN)
- **Virtualizace aplikací**: odděluje aplikace od OS
- **Virtualizace prezentační vrstvy**: terminálové služby

5.2 Vývoj virtualizace

V podstatě každý proces, který je v počítači spuštěn, pracuje automaticky s iluzí "vlastního" procesoru. Plná virtualizace předpokládá, že tuto iluzi má ne pouze jeden proces, ale všechny procesy, které tvoří OS a uživatelské programy dohromady. Jako první tuto vlastnost začala nabízet firma IBM koncem šedesátých let minulého století na svých sálových počítačích vybavených operačním systémem OS/370. Ten dovoľoval rozdělit jeden fyzický počítač na několik virtuálních strojů, přitom v každém virtuálním stroji běžel plnohodnotný OS (případně různý v různých strojích) a uživatelské programy.

Virtualizace v OS/370 byla postavena na tzv. hypervizoru, neboli virtuálním monitoru (virtual monitor). I dnes se tak označuje programová vrstva, která přímo komunikuje s fyzickou vrstvou počítače a která zajišťuje virtualizaci všech součástí. Virtuální počítače (virtual machines) se pak spouští jako procesy tohoto virtuálního monitoru. Uživatel může v každém virtuálním počítači instalovat samostatný operační systém a v něm následně spouštět programy.

Přestože virtualizace v rámci OS/370 byla pro řadu zákazníků zajímavá, vyžadovala velmi rozsáhlou hardwarovou podporu, která zvyšovala cenu. Ostatní výrobci počítačů proto plnou virtualizaci zpravidla nenabízeli a zájem o ni prakticky zmizel v souvislosti se zavedením osobních počítačů (ty totiž nabídly mnohem více fyzických počítačů než byla tehdejší technologie schopná nabídnout počítačů virtuálních, a to za mnohem lepších cenových i provozních podmínek).

S růstem výkonu osobních počítačů a jejich nasazením v podobě serverů využívajících stejné procesory i základní architekturu se však virtualizace stala znovu aktuální.

Dalším důvodem pro nový nástup virtualizace byla potřeba důkladného oddělení vývojových prostředí. Při vývoji software určeného je třeba ověřit jeho vlastnosti v prostředí nejrozličnějších operačních systémů. Instalace, správa a provoz odpovídajícího počtu fyzických počítačů je velmi drahý, využití neefektivní. Je tady sice možnost na jeden počítač postupně bootovat různé verze OS, ale je to časově příliš náročná. Nasazení virtuálních počítačů umožňuje různým verzím OS sdílet jediný fyzický počítač.

Stabilní řešení tvorby vývojového virtualizovaného prostředí umožnilo jeho využití i v dalších oblastech. Poskytovatelé různých internetových služeb zjistili, že mohou provozovat jednotlivé služby v dedikovaných virtuálních počítačích - tím zajistí maximální vyladění výpočetního prostředí (operačního systému) pro konkrétní službu - a přitom tyto dedikované servery (zejména v případě služeb s malým zatížením procesoru) je možné i nadále provozovat na jednom fyzickém počítači. Na jednom počítači je tak možné provozovat virtuální počítač s operačním systémem Linux a v něm webový server Apache, a současně další virtuální počítač, v němž jsou nainstalovány např. Windows XP a Internet Exchange.

Virtualizace tak umožňuje plnou individualizaci prostředí při vysoce efektivním využití zdrojů.

5.3 Typy virtualizace

- Emulace
- Částečná virtualizace

- Plná virtualizace
- Paravirtualizace
- Virtualizace na úrovni operačního systému
- Aplikační virtualizace

Emulace

Je nejstarší technikou virtualizace. Je založena na principu vytvoření virtuálního počítače prostřednictvím softwarových prostředků hostujícího operačního systému. Umožňuje tak provozování hostovaného operačního systému a jeho aplikací i pro odlišnou architekturu hardware, než má sám hostující systém. Emulace umožňuje programům běžet na jiné platformě, než pro jakou jsou naprogramovány.

Jedná se o virtualizaci hardwarových komponent za účelem simulace jiné hardwarové platformy. Hostované OS a aplikace není nutné modifikovat (často to ani není žádoucí). Emulace virtualizuje odlišnou hardwarovou platformu, nevyužívá hardwarovou podporu virtualizace, kterou nabízí dnešní procesory. Je pouze softwarová, režie emulace je proto vysoká.

Částečná virtualizace

Omezuje se na simulaci vybraného hardwaru fyzického počítače, většinou adhesního prostoru. Podporuje sdílení hardwarových zdrojů a izolování jednotlivých procesů, neumí však oddělit instance hostovaných operačních systémů.

Plná virtualizace

Běžné počítače se skládají na základní úrovni z několika komponent: procesoru, paměti a periférií (disky, klávesnice, myš, grafický subsystém, USB a síťové rozhraní atd.). Nahrazením všech fyzických komponent abstraktní variantou v podobě virtuálních komponent, vznikne virtuální počítač. Na něm lze spustit operační systém a vytvořit tak virtualizované prostředí. Jedná se o plnou virtualizaci (full virtualization). OS nemůže žádným způsobem poznat, že nemá přístup k fyzickému technickému vybavení (hardware). Jedná se v podstatě o ideální stav, kdy dochází k plnému oddělení fyzické vrstvy, veškeré programy běží pouze na virtuálním hardware a přístup k fyzickému vybavení je vždy zprostředkován.

Plná virtualizace umožňuje souběžný běh několika virtuálních strojů (s neupravenými operačními systémy) vedle sebe paralelně na jednom fyzickém serveru. Hardware neboli zdroje jsou pro tyto virtuální servery simulovány hypervizorem (virtualizační vrstva). Zároveň tyto operační systémy běží na od sebe izolovaně, takže se navzájem nijak neovlivňují.

To má řadu výhod. Virtuální prostředí lze navrhnout podle potřeby (velikost paměti, typ procesoru, typ a kapacitu disku apod.). Programy jsou nezávislé na konkrétním technickém vybavení, jeho změna nemá na

virtuální prostředí vliv (kromě výkonnostních charakteristik, tj. virtuální počítač může běžet rychleji nebo pomaleji, ale v každém případě poběží). To umožňuje plnou přenositelnost. Mezi profesionální systémy, které nabízí plnou virtualizaci počítačů s procesorem Intel, patří Microsoft Virtual Server, VMWare ESX, Server Oracle VirtualBox, Microsoft Virtual PC a VMware Workstation.

Protože dochází k úplnému oddělení fyzické a programové vrstvy, je při plné virtualizaci prakticky nemožné dosáhnout plného výkonu i v tom případě, že virtuální počítač je víceméně přesným obrazem hardware, na kterém běží. Virtuální monitor totiž musí kompletně odstínit virtuální počítač od jakékoliv možné změny hardware. Toho dosáhne tak, že emuluje fyzické vybavení, a většinu operací provádí ve vlastním software místo toho, aby je přímo vykonával hardware. Nemá-li dojít k výraznému zpomalení virtuálního počítače, je virtualizace omezena pouze na virtuální prostředí, které se maximálně podobá tomu fyzickému.

Paravirtualizace

Virtuální stroj nesimuluje hardware, ale místo toho nabízí speciální aplikační rozhraní (API), které vyžaduje určité modifikace hostovaného OS, aby mohl být tento OS nad virtuálním strojem spouštěn.

Paravirtualizace provádí jen částečnou abstrakci na úrovni virtuálního počítače. Virtualizace v tomto případě není úplná, některé vlastnosti např. procesoru mohou být omezeny a OS může rozpoznat, že běží ve virtuálním prostředí. Virtuální a fyzický hardware se příliš neliší. To umožňuje, aby virtuální počítač v maximální míře využíval vlastnosti základního fyzického prostředí (není potřeba emulovat všechny komponenty virtuálního počítače).

Pro paravirtualizaci je třeba modifikovat některé součásti operačního systému, změny jsou však malé a dobře lokalizovatelné (zvláště dobře je pak možné provést tyto změny u OS, k nimž jsou k dispozici zdrojové kódy; i proto je oblíbená v prostředí Linuxu). Problémem je totiž virtualizace procesoru. Každý procesor pracuje alespoň ve dvou různých režimech:

- privilegovaném, který je přístupný pouze jádru operačního systému, "
- uživatelském, ve kterém běží všechny programy.

Úkolem privilegovaného režimu je zajistit, že uživatelé mají kontrolovaný přístup k hardware a nemohou přímo provádět operace, které by mohly ohrozit jiné programy či integritu dat (např. přímý přístup na disk či složitější operace s virtuální pamětí). Při virtualizaci je potřebná ještě jedna úroveň, na které poběží virtuální monitor. V případě plné virtualizace to není problém, při tomto přístupu se emuluje celý procesor se všemi úrovněmi ochrany. U paravirtualizace je to složitější.

Virtuální monitor musí běžet na nejvyšším stupni ochrany. Na stejné úrovni však nemůže automaticky běžet OS, protože by mohl ovlivnit stav virtuálního monitoru. Pokud byly jen dvě úrovně ochrany (privilegované a neprivilegované), musel by operační systém virtuálního počítače pracovat neprivilegovaně, tím by však byl vystaven ohrožení ze strany aplikací.

Paravirtualizace je možná jen díky tomu, že konkrétní procesory podporují více úrovní ochrany. Procesory Intel mají definovány 4 úrovně ochrany, tzv. *okruhy (rings)*. Na nejvyšším stupni ochrany (*ring 0*) běží OS, uživatelské programy běží s nejnižším stupněm ochrany (*ring 3*). Ostatní stupně se běžně nevyužívají. Při použití paravirtualizace, pak virtuální monitor pracuje na nejvyšším stupni ochrany, tj. v okruhu 0. OS virtuálního počítače se posune o jeden stupeň (do okruhu 1), aplikační programy běží stále s nejmenší ochranou. OS má tak stále vyšší úroveň ochrany než aplikační programy, na druhé straně už nemůže provádět operace, které vyžadují plně privilegovaný přístup.

Paravirtualizace je široce využívána při tvorbě virtuálních prostředí nad procesory Intel (a AMD). VMWare workstation a Xen patří mezi neznámější systémy, které jsou postaveny na paravirtualizaci.

Přestože má paravirtualizace řadu výhod proti plné virtualizaci, potřebuje určité modifikace operačních systémů, což komplikuje její nasazení (zejména u proprietárních OS) a vede k určité neefektivnosti. Intel proto zavedl další systém podpory virtualizace v podobě tzv. *Intel Virtualization Technology (IVT)*. Jedná se o rozšíření možností procesorů tak, že přibývá další úroveň ochrany (*ring -1*) pro VMM a přibývají speciální instrukce na této úrovni. Virtuální monitor tak může obsluhovat několik virtuálních počítačů, které již pracují v prostředí, které se neliší od toho, které je k dispozici ve standardních procesorech bez podpory virtualizace. OS ve virtuálních počítačích není třeba modifikovat, přitom zůstávají základní výhody paravirtualizace, tj. přímé vykonávání instrukcí virtuálního počítače fyzickým procesorem.

Virtualizace na úrovni OS, virtuální privátní servery (VServer)

Nejedná se o virtualizaci celého virtuálního počítače, ale pouze o virtualizaci prostředí pro aplikace běžící nad hostujícím operačním systémem. Jedná se například o Linux-VServer, OpenVZ.

V tomto případě je virtualizace realizována až na úrovni aplikačních programů. Namísto virtuálního monitoru běží na počítači jádro standardního OS, v něm jsou pak spouštěny uživatelské virtuální servery, které toto jádro sdílí.

Každý z virtuálních serverů nabízí pouze uživatelské prostředí (v němž běží uživatelské programy), vzájemná ochrana programů i virtuálních serverů je pak řešena standardními prostředky jádra OS.

Zatímco v případě paravirtualizace je nutné modifikovat OS, v případě VServeru je třeba modifikovat aplikace, zejména pokud používají některé z vlastností, na nichž je tento koncept postaven. Je třeba rovněž upravit celou řadu systémových programů, které poskytují informace o stavu celého systému. Např. systémové volání *uptime* udává, jak dlouho je OS aktivní. V případě VServeru by však volání *uptime* nemělo vracet čas běhu základního operačního systému, ale pouze virtuálního privátního serveru, v němž byl *uptime* volán. Jakmile je ale prostředí VServeru vytvořeno, má ze všech virtualizačních technik nejmenší režii a garantuje tak nejlepší využití hardware.

Aplikační virtualizace

Poskytuje speciální virtualizované prostředí pro běh serverových a desktopových aplikací. Využívá sdílených prostředků a vlastních služeb nutných pro běh těchto aplikací. Je to vhodné řešení při vzájemné nekompatibilitě instalovaných aplikací. Příkladem je Java Virtual Machine.

5.4 Výhody virtualizace

- Plné využití hardwarového výkonu infrastruktury firmy, sloučení více služeb na méně serverů (tzv. konsolidace serverů);
- Možnost provozovat více operačních systémů na jednom fyzickém serveru (tj. Linux i Windows, odlišné distribuce Linuxu apod.);
- Zjednodušení zálohování, obnovy záloh, disaster recovery;
- Centralizování správy;
- Zrychlení migrace systému;
- Možnost dynamického přidělování výkonu (navyšování i snižování);
- Úspora energie, snížení nákladů;
- Testování vyvíjených aplikací, zvýšení spolehlivosti konkrétních výpočtů;
- Využitelnost pro interaktivní práci.

Virtualizace má jednoznačný praktický přínos. Uvažujme modelový příklad provozu čtyř síťových služeb (DNS server, webový server, mail server, ftp server), u kterých se často z bezpečnostních důvodů využívá samostatných počítačů, jeden pro každou službu. V těchto případech virtualizace umožňuje každou službu uzavřít v "jejím" počítači, avšak virtuálním. A všechny tyto virtuální počítače lze spustit na jednom fyzickém, což je úspora prostředků na nákup tří počítačů a zároveň nákladů na jejich provoz (elektřina, chlazení) a správu.

Toto využití možností virtualizace však má i svá úskalí a nedostatky. Hlavní problém je v robustnosti - všechny čtyři služby sdílí stejný počítač, pokud dojde k jeho výpadku, přestanou fungovat všechny služby současně.

Virtualizace však umožní řešit efektivně i tento problém. Místo jednoho lze použít dva fyzické počítače. Pokud vše funguje, na každém z těchto počítačů poběží dva virtuální stroje se dvěma funkcemi. Dojde-li k výpadku jednoho fyzického počítače, dojde k výpadku pouze dvou služeb. Hlavní výhoda se však projeví v nápravě (recovery) tohoto výpadku. Ty dva virtuální stroje, k jejichž výpadku došlo v důsledku zhroucení jednoho fyzického počítače, je možno s co nejmenší časovou ztrátou spustit na tom zbývajícím počítači, aniž bychom jakkoliv zasáhli do na něm již běžících služeb.

Virtualizace tedy umožňuje snížit počet fyzických počítačů, ale současně velmi efektivně reagovat na případné výpadky bez nutnosti držet si záložní počítače.

Tento přístup se dá dále rozšířit. Namísto pevného mapování virtuálních počítačů na fyzické je možné je přidělovat dynamicky, zpravidla podle aktuální zátěže. V předchozím modelovém případě dvou počítačů a čtyř služeb lze třeba v době vyšší zátěže webového serveru jeho virtuálnímu počítači přidělit jeden fyzický stroj a ostatní tři virtuální počítače (a jejich služby) ponechat na druhém. Při poklesu zátěže webové serveru pak přesunout některý z těch tří virtuálních strojů a zvýšit tak poskytovaný výkon všech tří služeb.

Co je to přesun virtuálního počítače? Každý virtuální počítač běží v prostředí nějakého hypervizoru (VMM, Virtual Machine Monitor), který mimo jiné rozhoduje o přidělení procesoru a také má plně pod kontrolou všechna virtuální rozhraní (především přístup na disk či do počítačové sítě). Jestliže hypervizor odebere konkrétnímu virtuálnímu počítači procesor, virtuální počítač se zastaví, ale "neví" o tom. V tomto stavu je možné virtuální počítač "uklidit", tj. vzít veškerou paměť, kterou používá, a zkopírovat ji na disk. Takto se vytvoří obraz virtuálního počítače ve stavu, který odpovídá hibernaci OS (bez virtualizace). Proti hibernovanému stavu, který zpravidla nelze spustit jinde než na tom počítači, kde došlo k hibernaci, lze virtuální obraz přesunout na jiný počítač a spustit jej tam. Dojde k přesunutí (migraci) virtuálního počítače na jiný fyzický, aniž by jakkoliv došlo k narušení vnitřního stavu virtuálního počítače. Samozřejmě reálná situace je komplikovanější kvůli vstup/výstupním operacím. Systém souborů lze přesunout též (s tím přesuneme i otevřené soubory).

Problém je však se síťovou komunikací. Po odebrání procesoru nemůže virtuální počítač přijímat data. Naštěstí toto může zajistit hypervizor. Pakety přichází na fyzickou síťovou kartu, hypervizor je přesune do virtuálního síťového rozhraní konkrétního virtuálního počítače. Hypervizor "ví", že konkrétní virtuální počítač je přesouván, může proto pro něj určené pakety ukládat do bufferu a tento buffer rovněž přesunout na cílový počítač (do odpovídajícího bufferu cílového hypervizoru). Tímto způsobem je možné

zajistit i bezeztrátovost síťové komunikace. Samozřejmě zůstává nebezpečí, že druhá strana čeká na odpověď a pokud ji nedostane v nějakém konečném časovém intervalu, spojení přeruší. Toto nebezpečí lze minimalizovat rychlostí přesunu virtuálního stroje a jeho rychlým znovu spuštěním. Toto schéma funguje pouze při přesunu v rámci lokální sítě, kdy nemusí dojít ke změně IP adresy virtuálního stroje.

Pokud je k dispozici obraz virtuálního stroje, lze jej nejen přesouvat, ale i kopírovat. Tímto způsobem je možno vytvořit vzorovou instalaci (gold image) a kdykoliv vytvořit její kopii a tu spustit na vhodném fyzickém počítači. Kromě rychlosti je takto zajištěna naprostá identita všech spuštěných strojů.

Výše uvedený způsob migrace virtuálního počítače má charakter "ulož a přesuň" (store and forward). Možná je ale i tvorba kopie v reálném čase, kdy se kopíruje běžící virtuální počítač. Výsledkem je, že na dvou fyzických strojích jsou dva identické virtuální počítače ve stejném stavu rozpracování. Pouze jeden z těchto počítačů však skutečně "počítá" (výpočet druhého je simulován tím, že se v něm zaznamenávají změny stavu toho aktivního virtuálního počítače). Ve vhodném okamžiku se přepne řízení a nově vytvořená kopie převezme aktivitu a původní virtuální počítač skončí. Při pečlivé práci s buffery je možné garantovat přesun v rámci lokální sítě se ztrátou nejvýše jednoho paketu, což odpovídá skutečně okamžité migraci.

Použití virtuálních počítačů a jejich migrace umožňuje i velmi významnou úsporu spotřeby elektrické energie. Všechny čtyři virtuální počítače poběží na jednom fyzickém (viz. výše uvedený příklad) a druhý fyzický buď bude úplně vypnutý nebo v nějakém energeticky úsporném režimu a bude se aktivovat, teprve při přetížení prvního počítače. Pokud se tento model rozšíří na více služeb, resp. jejich kopie, dosáhne se skutečně významných úspor elektrické energie. Např. velké webové servery běží na velkých clusterech, přitom jen část dne je pro obsluhu uživatelských požadavků skutečně třeba plný výkon všech uzlů. Virtualizace umožňuje využít v každém okamžiku optimální počet uzlů, ostatní mohou být vypnuté. Přitom díky kopírování a migraci virtuálních počítačů je možné velmi rychle reagovat na změny zátěže.

Virtualizace umožňuje také zvýšit spolehlivost konkrétních výpočtů. Snímek stavu virtuálního počítače se nemusí vytvářet jen pro migraci, ale i během výpočtu lze pravidelně vytvářet snímky stavu (checkpoints) a ty ukládat. Dojde-li z nějakého důvodu ke zhroucení počítače, je možno aktivovat nějaký z předchozích snímků a výpočet dokončit s minimální ztrátou.

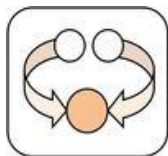
Zajímavou oblastí je i využitelnost virtuálních oblastí pro interaktivní práci. Máme-li jeden počítač (s jedním procesorem) a spustíme-li na něm

dva virtuální počítače, budou vzájemně soupeřit o výkon procesoru. Hypervizor však může nejen zvýšit prioritu jednoho virtuálního počítače (na úkor druhého), ale může změnit i parametry předávání procesoru mezi oběma virtuálními počítači (např. velmi snížit dobu, po kterou má virtuální počítač procesor garantován). Tímto způsobem lze dosáhnout toho, že jeden z obou virtuálních počítačů může být vysoce interaktivní, vhodný pro přímou práci uživatele, a přitom spotřebovává jen malou část celkového výkonu procesoru (v literatuře jsou popsány experimenty, kdy interaktivní virtuální počítač spotřebuje jen cca 10 % celkového výkonu a přitom uživatel má pocit, že počítač je pouze jeho a má vynikající odezvu).

Interaktivitu je možné zkombinovat s migrací: v první fázi všechny virtuální počítače běží na jednom fyzickém. Jakmile se uživatel připojí na virtuální počítač (např. ssh), je mu přidělen fyzický počítač a na něj je příslušný virtuální počítač odmigrován. Proces přihlášení trvá déle, ale fyzické počítače jsou použity až skutečně podle potřeby - kromě úspory elektřiny je možné i optimalizovat sdílení výpočetní infrastruktury mezi interaktivními a dávkovými úlohami.

Virtuální počítače, resp. virtualizace výpočetní infrastruktury nejen pomáhá řešit řadu existujících problémů, ale otevírá i prostor pro zcela nové způsoby využití výpočetních infrastruktur. Zmíněné způsoby použití představují jen část již známých možností.

Shrnutí kapitoly



Virtualizace je abstrakce technických prostředků od jejich použití. Jedná se o oddělení zdrojů (CPU, operační paměť, ...) od fyzických komponent.

Vrstvy virtualizace:

- Virtualizace desktopů
- Serverová virtualizace: softwarová a hardwarová
- Virtualizace úložišť
- Virtualizace sítí
- Virtualizace aplikací
- Virtualizace prezentační vrstvy

Je to technologie, která dovoluje rozdělit jeden počítač na několik samostatně nezávislých počítačů, které pak mohou podporovat nejrůznější operační systémy a aplikace běžící současně.

Typy virtualizace

- Emulace
- Částečná virtualizace
- Plná virtualizace
- Paravirtualizace
- Virtualizace na úrovni operačního systému
- Aplikační virtualizace

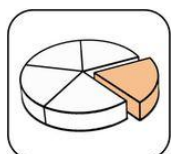
Výhody virtualizace

- Plné využití hardwarového výkonu infrastruktury firmy, sloučení více služeb na méně serverů (tzv. konsolidace serverů)
- Možnost provozovat více operačních systémů na jednom fyzickém serveru (tj. Linux i Windows, odlišné distribuce Linuxu apod.)
- Zjednodušení zálohování, obnovy záloh, disaster recovery
- Zrychlení migrace systému
- Možnost dynamického přidělování výkonu (navyšování i snižování)
- Úspora energie, snížení nákladů
- Zvýšení spolehlivosti konkrétních výpočtů
- Využitelnost pro interaktivní práci
- Centralizování správy
- Testování vyvíjených aplikací

Kontrolní otázky a úkoly



- 1) Co je to virtualizace?
- 2) Na jaké vrstvy lze použít virtualizaci?
- 3) Co je to softwarová a hardwarová virtualizace?
- 4) Co je to hypervisor, jakou funkci má při virtualizaci?
- 5) Jaké jsou typy virtualizace? Popište.
- 6) Jaké jsou výhody virtualizace?



Použitá literatura a jiné zdroje:

- [1] L. Matyska. Virtualizace výpočetního prostředí. Zpravodaj ÚVT MU. ISSN 1212-0901, 2006, roč. XVII, č. 2, s. 9-11.
- [2] L. Matyska. Techniky virtualizace počítačů (2). Zpravodaj ÚVT MU. ISSN 1212-0901, 2007, roč. XVII, č. 3, s. 9-12.
- [3] L. Matyska. Virtualizace výpočetního prostředí (3). Zpravodaj ÚVT MU. ISSN 1212-0901, 2007, roč. XVII, č. 5, s. 5-7.
- [4] RUEST, Danielle a Nelson RUEST. Virtualizace: podrobný průvodce. Brno. ISBN 978-80-251-2676-9.
- [5] Virtualizace operačních systémů. BERAN, Radek.
[Http://www.beranr.webzdarma.cz/](http://www.beranr.webzdarma.cz/) [online]. 2006 [cit. 2012-06-09].
 Dostupné z: <http://www.beranr.webzdarma.cz/virtualizace.html#litVirtualizaceServeru>

6 Serverová virtualizace

Obsah hodiny



Obsahem této hodiny je charakteristika virtuálních počítačů, možnosti serverové virtualizace a dimenzování hostitelských serverů.

Cíl hodiny



Po prostudování budete schopni:

- popsat virtuální počítač a jeho soubory,
- charakterizovat jednotlivé modely serverové virtualizace,
- jmenovat hlavní výrobce virtualizačního SW a orientace v jejich produktech,
- orientovat se v dimenzování hostitelských serverů,
- orientovat se v konfiguraci virtuálního počítače.

Klíčová slova



Virtuální počítač, Soubory virtuálního počítače, Modely serverové virtualizace, Fondy zdrojů serveru, Konfigurace virtuálního počítače

6.1 Virtuální počítač

Virtuální počítač je ve své podstatě několik souborů uložených na disku. Tyto soubory obsahují nastavení virtuálního stroje, diskovou jednotku či další důležité informace o počítači. Při spuštění virtuálního stroje se soubory nahrají do paměti a emulátor začne spouštět daný stroj běžným způsobem tak, jak je na dané platformě zvykem. Hostitel pak dostává a zpracovává dodaná data a posílá je zpět emulátoru a ten je uplatní ve virtuálním stroji.

Nejčastěji se jedná o následující soubory:

- konfigurační soubor,
- soubor(y) pevného disku,
- soubor obsahu paměti,
- stav virtuálního počítače,
- soubory, které obsahují protokoly a další informace.

Existují ještě další soubory, které podporují pokročilé funkce virtualizace. Každý virtualizační produkt podporuje disky umožňující provést akce, které lze vrátit zpět, lze zrušit změny a vrátit se do dřívějšího stavu na základě dřívějšího „snímku“ souborů apod.

Princip souborů umožňuje, že je virtuální počítač, jednoduše přenositelný, lze jej snadno duplikovat, zálohovat, obnovovat.

Konfigurační soubor

Obsahuje informace o nastavení virtuálního stroje jako velikost operační paměti RAM, počet procesorů, počet a typ síťových karet, počet a typ virtuálních disků. Je malý, většinou jde o soubor textový nebo ve formátu XML.

Virtualizační software na základě tohoto souboru alokuje zdroje hostitele pro virtuální počítač. Říká, kde se nachází soubor(y) pevného disku, kolik se použije RAM, jak spolupracovat se síťovými kartami, který procesor(y) se má použít.

Soubor(y) pevného disku

Obsahuje data, které se nacházejí běžně na disku. Když se vytvoří virtuální počítač, vytvoří virtualizační SW virtuální pevný disk, což je soubor, který simuluje typický na sektorech založený pevný disk. Po instalaci OS je pak celý OS obsažený v tomto souboru.

Soubor je proto značně velký, funguje na principu databáze: jeho velikost, čili velikost virtuálního disku, se s přidáním dat může zvětšovat (podle použitého virtualizačního SW⁵), lze jej komprimovat.

Hlavní typy disků virtuálního počítače:

- disky virtuálního počítače (VMDK) od společnosti VMware,
- virtuální pevné disky VHD) od společnosti Microsoft.

Soubor obsahu paměti

Obsahuje informace nacházející se v paměti a určené pro běžící virtuální počítač. Po vypnutí virtuálního počítače se zapíší do souborů pevného disku.

Stav virtuálního počítače

Obsahuje stav virtuálního počítače, je-li počítač pozastaven (obdoba Úsporného režimu nebo Režimu spánku). Soubor je obvykle menší než soubor pevného disku.

⁵ Server ESX používá soubory virtuálních pevných disků pevné velikosti.

6.2 Modely serverové virtualizace

Serverová virtualizace je technologie, která rozděluje počítač na několik nezávislých počítačů, které mohou podporovat různé OS a aplikace. Existují dva virtualizační modely:

- softwarová virtualizace,
- hardwarová virtualizace.

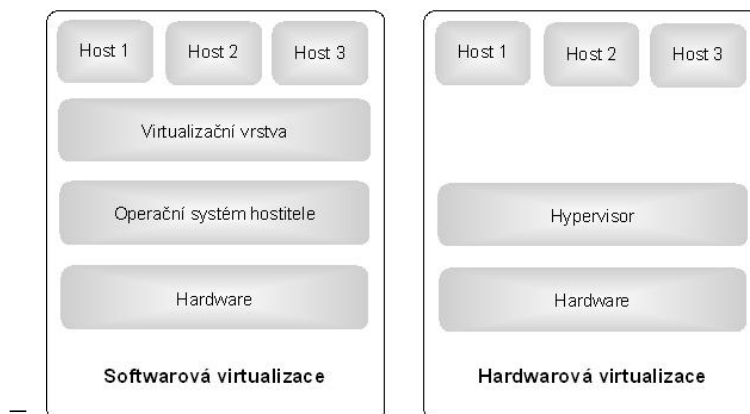
Softwarová virtualizace (na úrovni OS) využívá pro svůj běh jádro hostitelského OS. Umožňuje spouštět více na sobě nezávislých a vzájemně izolovaných virtuálních počítačů. Ty se označují jako kontejnery, virtuální privátní servery (VPS), virtuální prostředí (VEs).

Základem každého virtuálního stroje je hostitelský OS. Aplikace pro virtualizaci vytvoří virtualizační vrstvu, která zajistí virtualizaci prostředí a řídí běh více virtuálních kontejnerů. Zajišťuje abstraktní rozhraní pro přístup k hostitelskému systému a přidělování prostředků od hostitelského systému.

Hlavní výhodou je rychlost, dále využívá jednodušší a mnohdy bezplatné technologie.

Hlavní nevýhodami jsou závislost na jednom OS. OS hostitele vyžaduje zdroje a tak ovlivňuje provoz nad ním běžících počítačů. Chyby přímo v hostitelském OS mohou mít fatální následky pro všechny virtuální stroje. Mohou nastat problémy s případným upgradem hostitelského OS, který může vést k nestabilitě, pádu, zhavarování některých aplikací. Je-li vyžadován restart počítače (např. kvůli aktualizacím OS), restartují se rovněž virtuální počítače.

Hardwarová virtualizace spouští virtualizovaný OS nad softwarovou virtualizační platformou přímo nad hardwarem, bez existujícího OS. Virtualizační vrstva je vytvořena hypervizorem. Kód hypervizoru může být přímo integrován do hardware (VMware) nebo může běžet z firmware nebo interního USB klíče. Vliv hypervizoru na virtuální počítače je minimální.



Obrázek 6-1: Modely serverové virtualizace.

6.3 Hlavní výrobci produktů pro serverovou virtualizaci

Na trhu je řada výrobců virtualizačního software, ale nejvyšší postavení mají následující společnosti: Citrix, Microsoft, VMware. Tyto společnosti nabízí velké množství virtualizačních technologií pro různé oblasti virtualizace.

Citrix (www.citrix.com/xenserver)

- Citrix XenExpressEdition (až čtyři virtuální počítače, bezplatná);
- Citrix XenServer Standard/Enterprise/Platinum Edition: pro hardwarovou virtualizaci, 64bitový hypervizor XEN, pro platformy Linux, Windows, open source;
- Citrix XenDesktop v různých edicích pro virtualizaci desktopů;
- Citrix XenApps pro virtualizaci aplikací.

Microsoft (www.microsoft.com/virtualization)

- Microsoft Virtual Server R2 SP1 (Release 2 Service Pack 1 Enterprise Edition) pro softwarovou virtualizaci; bezplatný;
- Microsoft Virtual Server pro softwarovou virtualizaci; je určen pro serverové OS; možnosti konfigurace virtuálního serveru odpovídají možnostem managementu skutečných serverových systémů, což s sebou například přináší složitější konfigurační prostředí;
- Microsoft Virtual PC 2007 pro softwarovou virtualizaci; bezplatná aplikace je primárně určena pro desktopové OS, tomu odpovídá uživatelské prostředí aplikace a možnosti konfigurace vlastností virtuálního stroje;
- Hyper-V: pro hardwarovou virtualizaci; je součástí OS Windows Server 2008; běží buď jako jádro nebo jako součást úplné instalace; pro HW architekturu x64;
- Microsoft Application Virtualization pro virtualizaci aplikací;
- Terminal Services pro virtualizaci prezentační vrstvy.

VMware (www.vmware.com)⁶

- VMware Server bezplatný produkt pro softwarovou virtualizaci serverů; obsahuje vlastní web server (Apache) pro správu;
- VMware ESXi: pro hardwarovou virtualizaci; bezplatný 32 MB hypervisor, dostupný s HW nebo ke stažení, (může být zaveden do interního flash disku);
- VMware ESX Server: pro hardwarovou virtualizaci; 32 bitový hypervisor; 64 bitový správce paměti;

⁶ První společnost, která nabídla hypervisor integrovaný do HW serveru se systémem ESXi

- VMware Virtual Infrastructure komplexní sada nástrojů pro správu virtualizace a nasazení;
- Virtual Desktop Infrastructure (VDI) pro virtualizaci desktopů;
- VMware Workstation: pro virtualizaci desktopů, může spouštět různé OS;
- VMware fusion: pro virtualizaci desktopů, pro systémy Macintosh;
- ThinApp pro virtualizaci aplikací.

Další společnosti a jejich produkty, např.: Oracle (Oracle VM), Novell (Xen), IBM, SUN (xVM), Virtual Iron.

6.4 Hardwarová náročnost virtualizace serverů

Dimenzování serveru pro fondy zdrojů

Virtualizace je záležitost velmi náročná na zdroje hostitelského počítače (tj. počítače, na kterém budou provozovány virtuální počítače). Klíčové pro hostitelské servery jsou následující zdroje:

- procesor (x64, 3 GHz nebo více),
- paměť RAM,
- síť,
- disk.

Jaké jsou tedy požadavky na uvedené hardwarové zdroje? Vychází se z max. počtu hostovaných počítačů na serveru (podniky v průměru provozují 10 – 30 virtuálních počítačů na jednoho hostitele).

Hostitelský server by měl mít co největší počet procesorů, nejlépe vícejádrové procesory (alespoň dva čtyřjádrové). Pro více hostitelských serverů se doporučuje mít stejné procesory.

Paměť RAM by měla mít, co největší kapacitu, alespoň 16 GB nebo 32 GB. Doporučuje se používat 64 GB (při nasazení v podniku). Velikost RAM ovlivňuje velikost stránkovacího souboru, pro stránkovací soubor je třeba vyhradit min. a max. velikost místa na disku.

Při dimenzování disku je nutno zvážit kapacitu a počet disků pro přiřazení jednotlivým serverům, prostor pro stránkovací soubor. Zvažuje se počet oddílů, jejich velikost. Doporučuje se min. tři pro jeden server: první pro serverové utility, druhý pro OS a programy, třetí pro data. Datové oddíly by měly být na sdílených discích, odděleny od systémových.

Ochranu disků by mělo zajišťovat diskové pole RAID 1 (zrcadlení, dva disky), RAID 5 (prokládané svazky s paritou, min. tři disky) nebo RAID 10 (zrcadlené prokládané svazky, čtyři disky).

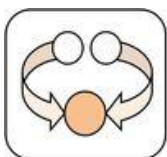
Server by měl být vybaven minimálně čtyřmi síťovými kartami o rychlosti alespoň 1 GB.

Všechny systémy by měly být navrženy tak, aby umožňovaly růst (přidání dalších procesorů, paměti, diskové kapacity).

Konfigurace virtuálních počítačů

- Operační paměť RAM min. 512 MB,
- OS (včetně aktualizací),
- Počet disků 1-3 (podle rolí serveru),
- Kapacita (dle potřeby, min 20 GB),
- Alespoň jedna síťová karta.

Shrnutí kapitoly



Virtuální počítač je ve své podstatě několik souborů uložených na disku. Tyto soubory obsahují nastavení virtuálního stroje, diskovou jednotku či další důležité informace o počítači.

- Konfigurační soubor
- Soubor(y) pevného disku
- Soubor obsahu paměti
- Stav virtuálního počítače

Serverová virtualizace je technologie, která rozděluje počítač na několik nezávislých počítačů, které mohou podporovat různé OS a aplikace. Existují dva virtualizační modely:

- softwarová virtualizace
- hardwarová virtualizace

Hlavními výrobci virtualizačního software jsou společnosti Citrix, Microsoft, VMware. Nabízí velké množství virtualizačních technologií pro různé oblasti virtualizace

Virtualizace je záležitost velmi náročná na zdroje hostitelského počítače (tj. počítače, na kterém budou provozovány virtuální počítače). Klíčové pro hostitelské servery jsou následující zdroje:

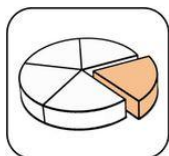
- procesor (x64, 3 GHz nebo více)
- paměť RAM
- síť
- disk

Kontrolní otázky a úkoly



- 1) Co je to virtuální počítač?
- 2) Jaké soubory tvoří virtuální počítač?
- 3) Popište virtualizační modely pro serverovou virtualizaci.
- 4) Jmenujte tři hlavní výrobce virtualizačního SW a příklad jejich produktů.
- 5) Které zdroje jsou důležité pro hostitelské servery?
- 6) Jak by měly být zdroje hostitelských serverů dimenzované?
- 7) Jaká je konfigurace virtuálních počítačů?

Použitá literatura a jiné zdroje:



- [1] RUEST, Danielle a Nelson RUEST. Virtualizace: podrobný průvodce. Brno. ISBN 978-80-251-2676-9.

7 Synchronizace času v síti

Obsah hodiny



Obsahem této hodiny jsou časové služby v síti, které zajišťují synchronizaci času v síti, důvody pro časovou synchronizaci, protokoly a časové servery.

Cíl hodiny



Po prostudování budete schopni:

- vysvětlit co je to časová synchronizace v síti a jaký je její význam,
- popsat protokol a službu NTP,
- orientovat se hierarchii časových serverů v rámci služby NTP,
- charakterizovat typy časových serverů a možnosti konfigurace.

Klíčová slova



UTC, Synchronizace času, NTP protokol, Stratum, Referenční ČS, primární ČS, Sekundární ČS, Režim vnucování času

7.1 Důvody pro synchronizaci času

Každá událost, ke které v síti dojde, získává časovou značku v UTC⁷, která jednoznačně určuje čas, kdy k události došlo. Časový standard pro každý server je jeho lokální čas, ze kterého si server čas UTC vypočítává podle vzorce:

$$UTC = LOCAL\ TIME + (time\ zone\ offset) - (current\ daylight\ saving\ offset)$$

Aby bylo možné správně interpretovat časové údaje, musí být v síti zajištěn jednotný čas.

Synchronizace času je nezbytnou podmínkou fungování počítačových sítí. Bez synchronizace času by nebylo možné korektně realizovat řadu síťových služeb počínaje běžným sdílením souborů až např. po elektronické obchodování.

⁷ UTC: Universal Time Coordinates – čas který se koordinuje k času nultého meridiánu GMT Grendwich Mean Time

Tady jsou některé důvody, proč je třeba mít všude v síti jednotný čas:

- Monitorování systémů: správné řazení událostí v čase, tedy pořadí v jakém proběhly (log soubory).
- Měření časových intervalů např. mezi dvěma událostmi.
- Plánování událostí – možnost definování různých časových souvislostí mezi úlohami.
- Podpora autentizačních mechanismů.

Všechny systémy v síti proto musí mít přístup k jednotným časovým údajům a právě časové služby zajišťují jednotný a korektní čas pro všechny servery a počítače v síti.

7.2 NTP (Network Time Protocol)

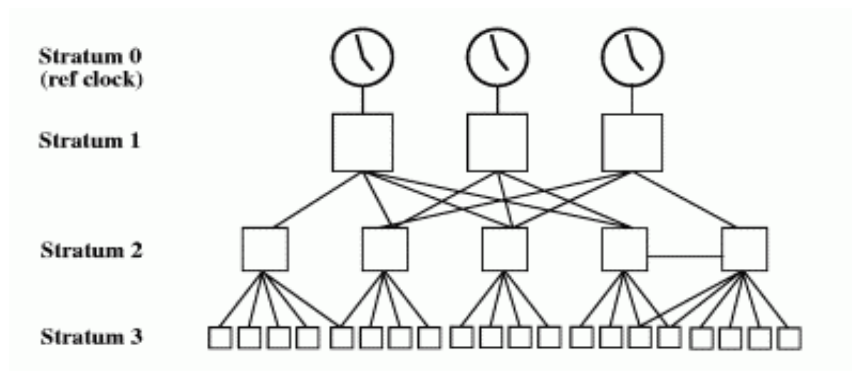
Pro synchronizaci času zařízení zapojených do počítačové sítě se zpravidla používá standard NTP (Network Time Protocol). Je podporován ve velké většině používaných platform. Vedle standardu NTP existuje i jeho „odlehčená verze“ Small Network Time Protocol (SNTP).

NTP je protokol, který funguje na principu klient server. Na počítačích musí být nainstalovaný klientský program, který se dotazuje na přesný čas NTP serveru, ten přesný čas poskytuje. Klient z množství dostupných serverů vyhodnotí jeden co možná nejdůvěryhodnější a současně síťově nejlépe dostupný zdroj času UTC a podle něj se pak synchronizuje.

Standard NTP umožňuje vytvářet hierarchickou strukturu serverů a klientů. Různá zařízení schopná poskytnout přesný čas tvoří vrstvu 0 označovanou jako Stratum 0. Servery jsou rozděleny do dalších vrstev. Na vrcholu je primární časový server úrovně Stratum 1 obvykle vybavený rádiovým nebo satelitním přijímačem. Jeho vnitřní čas je řízen z referenčního, externího zdroje, např. GPS, DCF⁸, atomové hodiny. Ten synchronizuje další NTP servery nižší úrovně označované jako Stratum 2

Počítače v této druhé vrstvě si však nevyberou jeden z první vrstvy, typicky získávají informace hned z několika. Navíc mohou spolupracovat i mezi sebou. Dochází tedy k jistému doladování přesného času. Ve třetí vrstvě většinou bývají klienti, kteří se obvykle synchronizují pouze s jedním nadřazeným serverem. Ve třetí vrstvě se také nachází vůbec nejvíce počítačů. Vrstvy jsou definovány až do patnáctky, už pátá vrstva se však vyskytuje zcela výjimečně.

⁸ DFC: v signálu DCF je zakódována informace o momentálním přesném čase. Tato časová informace je vysílána stanicí DCF77 na dlouhých vlnách s kmitočtem 77,5 kHz z vysílače v Mainflingu (asi 24 km jihovýchodně od Frankfurtu nad Mohanem v Německu)



Obrázek 7-1: Hierarchická struktura NTP serverů

Úroveň Stratum vyjadřuje "důvěryhodnost" serveru. Klient si jako svůj zdroj času zvolí takový server, který má co nejnižší Stratum (je nejdůvěryhodnější), ale současně dobře dostupný.

Je třeba si ale uvědomit, že důvodem hierarchického rozdělení NTP serverů do vrstev, je možnost rozložit zátěž a distribuovat službu NTP podle potřeb uživatelů. Servery vyšších úrovní (Stratum-1 a Stratum-2) jsou určeny především k synchronizaci dalších serverů a nikoliv koncových stanic.

Časový server může být realizován hardwarově jako samostatné specializované zařízení nebo softwarově jako síťový počítač s příslušným programovým vybavením.

Na obrázku je server GPSNTP. Jedná se o Stratum 1 SNTP server pro synchronizaci NTP či SNTP klientů: počítačů, digitálních hodin, PLC automatů. Časová informace je získávána z družicového systému GPS.



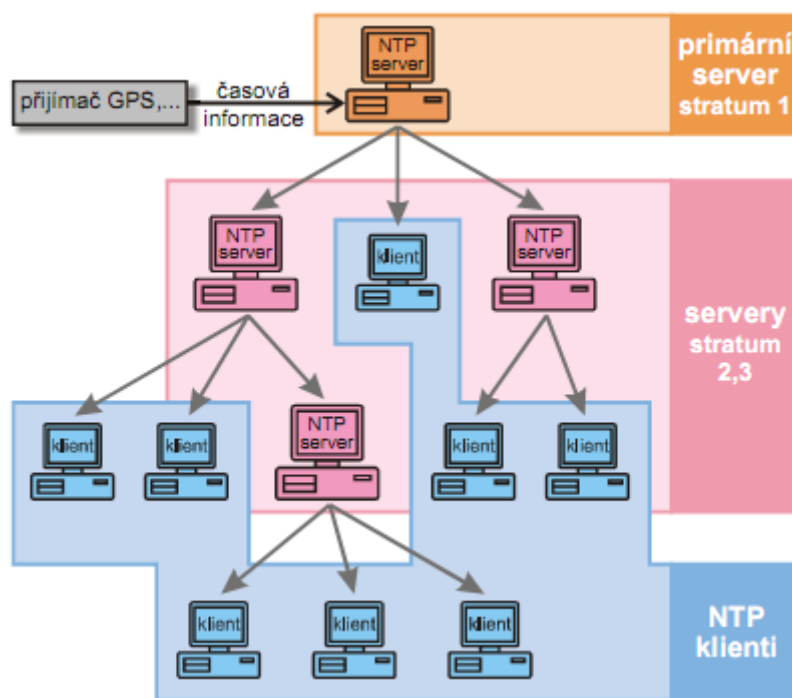
Obrázek 7-2: GPSNTP server Stratum 1 řízený GPS

Funkce NTP klienta je v moderních operačních systémech již standardně zahrnuta. Kde tomu tak není, lze pro jeho realizaci použít některý z mnoha dostupných programů. (Např. OSCNTP klient pro OS Windows NT a vyšší).

V sítích s přístupem k Internetu se k synchronizaci času obvykle využívá některý z veřejných NTP serverů.

Seznam veřejně dostupných NTP serverů Stratum 1 a 2 je k dispozici na <http://www.eecis.udel.edu/~mills/ntp/servers.htm>. Poskytovatelé připojení obvykle mají své vlastní NTP servery přístupné pro své klienty. V každém případě je slušností respektovat pravidla používání stanovené provozovateli serverů a zejména zbytečně nepřetěžovat vytížené Stratum 1, 2 servery.

Pokud však není počítačová síť z organizačních či z technických důvodů k Internetu připojena, je třeba zřídit místní NTP server.



Obrázek 7-3: Organizace sítě z pohledu NTP

7.3 Konfigurace času

Časové servery (ČS) jsou vybrané uzly v síti, které jsou schopny poskytovat ostatním uzlům v síti správné časové informace

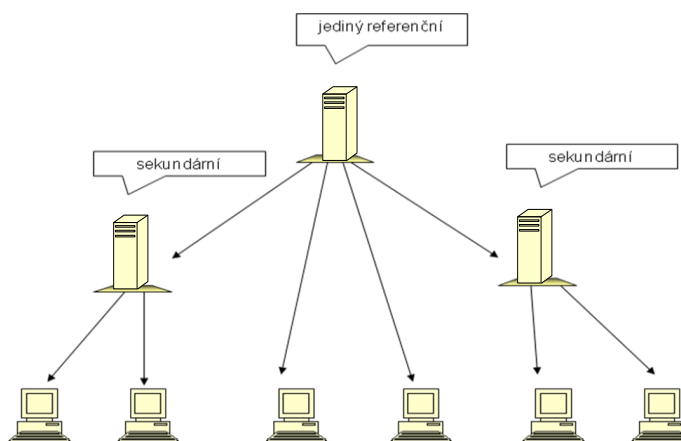
Časové servery obecně rozdělujeme na:

- Poskytovatele času (Stratum 1,2, ...) – čas do sítě poskytují
 - jediný referenční,
 - referenční,
 - primární.

- Konzument času – čas pouze přebírají, nastavují podle něj své interní hodiny a předávají jej dále
 - sekundární.

Jediný referenční ČS (SINGLE) – konfigurace času standardní

Jediným zdrojem času pro celou síť je jediný referenční ČS (pro sekundární servery i pracovní stanice). Zdrojem času jsou interní hodiny, správce nebo NTP poskytovatel. Čas je ostatním „vnucován“. Režim vnucování času je vhodný pro menší sítě.



Obrázek 7-4: Síť s jedním referenčním ČS

Výhodou je jednoduchá správa času v síti. Nevýhodou, že při havárii při přetížení a výpadku serveru není jednotný čas v síti zajištěn.

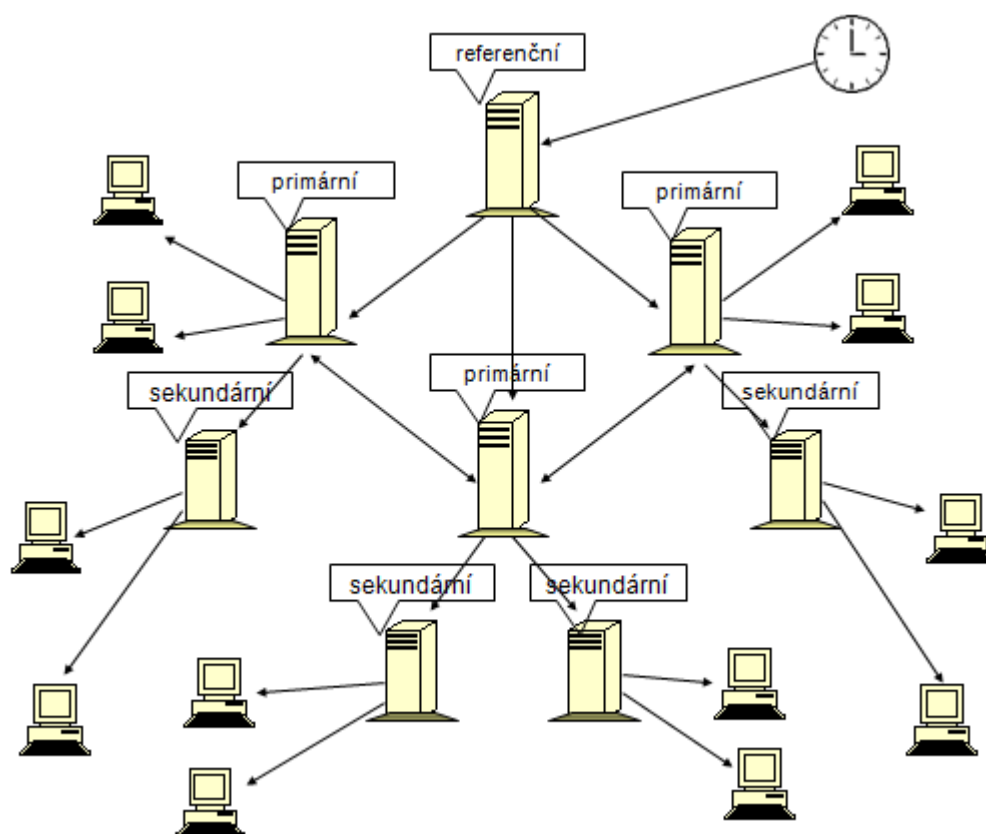
Konfigurace času vlastní

Je určena pro velké sítě, umožňuje vytvářet hierarchickou strukturu časových serverů. Nad procesem časové synchronizace je plná kontrola.

Poskytovatelem času jsou referenční ČS (odpovídají Stratum 1) a primární ČS servery (odpovídají Stratum 2, 3).

Referenční ČS získává čas z externího časového zdroje nebo od NTP poskytovatele, většinou je jediný v síti, je-li jich více, musí být vzájemně synchronizovány.

Čas, který se poskytuje sekundárním serverům a stanicím je plovoucí. Určuje se v režimu hlasování o čase: Aktuální čas v síti se vytváří ve spolupráci se všemi referenčními a primárními časovými servery (váženým průměrem všech časů, referenční má větší váhu).



Obrázek 7-5: Síť s referenčními a primárními servery

Výhodou je vyšší odolnost sítě proti poruchám. Při výpadku jednoho serveru mohou získávat Sekundární servery čas z jiného Primárního serveru.

Shrnutí kapitoly



Synchronizace času je nezbytnou podmínkou fungování počítačových sítí. Každá událost získává časovou značku v UTC, určuje čas, kdy k události došlo.

Synchronizaci času v síti zajišťují časové servery, prostřednictvím protokolu NTP (Network Time Protocol). Funguje na principu klient server: Klient se ptá na čas NTP serveru. NTP servery tvoří hierarchickou strukturu, jednotlivé úrovně se označují Stratum 0, 1, 2, 3 ...

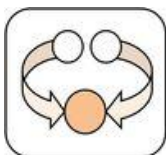
Čas na vrstvě Stratum 1 je řízen z referenčního, externího zdroje (GPS, DCF, atomové hodiny). Stratum 1 synchronizuje další NTP servery nižší úrovně.

Časový server může být realizován hardwarově jako samostatné specializované zařízení nebo softwarově jako síťový počítač s příslušným programovým vybavením.

Časová synchronizace v místních sítích je založena

- na jediném referenčním ČS, který vnucuje čas ostatním. Režim vnucování času je vhodný pro menší síť.
- na hierarchické struktuře časových serverů. Poskytovatelem času jsou referenční ČS a primární ČS servery, kdy se čas určuje v režimu hlasování o čase. Aktuální čas v síti se vytváří ve spolupráci se všemi referenčními a primárními časovými servery.

Kontrolní otázky a úkoly



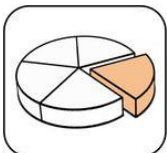
- 1) Co je to UTC?
- 2) Vysvětlete hierarchickou strukturu NTP serveru.
- 3) Jak funguje synchronizace času v síti s jediným referenčním ČS?
- 4) Jak funguje synchronizace času ve velkých sítích?
- 5) Čím je určován čas ve vrstvě Stratum 1?

Otázky k zamyšlení



1) Proč je jednotný čas v síti důležitý?

Použitá literatura a jiné zdroje:



- [1] CHVALOVSKÝ, Karel. NTP: Filozofie synchronizace času po Internetu. Lupa.cz [online]. 16. 5. 2003 [cit. 2012-01-29]. Dostupné z: <http://www.lupa.cz/clanky/ntp-filozofie-synchronizace-casu-po-internetu/>
- [2] TUPÝ, Jan. Synchronizace času počítačové sítě. OSC, a.s., Brno. Osc.cz [online]. [cit. 2012-01-29]. Dostupné z: http://www.osc.cz/cz/produkty/cas/cas_cz.asp

8 Proces bootování a inicializace OS

Obsah hodiny



Obsahem této hodiny popis procesu bootování a inicializace OS.

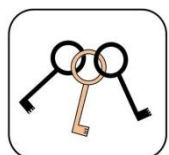
Cíl hodiny



Po prostudování budete schopni:

- popsat proces bootování z pevného disku,
- popsat úlohu BIOSu při bootování,
- orientovat se nastavení BIOSU pro bootování,
- vysvětlit funkci zavaděče,
- orientovat se v možnostech bootování z dalších.

Klíčová slova



Bootování, MBR, BIOS, Boot loader, Boot Manager

8.1 Proces bootování systému

Bootování je proces zavedení operační systém po zapnutí počítače. Probíhá v několika krocích.

Po zapnutí počítače se jako první provede program BIOS (*Basic Input/Output System*). Realizuje některé základní testy a identifikuje technické vybavení (*POSTest*).

Identifikuje zařízení, ze kterého se bude bootovat. Většinou je jako první nastavený pevný disk. Další možnosti jsou CD, USB nebo lze bootovat ze sítě. V Setupu BIOSu je nastaveno jako primární.

Po identifikaci disku pro zavádění na něm BIOS hledá zaváděcí sektor (boot sector), aby mohl spustit zaváděcí program. Úkolem zaváděcího programu je zavést do paměti jádro operačního systému.

Dále následuje start a inicializace OS, což jsou procesy probíhající v režii daného OS.

8.2 Zaváděcí sektor, MBR

Zavaděč, který zahajuje a řídí zaváděcí proces, je umístěn v zaváděcím (bootovacím) sektoru⁹, což je obvykle MBR pevného disku.

Struktura MBR je standardizována a není závislá na použitém operačním systému. Prvních 446 bytů je rezervováno pro kód startovacího programu. Následujících 64 bytů je určeno pro uložení tabulky diskových oddílů, která obsahuje informace o maximálně 4 oddílech. Bez této tabulky nemůže být na disku žádný souborový systém - disk je bez této tabulky nepoužitelný. Poslední 2 byty musí obsahovat speciální magické číslo AA55 (End of Sector marker), označuje konec MBR, Pokud je na této pozici jiné číslo, může být BIOSem, a některými operačními systémy, MBR posouzen jako neplatný.

Bootovací sektor je tedy oblast 512 bajtů na záznamovém médiu, nachází se na prvním sektoru (v případě pevných disků je to válec 0 hlava 0 stopa 0 sektor 1).

BIOS se snaží na tomto sektoru najít Master Boot Record (MBR) – hlavní spouštěcí záznam. Ten nahraje do paměti a v případě úspěchu mu předá řízení.

V případě chybného MBR se bootovací proces přeruší a vypíše se chybové hlášení, jež může vypadat takto:

NO ROM BASIC - SYSTEM HALTED

nebo:

Non-System Disk or Disk Error

MBR se skládá ze dvou částí

- Partition Loaderu
- Partition Table - tabulka rozdělení disku

V MBR v Partition Table má BIOS uloženy záznamy o rozdělení disku na oddíly a informaci, ze kterého oddílu se bude bootovat (aktivní oddíl).

Je-li MBR v pořádku, řízení se předá Partition Loaderu. Ten v Partition Table vyhledá aktivní (bootovací) oddíl a přejde na první sektor tohoto oddílu a předá mu řízení

⁹ Zaváděcí sektory jsou uloženy na každém diskovém oddílu jako první. Zaváděcí sektory jsou velké 512 bytů, a slouží k uložení kódu pro spuštění operačního systému uloženého na tomto oddílu. Zaváděcí sektor s platným zaváděcím kódem obsahuje na stejné pozici jako MBR (poslední 2 byty) shodné magické číslo (AA55).

Také na začátku tohoto oddílu je sektor - Volume Boot Record (VBR), který obsahuje:

- krátký program a
- tabulku rozdělení svého oddílu (logické disky, počet bajtů na sektor, počet sektorů na cluster atp.)

Přesná činnost VBR je závislá na konkrétním operačním systému. Hlavním úkolem je najít a spustit zaváděcí program, který obsahuje zaváděcí sekvenci OS.

Diskety a jednotky flash neobsahují MBR, ale VBR.

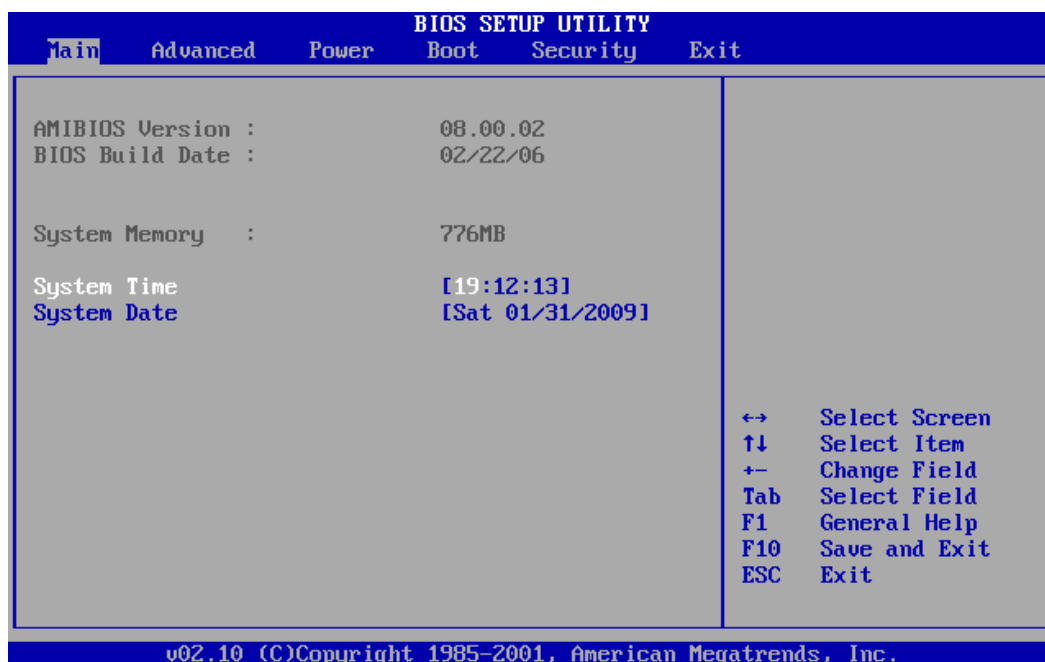
8.3 BIOS

O zavedení jádra do paměti (bootování) se stará malý program – zavaděč (bootovací program), který je umístěný v zaváděcím sektoru na disku. Obsahuje zaváděcí sekvenci OS.

BIOS je systém, který se stará o nejzákladnější funkce počítače, zajišťuje kompatibilitu a bezproblémový chod počítače jako celku. Předává dál operačnímu systému seznam všech HW komponent včetně jejich konfigurace.

Zajišťuje bootování OS a umožňuje operačnímu systému po instalaci nového hardwaru automaticky rozpoznat nový HW.

Je to vlastně základní ovladač pro základní desku uložený v paměti flash (Flash PROM) výrobcem. Jeho konfigurace se provádí prostřednictvím textového rozhraní - BIOS SETUP utility.



Obrázek 8-1: BIOS SETUP utilita

Pro vstup do tohoto textového rozhraní je nutno ihned po spuštění nebo restartu PC přerušit bootovací sekvenci stiskem klávesy pro vstup do BIOSu. Většinou je to klávesa *Delete*, *F2* (u notebooků), *Shift+F2*. Potřebná varianta je vypsána při startu na obrazovce – např.: „*Press DEL to enter Setup*“ - česky to znamená „*Stiskněte Delete pro vstup do nastavení*“ nebo „*SETUP press Shift+F2*. Tím se přeruší proces zavádění a zpřístupní se konfigurace BIOSu. V síti je velmi často ještě vyžadovaná autentizace uživatele zadáním hesla. Jakékoli provedené změny je třeba vždy uložit.

Po vstupu do BIOSU je k dispozici textové menu. Na jednotlivé položky se přechází pravou nebo levou šipkou. Na obrazovce je k dispozici seznam kláves pro ovládání, myška v tuhle chvíli ještě není k dispozici.

8.4 Zavaděč, boot loader

Základní bootloader (zavaděč) je program umístěný v MBR nebo VBR, který se stará o zavedení jádra OS do paměti a jeho aktivaci (spuštění).

Instalace zavaděče je zpravidla prováděna při instalaci operačního systému, do MBR, složitější pak mají své součásti uloženy uvnitř diskového oddílu.

Některé zavaděče pracují dvoustupňově (např. GRUB): Jádro OS je umístěno na nějakém souborovém systému a zavaděč musí znát způsob jak jádro přečíst. Nejdříve se načte první část (z MBR). Ta má za úkol vyhledat v souborovém systému další část zavaděče a přečíst druhý stupeň zavaděče. Až tato druhá část zavaděče umí číst systém souborů (čtení stačí), na kterém je umístěno jádro systému. Zavaděč načte jádro do operační paměti a předá mu řízení.

Základní Boot loader bývá často nahrazen složitějším programem, který se někdy označuje také jako Boot Manager. Umožňuje uživateli, který má více operačních systémů na jednom počítači, vybrat si, který OS se má spustit.

Má větší možnosti konfigurace, umožňuje při startu jádra OS předávat parametry nebo omezit přístup ke startu systému na základě autentizace uživatele. Uživatel se pak musí při spuštění systému identifikovat heslem.

Nejčastěji používané zavaděče:

- LILO (*Linux Loader*) – zavaděč, který je standardní součástí linuxových distribucí; konfigurace v */etc/lilo.conf*.
- GRUB (*the Grand Unified Bootloader*) – zavaděč, který je součástí linuxových distribucí; konfigurace v */boot/grub/grub.conf*, popř. */etc/grub.conf*.

- xOSL (*eXtended Operating System Loader*) – spolehlivý freewarový zavaděč OS.
- NTLDR (*NT OS Loader*) – zavaděč OS Windows NT/2000/XP; konfigurace v *C:\boot.ini*. Od verze Windows Vista nahrazen komponentami *winload.exe* a *Windows Boot Manager*.
- další zavaděče: OSL2000 Boot Manager (*OS Loader*), Boot Magic, chos aj.

8.5 Bootování z jiného média

Jsou situace, kdy je třeba OS zavádět nikoli z pevného disku, ale z nějakého jiného média jako je CD, USB flash, disk, externí disk. Kdysi se za tímto účelem používala často disketa.

Aby počítač bootoval z konkrétního média, je třeba změnit pořadí bootování v nastavení systému BIOSu. Je obvykle v nabídce *Advanced BIOS Features - Boot sequence* nebo v nabídce *Boot - Boot Device Priority*. BIOS zobrazí seznam zařízení. Určuje tak, v jakém pořadí se bude pokoušet BIOS o bootování, pokud médium uvedené jako první nebude k dispozici.

Dále je nutné připravit si médium tak, aby se z něj dalo bootovat, tj. umístit na něj potřebné soubory z operačního systému.

Zaváděcí kód je umístěn ve Volume Boot Record (VBR), což je první sektor úložného zařízení, které nebylo rozděleno na diskové oddíly.

USB flash disk

Pro vytvoření bootovacího USB disku existují SW nástroje. Jednak přímo od výrobce, kdy už při nákupu je součástí CD s ovladači a ovládacím softwarem nebo SW stáhnout ze stránek výrobce a lze využít aplikace „třetí strany“ např. HP USB Disk Storage Format Tool.

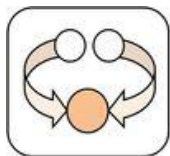
Soubory potřebné pro start různých verzí operačních systémů jsou k dispozici na <http://masterbootrecord.de/english/bootdisketten.php>.

Ultimate Boot CD

Bootovací CD s mnoha užitečnými nástroji. Obsahuje soubor různých diagnostických a testovacích nástrojů. Pro jejich použití, není třeba funkční OS, ani zapojený pevný disk, stačí pouze toto CD a nabootovat z něj.

Po nabootování je k dispozici textové menu, které zpřístupní řadu nástrojů: Memtest, Ranish Partition Manager, CPU Burn-in, McAfee Antivirus Scanner, AVG Free Edition atd.

Shrnutí kapitoly



Bootování je proces zavedení operačního systému po zapnutí počítače. Po zapnutí počítače se jako první provede program BIOS. Po identifikaci disku pro zavádění se z MBR spustí zaváděcí program, který zavede do paměti jádro OS a spustí ho. O zavedení jádra OS do paměti a jeho aktivaci se stará zaváděč systému boot loader nebo Boot Manager.

Bootovat lze nejen z pevného disku, ale i z dalších médií. Pak je třeba nastavit v BIOSu bootování z příslušného média a médium připravit, aby se z něj dalo bootovat.

Kontrolní otázky a úkoly



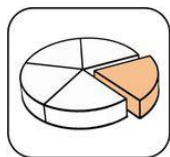
- 1) Co je to bootování OS?
- 2) Jaký je princip bootování?
- 3) Jakou úlohu při bootování má BIOS?
- 4) Co je to MBR, VBR?
- 5) Vysvětlete úlohu zaváděče.
- 6) Jaký je postup pro vytvoření a použití bootovacího USB disku?

Otázky k zamyšlení



- 1) Je výhodné bootování ze sítě, co pro bootování ze sítě umožňuje?

Použitá literatura a jiné zdroje:



- [1] STRÁNSKÝ, Petr. BIOS: Advanced CMOS Setup - bootujeme napoprvé [online]. 21.7.2008 [cit. 2012-02-05]. Dostupné z: <http://www.svethardware.cz/artp.jsp?doc=8AB0025C65C7F561C125747F0033D257>
- [2] Slovník: Zaváděč. Wwww.abclinuxu.cz [online]. 10.10.2004, 25.3.2009 [cit. 2012-02-05]. Dostupné z: <http://www.abclinuxu.cz/slovník/zavadeč>

9 Linux: start a konfigurace zavaděče

Obsah hodiny



Obsahem této hodiny popis startu OS Linux a konfigurace zavaděčů se zaměřením na GRUB.

Cíl hodiny



Po prostudování budete schopni:

- popsat zavádění OS Linux,
- orientovat se v zavaděčích a jejich konfiguraci,
- popsat možnosti konfigurace zavaděče GRUB 2.

Klíčová slova



LILO, GRUB Legacy, GRUB 2

9.1 Start systému

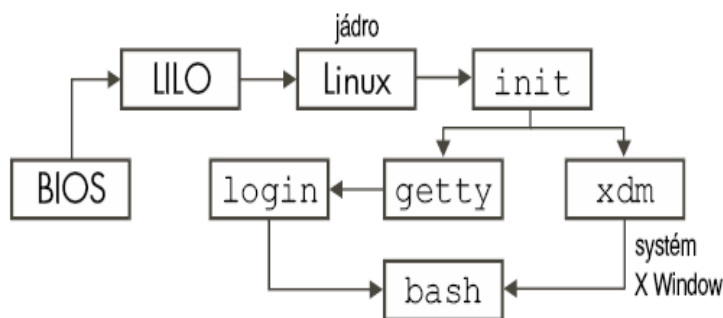
Start a inicializace OS začíná v okamžiku, kdy BIOS předá kontrolu zaváděcímu programu (LILO, GRUB, ...), který je umístěn v zaváděcím sektoru, nejčastěji v MBR.

V Linuxu je zaváděcí sektor i po vytvoření souborového systému prázdný. Linuxový oddíl není schopen zavést sám sebe, i když oddíl obsahuje platný souborový systém s jádrem. Aby bylo možné zavést z tohoto oddílu Linux, musíme do tohoto sektoru uložit zaváděcí program. Proto je součástí instalačního procesu také instalace a konfigurace zavaděče.

Zavaděč OS zavede jádro Linux kernel do paměti a aktivuje ho. Jádro OS (proces 0) detekuje technické vybavení počítače, nastaví ovladače a průběžně vypisuje zprávy o nalezených zařízeních a jejich konfiguraci. Připojí kořenový svazek pro čtení a spustí z adresáře /sbin na pozadí proces init. Po spuštění programu init se jádro stane jakýmsi “manažerem” OS, není už aktivním programem.

Další část startu systému je záležitostí procesu init. Provádí inicializaci systému, tj. spuštění všech služeb – démonů, na základě konfiguračního souboru `/etc/inittab`, odkud spouští tzv. rc-skripty.

Proces init je ukončen spuštěním procesů getty pro terminály a virtuální konzoly. Getty spouští login a systém je tak připraven pro přihlášení uživatele.



Obrázek 9-1: Start OS Linux

9.2 Zavaděče v Linuxu

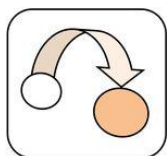
V Linuxu je pro zavádění OS k dispozici několik zavaděčů. Nejznámější jsou:

- LILO (*Linux LOader*) starší zavaděč
- GRUB (*the Grand Unified Bootloader*) dnes asi nejčastěji používaný

Linux LOader - LILO

Konfiguračním souborem zavaděče LILO je `/etc/lilo.conf`. Po ukončení editace konfiguračního souboru musí být provedena aktualizace MBR pomocí příkazu `lilo (/sbin/lilo)`.

Pro odinstalování se spustí program s volbou `-u`: `/sbin/lilo -u`



```

-----                                /etc/lilo.conf                                -----
prompt
timeout=50
default=linux
boot=/dev/hdc7
map=/boot/map
install=/boot/boot.b
message=/boot/message
linear
  
```

```

image=/boot/vmlinuz-2.4.7-10
label=linux
initrd=/boot/initrd-2.4.7-10.img
read-only
root=/dev/hdc7

other=/dev/hda1
optional
label=DOS

```

9.3 GRUB Legacy

GRUB byl původně vyvíjen v rámci projektu Hurd, tedy přímo pod iniciativou GNU. Od roku 1999 je to oficiální boot loader projektu GNU a postupně jej převzaly všechny velké distribuce.

Proti zavaděči LILO, je GRUB výrazně silnějším nástrojem. Je dynamicky konfigurovatelný. To znamená, že zavádí systém buď z konfiguračního souboru, nebo je možné celý zaváděcí proces řídit interaktivně pomocí GRUB shellu:

```

grub > root (hd0,0)      (zadání umístění oddílu /boot)
grub> setup (hd0)        (nainstalování GRUB do MBR)
grub> quit                (ukončení příkazovou řádku GRUBu)

```

GRUB shell (/usr/sbin/grub) se spouští příkazem `grub` nebo při startu, po přerušení startovací sekvence.

Automatické nabootování je řízeno ručně editovatelnými textovými konfiguračními soubory. Konfigurační soubory, jejich umístění, se mohou lišit podle použité distribuce:

- */boot/grub/menu.lst* - informace o všech diskových oddílech a operačních systémech, které lze spustit pomocí zavaděče GRUB.
- */boot/grub/grub.conf* - informace o všech diskových oddílech a operačních systémech, které lze spustit pomocí zavaděče GRUB.
- */etc/grub.conf* - parametry a volby zavaděče GRUB potřebné pro správnou instalaci zavaděče.
- */boot/grub/device.map* - Překlad jmen zařízení od zavaděče GRUB a BIOSu do linuxových jmen.

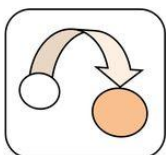
Instalace GRUB do MBR se provádí příkazem `grub-install /dev/hda`, kde *hda* je disk, ze kterého systém bootuje. Totéž lze provést z příkazového řádku GRUB shell (`install` a `setup`).

Při změně konfiguračního souboru není nutno provádět aktualizaci, GRUB si načte konfigurační soubor při spuštění počítače.

GRUB pracuje dvoustupňově. Nejdříve se načte první část z MBR (1. stupeň), spustí kód velký pouze 512 bytů. Jedinou funkcí programu v první fázi je zavést druhou, větší, část zavaděče. Tu vyhledá v souborovém systému (2. stupeň). Až tato druhá část zavaděče umí číst systém souborů a provede vlastní zavádění.

menu.lst

GRUB zobrazuje zaváděcí menu na grafické titulní obrazovce nebo v rozhraní textového režimu. Co bude obsahem této obrazovky, lze nastavit v souboru s menu `/boot/GRUB/menu.lst`. V tomto souboru jsou popsány veškeré informace o diskových oddílech a operačních systémech, které lze zvolit z nabídky při zavádění. GRUB nahraje menu přímo ze souborového systému při každém startu systému.



----- /boot/grub/menu.lst -----

#Všeobecné volby

`default 0` *určuje, že se implicitně spustí OS*
`timeout 30` *GRUB bude čekat na 30 sekund na výběr*

`splashimage=(hd0,7)/grub/splashes/$seachair.xpm.gz`
obrázek pozadí

`password --md5 1ŽwŮ?~Xôć$bEpajjjGr7Ej7HrVy75Lb`
zahaslování

#první položka v menu

`title Linux (2.4.22-1)` *text, který se objeví v menu*
`root (hd0,7)` *oddíl, kde se nachází adresář /boot/*
`kernel /vmlinuz-2.4.22-1 ro root=LABEL=`
cesta k souboru s jádrem

#druhá položka v menu

`title Windows`
`root noverify(hd0,0)`
`chainloader +1` *předává ovládání dalšímu zavaděči*

Konvence pojmenování pevných disků a oddílů[3]

GRUB pojmenovává disky a oddíly podle jiných konvencí, než je zvykem v Linuxu, např. `/dev/hda1`. První disk je vždy odkazován jako `hd0`.

Nerozlišuje mezi IDE, SCSI nebo RAID zařízením. Veškeré pevné disky detekované BIOSem nebo diskovým řadičem jsou číslovány podle pořadí zavádění, jaké je nastaveno v BIOSu.

Protože disky jsou jinak adresovány Linuxem a jinak BIOSem, používá GRUB algoritmus pro mapování a výsledek tohoto algoritmu ukládá do souboru *device.map*.

Soubor *device.map* mapuje zařízení pojmenovaná podle notace programu GRUB na jména podle Linuxové notace

GRUB počítá diskové oddíly od nuly: *hd0,0* tedy odkazuje na první oddíl prvního disku. Označení odpovídá typickému PC s jedním diskem připojeným jako primární master disk. V Linuxu se na něj odkazuje pomocí */dev/hda1*.

Čtyři primární oddíly (které lze na disku vytvořit) jsou číslovány od 0 do 3 a logické oddíly jsou číslovány od 4 výš.

- (*hd0,0*) první primární oddíl prvního disku
- (*hd0,1*) druhý primární oddíl prvního disku
- (*hd0,2*) třetí primární oddíl prvního disku
- (*hd0,3*) čtvrtý primární oddíl prvního disku
- (*hd0,4*) první logický oddíl
- (*hd0,5*) druhý logický oddíl

...

V programu GRUB musí být cesta uvedena jako jméno zařízení, uzavřené do kulatých závorek, následovaná jménem souboru včetně plné cesty na tomto zařízení nebo oddílu. Cesta musí vždy začínat lomítkem. Například v systému s jedním IDE diskem a Linuxem uloženým na prvním oddílu, se odkážete na jádro takto:

(hd0,0)/boot/vmlinuz

Původní první řada GRUB (nejnovější je verze 0.97) je dnes označována jako GRUB Legacy a už není nadále vyvíjena, provádí se pouze opravy chyb. Další vývoj se zaměřuje na GRUB2. Je logickým pokračovatelem první řady, jedná se ale o kompletní přepis původního kódu.

9.4 GRUB 2

Hlavní novinky GRUB2:

- podpora lokalizace,
- možnost zobrazení ne-ASCII znaků,
- podpora modulů,
- vylepšená správa paměti,
- vlastní skriptovací jazyk,
- přesun platformě závislého kódu do modulů.

Konfigurace GRUB 2 se provádí automaticky z automatických skriptů a modulů. Moduly jsou v adresáři */boot/grub*. Mají příponu *mod* a v konfiguračním souboru se volají příkazem *insmod*. Formou modulů je řešena podpora pro png či tga obrázky pozadí, ovladač pro čtení ze souborových systému etx2, ZFS, NTFS a dalších.

Pro konfiguraci se už nepoužívá soubor */boot/grub/menu.lst*, ani */boot/grub/grub.conf*. Nahradil je soubor */boot/grub/grub.cfg*. Podstatný rozdíl je, že tento nový soubor už se ručně needituje, ale je generován specializovanými utilitami, především *update-grub*.

Skript *update-grub* obsahuje:

```
grub-mkconfig -o /boot/grub/grub.cfg
```

Tím se spouští skript, který začne automaticky na základě jiných souborů generovat finální konfiguraci. Pro vyzkoušení je možné vynechat volbu *-o*, výstup se bude vypisovat na obrazovku.

Zdroje pro konfiguraci:

/etc/default/grub

/etc/grub.d/

/etc/default/grub

Obsahuje základní globální konfigurace zavaděče. Lze zde nastavit, která položka bude po startu standardně zvolena, kolik sekund bude GRUB čekat na uživatelský vstup a podobně. Je ručně konfigurovatelný.

adresář */etc/grub.d/*

Jsou to spustitelné bash skripty, které utilita *update-grub* postupně spouští a generují jednotlivé položky do */boot/grub/grub.cfg*.

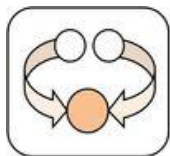
Skripty začínají číslem (podobně jako init skripty) a jsou automaticky spouštěny ve správném pořadí. Čísla nejsou volena náhodně, ale mají vlastní pravidla:

- 00 je rezervováno pro generování hlavičky z konfiguračního souboru
- 10 hlavní bootovací položky
- 20 aplikace třetích stran

Pokud je nutno přidat vlastní položky menu do */boot/grub/grub.cfg*, jsou dvě možnosti. Napsat vlastní skript nebo využít souboru *40_custom*, který je standardně prázdný a je určen právě pro uživatele. Skript může být velmi jednoduchý, jen může prostě vypsát to, co byste postaru vepsali do konfiguračního souboru.

Skripty spouštějí vždy ve stejném pořadí, tím lze ovlivňovat to, jak bude poskládána výsledná konfigurace.

Shrnutí kapitoly



Start a inicializace OS začíná v okamžiku, kdy BIOS předá kontrolu zaváděcímu programu. Zavaděč OS zavede jádro Linux kernel do paměti. Spustí se první proces v systému: proces init. Ten provádí inicializaci systému na základě konfiguračního souboru `/etc/inittab`, odkud se spouští rc-skripty.

V Linuxu je pro zavádění OS k dispozici několik zavaděčů. Nejznámější jsou LILO a GRUB.

LILO (Linux LOader) konfigurace: `/etc/lilo.conf`, uložení do MBR: `/sbin/lilo` a GRUB (the Grand Unified Bootloader) dnes asi nejčastěji používaný.

GRUB Legacy je dynamicky konfigurovatelný. Načítá svou konfiguraci při startu z konfiguračního souboru (změny není třeba ukládat do MBR) nebo je možné řídit zavádění přímo z příkazové řádky GRUB prompt.

GRUB 2 je nová verze, která je postavená na konfiguraci, která se provádí z automatických skriptů a modulů. Pro konfiguraci se generuje konfiguračního souboru `/boot/grub/grub.cfg`.

Kontrolní otázky a úkoly



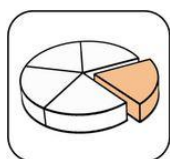
- 1) Jak probíhá start systému?
- 2) Jaké jsou nejznámější zavaděče?
- 3) Jak se konfiguruje GRUB Legacy?
- 4) Jak se konfiguruje GRUB 2?
- 5) Jaký je rozdíl mezi GRUB Legacy a GRUB 2?

Otázky k zamyšlení



- 1) Pokud chceme nainstalovat nový zavaděč, jak budeme postupovat?

Použitá literatura a jiné zdroje:



- [1] GRUB – zavaděč systému. VETVICKA, Jiří. www.suseportal.cz [online]. 10. 11. 2005 [cit. 2012-02-05]. Dostupné z: http://www.suseportal.cz/grub_zavadec_systemu

- [2] KRČMÁŘ, Petr. Poznejte boot loader GRUB2. Wwww.root.cz [online]. 11. 2. 2010 [cit. 2012-02-05]. Dostupné z:
<http://www.root.cz/clanky/poznejte-boot-loader-grub2/>
- [3] KOLEKTIV. SUSE Linux: uživatelská příručka [online]. 1. vyd. Praha: SuSE CR, s.r.o., 2003, 323 s. [cit. 2012-02-11]. ISBN 80-239-1942-3. Dostupné z: http://guidalinux.altervista.org/suselinux-manual_cs-10.1-16/index.html
- [4] SHAH, Steve. Administrace systému Linux: jak porozumět svému počítači : podrobný průvodce začínajícího administrátora. 2. vyd. Praha: Grada, 2003, 533 s. ISBN 80-247-0641-5.

10 Linux: inicializace systému

Obsah hodiny



Obsahem této hodiny je popis inicializace OS Linux, popis procesu init a jeho konfigurace.

Cíl hodiny



Po prostudování budete schopni:

- popsat proces init a jeho konfiguraci,
- orientovat se v `/etc/inittab`,
- charakterizovat rc skripty.

Klíčová slova



init, `/etc/inittab`, run level, rc skript

10.1 Proces init

Poslední akcí jádra při startu OS je spuštění prvního uživatelského procesu – procesu init. Je to první spuštěný proces (PID=1). Inicializuje OS a je spuštěn po celou dobu běhu OS. Je rodičem všech procesů v systému, ošetřuje řadu událostí po celou dobu chodu systému: umožňuje uživatelům se přihlásit se do systému, implementuje úroveň běhu systému, stará se o osířelé procesy, řídí vypínání nebo restart OS, atd. Činnost procesu init řídí konfigurační soubor **`/etc/inittab`**.

10.2 Konfigurační soubor `/init/tab`

Jedná se o textový konfigurační soubor, který má v podstatě formu tabulky. Každý řádek má čtyři položky oddělené dvojtečkou:

id:úroveň_běhu:akce:proces

→ **id neboli návěští:** max. 4 znaky, identifikátor řádky

→ **úroveň:** výčet spouštěcích úrovní (úroveň běhu systému, run levels), pro kterou řádka platí (výjimku tvoří řádek s typem akce `initdefault`),

úrovně se zadávají jako číslíčky bez oddělovače, pokud je položka prázdná, platí pro všechny spouštěcí úrovně.

- **typ_akce:** klíčové slovo určující způsob interpretace řádky, to znamená, jakým způsobem se realizuje příkaz, např.:
- **wait:** provádění příkazu v řádce blokuje další příkazy, čeká se na jeho dokončení – příkaz se provádí na popředí
 - **respawn:** příkaz se opakovaně provádí na pozadí, pokud skončí, je spouštěn znovu, po jeho spuštění se ihned se pokračuje v provádění dalších akcí
 - **once:** příkaz se spustí pouze jednou, jen při prvním přechodu do uvedené úrovně,
 - **powerfail:** umožní procesu init v případě výpadku napájení zastavit systém
 - **ctrlaltdel:** umožňuje procesu init znovu zavést systém, když uživatel současně zmáčkne klávesy Ctrl+Alt+Del.
 - **sysinit:** příkaz, jenž se provede při zavádění systému, tímto způsobem se například obvykle mažou soubory v adresáři /tmp.
 - **boot:** provádí se pouze při startu systému
 - **initdefault:** defaultně nastavuje spouštěcí úroveň při startu, řádek neobsahuje příkaz.
 - ... další jsou uvedeny v manuálových stránkách: inittab(5).
- **příkaz:** příkaz, který se má provést

10.3 Proces init a start systému

Spuštěním procesu init při startu systému se zahájí inicializace OS a ukončí se tak proces zavedení systému. Provede se:

- kontrola souborových systémů,
- "úklid" v adresáři /tmp,
- start obsluhy různých služeb v rámci zavedení příslušného run levelu (spouštěcí úrovně, úrovně běhu systému),
- spuštění procesu getty pro každý terminál nebo virtuální konzolu, getty umožňují přihlašování.

V souboru inittab jsou specifikovány spouštěcí úrovně: 0, 1, 2, 3, 4, 5 a 6. mohou být v různých distribucích specifikovány trochu jinak, ale obvykle mají tento význam:

- 0 Zastavení systému,
- 1 Jednouživatelský režim (pro zvláštní úkoly, spojené s administrací systému),
- 2-5 Běžný provoz (uživatelsky definovaný),

– 6 Znovuzavedení systému.

Úrovně běhu systému se konfigurují v souboru */etc/inittab*.

```
12:2:wait:/etc/init.d/rc 2
```

V prvním poli je uvedeno návěstí, druhé pole znamená, že se tento záznam (řádek) uplatní při úrovni běhu systému číslo 2. Třetí položka (pole *wait*) říká procesu *init*, aby spustil příkaz uvedený ve čtvrtém poli jenom jednou, a to při startu dané úrovně běhu systému a pak vyčkal, než se příkaz provede. Samotný příkaz */etc/init.d/rc* spustí všechny procesy a příkazy uložené v adresáři */etc/init.d/rc* (liší se podle distribucí), které jsou potřebné pro spuštění a ukončení služeb, jimiž se implementuje úroveň běhu číslo 2.

Run level lze za chodu systému změnit pomocí příkazu *telinit* (*telinit run_level*).

Při startu OS se nejprve provedou řádky v poli akce označené: *sysinit*: Pro všechny úrovně se spustí se inicializační skripty z */etc/init.d/rcS*

```
si::sysinit:/etc/init.d/rcS
```

Další v pořadí se provede řádek s akcí *initdefault*. Specifikuje implicitní, run level (úroveň běhu systému) a zajistí tak spuštění správného řádku *inittab* pro daný run level. např.: spuštění runlevel 2:

```
id:2:initdefault:
```

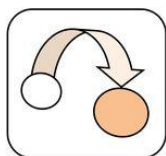
```
12:2:wait:/etc/init.d/rc 2
```

Pozor! Při startu lze jádru předat parametr, kterým se procesu *init* run level vnutí, nastavení *initdefault* se pak ignoruje. Z hlediska bezpečnosti je nebezpečné spuštění v jednouživatelském režimu. Proto je vhodné ošetřit spuštění heslem (při konfiguraci zavaděče).

Po spuštění služeb daného run levelu *init* spouští pro jednotlivé terminály a virtuální konzoly procesy *getty*. Akce *respawn* zajišťuje, že *init* po každém odhlášení uživatele restartuje procesy *getty*. Umožní tím případné další přihlášení jiných uživatelů.

```
2:23:respawn:/sbin/getty tty2 VC linux
```

A takhle vypadá obsah konfiguračního souboru */etc/inittab* pro proces *init*, je převzat z manuálových stránek:



```
# Level to run in
```

```
id:2:initdefault:
```

```
# Boot-time system configuration/initialization
script.
```

```
si::sysinit:/etc/init.d/rcS
```

```

# What to do in single-user mode.
~:S:wait:/sbin/sulogin

# /etc/init.d executes the S and K scripts upon change
# of runlevel.
#
# Runlevel 0 is halt.
# Runlevel 1 is single-user.
# Runlevels 2-5 are multi-user.
# Runlevel 6 is reboot.

10:0:wait:/etc/init.d/rc 0
11:1:wait:/etc/init.d/rc 1
12:2:wait:/etc/init.d/rc 2
13:3:wait:/etc/init.d/rc 3
14:4:wait:/etc/init.d/rc 4
15:5:wait:/etc/init.d/rc 5
16:6:wait:/etc/init.d/rc 6

# What to do at the "3 finger salute".
ca::ctrlaltdel:/sbin/shutdown -t1 -h now

# Runlevel 2,3: getty on virtual consoles
# Runlevel 3: getty on terminal (ttyS0) and modem
(ttyS1)
1:23:respawn:/sbin/getty tty1 VC linux
2:23:respawn:/sbin/getty tty2 VC linux
3:23:respawn:/sbin/getty tty3 VC linux
4:23:respawn:/sbin/getty tty4 VC linux
S0:3:respawn:/sbin/getty -L 9600 ttyS0 vt320
S1:3:respawn:/sbin/mgetty -x0 -D ttyS1

```

10.4 Run level 1

Jedná se o jednouživatelský režim, určený pro správce systému. V tomto režimu běží jenom minimum systémových služeb (včetně možnosti přihlášení do systému). Jednouživatelský režim je nutný pro některé úlohy spojené s údržbou systému.

Riziko této úrovně je v tom, že se předpokládá, že tím uživatelem je root a není vyžadováno přihlášení uživatele. Proto je vhodné ošetřit spuštění jednouživatelského režimu heslem (při konfiguraci zavaděče).

10.5 Run level 0, 6

Spouštěcí úroveň 0, 6 provádí vypnutí OS (0) a restart OS (6). I tyto činnosti má na starost proces `init` a jsou řízeny konfiguračním souborem *inittab*.

Odpojí se nejdříve všechny souborové systémy (kromě kořenového svazku). Všechny uživatelské procesy (je-li někdo stále přihlášen) se ukončí. Před ukončením procesů se uživateli objeví informace o zastavení systému s výzvou k ukončení práce. Ukončí se služby, tj. zastaví se běžící démoni. Nakonec odpojí kořenový souborový systém a `init` vypíše zprávu, že počítač může být vypnut ze sítě.

Vypnutí a restart systému může provést pouze root a to pomocí příkazu *shutdown*:

<i>shutdown -h now</i>	příkaz pro vypnutí OS (alias <code>halt</code>)
<i>shutdown -h 22:00</i>	znamená "vypni se v deset večer"
<i>shutdown -r +30</i>	za půl hodiny rebootuj počítač
<i>shutdown -r now</i>	rebootuj hned teď (alias <code>reboot</code>)
	trojhmat [CTRL] + [ALT] + [DEL]
<i>shutdown -c</i>	zruš běžící čas limit pro vypnutí/restart počítače

10.6 Startovací skripty: rc skripty

Rc-skripty jsou textové soubory, které vykonává shell při startu systému. Spouštějí se z */etc/inittab*, např.:

```
l2:2:wait:/etc/init.d/rc 2
```

Slouží zejména k nastartování služeb v rámci daného run levelu, které pak bude systém poskytovat. Bývají uloženy v */sbin/init.d* u distribuce SuSE, případně v */etc/rc.d* u distribucí vycházejících z distribuce RedHat. Tyto skripty nejen startují služby, ale rovněž je i zastavují nebo zjišťují, zda běží.

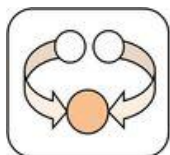
Pomocí rc-skriptů lze jednoduše upravovat konfiguraci spouštěných služeb při startu systému. Pro jednotlivé run levely se spouští přes symbolické odkazy nejčastěji z adresářů */etc/rcn.d* (přesné umístění je v */etc/inittab*)

Jména symbolických odkazů mají obvykle strukturu: *Xnnjmeno*:

- *X* je **S** nebo **K**
- *nn* je dvou (nebo tří) ciferné číslo (pořadí spouštění)
- *jmeno* je jméno služby v adresáři **init.d**

Skripty začínající na velké **S** jsou volány s parametrem **start** příslušnou a službu spustí. Skripty začínající na velké **K** s parametrem **stop**, službu zastaví.

Shrnutí kapitoly



Proces init je první spuštěný proces (PID=1). Inicializuje OS a je spuštěn po celou dobu běhu OS. Je rodičem všech procesů v systému, ošetřuje řadu událostí po celou dobu chodu systému: umožňuje uživatelům se přihlásit se do systému, implementuje úroveň běhu systému, stará se o osiřelé procesy, řídí vypínání nebo restart OS, atd. Činnost procesu init řídí konfigurační soubor */etc/inittab*.

Jedná se o textový konfigurační soubor, který má v podstatě formu tabulky. Každý řádek má čtyři položky oddělené dvojtečkou:

id:úroveň_běhu:akce:proces

V souboru inittab jsou specifikovány spouštěcí úrovně OS 0 - 6.

Proces init ukončuje zavedení systému tím, že se provede:

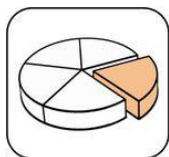
- kontrola souborových systémů,
- "úklid" v adresáři */tmp*,
- start obsluhy různých služeb v rámci zavedením příslušného run levelu (spouštěcí úroveň, úroveň běhu systému), přes RC skripty
- spuštění procesu getty pro každý terminál nebo virtuální konzolu, getty umožňují přihlašování.

Kontrolní otázky a úkoly



- 1) Charakterizujte proces init a jeho úlohu při startu OS.
- 2) Jakým souborem se proces init konfiguruje?
- 3) Popište /etc/inittab.
- 4) Co jsou to RC skripty?
- 5) Co je to run level?

Použitá literatura a jiné zdroje:



- [1] KOLEKTIV AUTORŮ. Linux: Dokumentační projekt. Brno: Computer Press, a.s., 2008. ISBN 978-80-251-1525-1. Dostupné z:
<http://www.root.cz/knihy/linux-dokumentacni-projekt-4-vydani/>
- [2] SHAH, Steve. Administrace systému Linux: jak porozumět svému počítači : podrobný průvodce začínajícího administrátora. 2. vyd. Praha: Grada, 2003, 533 s. ISBN 80-247-0641-5.

11 MS Windows: start systému

Obsah hodiny



Obsahem této hodiny je popis startu operačního systému MS Windows, vysvětlení bootovacího procesu.

Cíl hodiny



Po prostudování budete schopni:

- popsat jednotlivé kroky bootovacího procesu,
- vysvětlit rozdíly mezi bootováním Windows XP a Windows 7.

Klíčová slova



Předbootovací sekvence, Bootovací sekvence, NTLDR, BootMGR, Přihlašovací sekvence, Winlogon

11.1 Před bootovací sekvence

Po zapnutí počítače BIOS provede POST test, načte a zkontroluje MBR. Je-li MBR v pořádku, řízení předá Partition Loaderu (zavaděč prvního stupně). Ten testuje, zda označený oddíl obsahuje platný zavaděcí sektor. Vyhledá v Partition Table aktivní (bootovací, systémový) oddíl¹⁰ a přejde na první - zavaděcí sektor tohoto oddílu, kde je rovněž Boot Record (VBR, Volume Boot Record) a předá mu řízení.

Hlavním úkolem VBR je najít a spustit v souborovém systému v kořenovém adresáři root zavaděcí program (zavaděč druhého stupně), který obsahuje zavaděcí sekvenci OS. DOS/Windows 95/98/ME to byl IO.sys, pro systém Windows NT/2000/XP je to NTLDR, pro Visty a Windows 7 je to BootMGR.

¹⁰ V DOSu lze označit jako aktivní pouze primární diskové oddíly. Z toho důvodu nemůžete použít pro zavádění DOSu logické diskové oddíly, které jsou uvnitř rozšířených oddílů.

11.2 Bootovací sekvence

Začíná po načtení zaváděcího programu do paměti. Jde o skrytý systémový soubor, který se nachází v kořenovém adresáři systémového oddílu. Provádí

- inicializaci,
- výběr OS,
- detekci HW,
- výběr HW konfigurace.

V rámci inicializace startuje mini FAT a NTFS ovladače, které obsahuje přímo ve svém kódu, zapíná stránkování a přepíná procesor z reálného do protected módu. V protected módu a se zapnutým stránkováním zpřístupňuje 32bitové adresování paměti a to znamená, že od této chvíle dokáže pracovat až se 4 GB fyzické paměti. Vyhledá soubory, které ovlivňují start systému.

Pokud v této fázi najde „aktivní“ soubor *Hiberfil.sys*¹¹, předá se startovací proces kódu jádra, který se stará o hibernaci a postupně se obnoví systém do stavu před hibernací.

Pokud soubor *Hiberfil.sys* nalezen není, zavaděč pokračuje dál výběrem OS. Výběr operačního systému včetně parametrů pro jeho zavedení je řízen příslušným konfiguračním souborem.

Dále následuje detekce a konfigurace hardware. Výsledkem je seznam aktuálně nainstalovaných HW komponent. Získané informace jsou následně uloženy v registrech, v klíči:

HKEY_LOCAL_MACHINE\HARDWARE\DESCRIPTION

Pokud je v systému definováno více hardwarových profilů, zobrazí se menu s nabídkou pro výběr. Posledním úkolem zavaděče, než odevzdá řízení jádru, je načíst do paměti ovladače zařízení.

Ovladače mají přesně stanovené pořadí startu, které je zapsané v klíči *HKLM\SYSTEM\CurrentControlSet\Control\ServiceGroupOrder*. Jak jsou ovladače postupně nahrávány, zapisují se o nich informace do registru do klíče *HKLM\SYSTEM\CurrentControlSet\Services*.

Činnost zavaděče je ukončena načtením souborů

- *Ntoskrnl.exe*: jádro systému, přebírá řízení startu
- *Hal.dll* (Hardware Abstraction Layer)

¹¹ Hiberfil.sys mimo jiné obsahuje „full memory image“, tedy uloženou celou paměť ve chvíli hibernace a ARC cestu k boot partition, která byla použita pro start systému před hibernací.

11.3 Bootovací sekvence ve Windows XP

Začíná po načtení zaváděcího programu **NTLDR** (NT Loader) do paměti. Jde o skrytý systémový soubor, který se nachází v kořenovém adresáři systémového oddílu.

Výběr OS: boot.ini

Další soubor, který NTLDR hledá je *boot.ini*. Pokud je *boot.ini* v kořenovém adresáři nalezen načte jeho obsah do paměti a když obsahuje záznamy o více než jednom operačním systému, zastaví se na tomto bodě a vyčká se na uživatelský výběr.

Jestliže NTLDR soubor *boot.ini* v kořenovém adresáři nenajde, pokračuje v bootovací sekvenci nahráním systému z prvního oddílu prvního disku, kterým je běžně C:\.

Detekce a konfigurace HW, aktivace jádra

Pokud je zaváděným systémem Windows 2000 nebo XP. Inicializuje NTLDR soubor *Ntdetect.com*.

Ntdetect.com provede detekci hardware a výběr hardwarové konfigurace počítače. Načte do paměti ovladače zařízení a ukončí činnost načtením souborů

- *Ntoskrnl.exe*,
- *Hal.dll*.

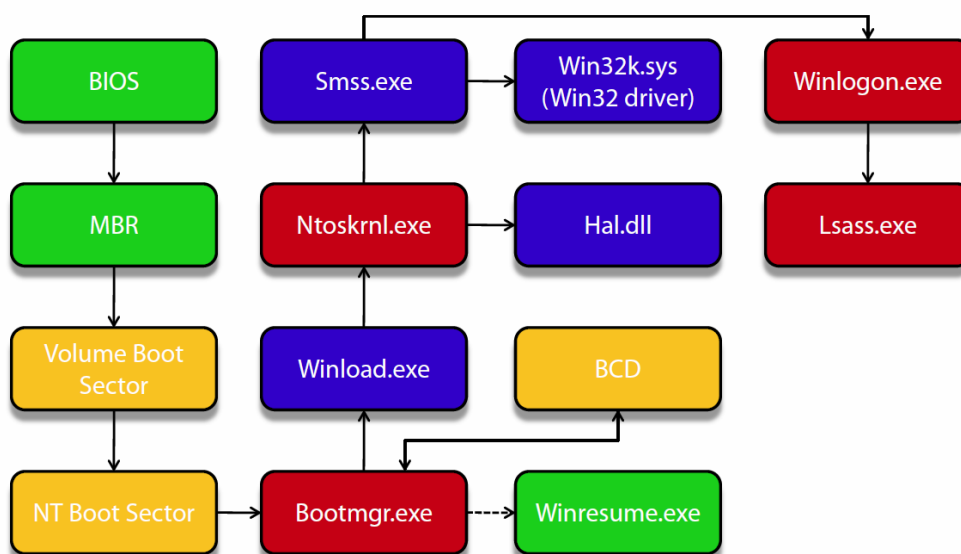
11.4 Bootovací proces ve Windows Vista, Windows 7, Windows Server 2008

Bootovací sekvence začíná po lokalizaci zaváděcího manažeru *bootmgr* - Windows Boot Manager a jeho načtení do paměti. Obvykle je umístěn v *C:\Boot*.

Bootmgr.exe

BootMGR nahrazuje NTLDR. Zahajuje a řídí proces bootování. Podporuje bootování nejen z BIOSU, ale i z EFI. Pokud existují soubory hibernace, spustí *winresume.exe*, pokud ne

- načte informace z BCD a nechá uživatele vybrat systém a
- spustí *winload.exe* (zaváděč systému Windows).



Obrázek 11-1: Bootování ve Windows 7

Výběr OS: BCD

BCD (Boot Configuration Data) nahrazuje soubor *boot.ini*. Je to databáze konfiguračních parametrů pro zavádění různých operačních systémů platformy MS Windows. K editaci, přidávání a odstraňování záznamů v BCD se používá konzolová aplikace *bcdedit.exe*. Existují i pohodlnější grafické utility, např. BellaVista, EasyBCD.

V systémech, které používají BIOS je BCD soubor je uložen na aktivním oddílu (systémový, bootovací) v *\Boot\Bcd* adresáři¹².

Detekce a konfigurace HW, aktivace jádra: Winload.exe

Jedná se o zaváděcí program OS MS Windows. Má za úkol načíst

- *Ntoskrnl.exe* (jádro systému Windows),
- *Hal.dll*,
- ostatní vyžadované soubory, ovladače HW a větev registru SYSTEM.

Posledním úkolem *Winload.exe* je spuštění *ntoskrnl.exe*, což je jádro OS. Další kroky startu a inicializace systému jsou v režii jádra a jsou ve Windows 7 a Windows XP obdobné.

¹² V systémech používajících EFI je BSD v EFI systémovém oddílu.

```

C:\> Správce: C:\WINDOWS\system32\cmd.exe

C:\>bcdedit

Správce spouštění systému Windows
-----
identifikátor           {bootmgr}
device                  partition=X:
description              Windows Boot Manager
locale                  en-US
inherit                  {globalsettings}
default                 {current}
resumeobject             {41175fc7-7a94-11e0-8b3e-5c260a4fc51a}
displayorder             {41175fc8-7a94-11e0-8b3e-5c260a4fc51a}
toolsdisplayorder       {current}
timeout                 5

Zavádecí program pro spouštění systému Windows
-----
identifikátor           {41175fc8-7a94-11e0-8b3e-5c260a4fc51a}
device                  partition=\Device\HarddiskVolume3
path                    \Windows\system32\winload.exe
description              Windows Server 2008 R2
locale                  en-US
inherit                  {bootloadersettings}
recoveryenabled         No
osdevice                partition=\Device\HarddiskVolume3
systemroot              \Windows
resumeobject             {41175fc7-7a94-11e0-8b3e-5c260a4fc51a}
nx                      OptOut
hypervisorlaunchtype    Auto

Zavádecí program pro spouštění systému Windows
-----
identifikátor           {current}
device                  partition=C:
path                    \WINDOWS\system32\winload.exe
description              Windows 7
locale                  cs-CZ
inherit                  {bootloadersettings}
recoverysequence        {eaa2addf-7bc6-11e0-ae50-68a3c44613f4}
recoveryenabled         Yes
osdevice                partition=C:
systemroot              \WINDOWS
resumeobject             {41175fc3-7a94-11e0-8b3e-5c260a4fc51a}
nx                      OptOut

C:\>

```

Obrázek 11-2: Windows 7, soubor BCD

11.5 Co se děje po spuštění *ntoskrnl.exe*

Bootovací proces je předán souboru *Ntoskrnl.exe*. *Ntoskrnl.exe* je považován za mini jádro systému a spolu se souborem *Hall.dll* v této fázi startu počítače inicializují výkonné subsystémy exekutivy, ovladače zařízení, připravují systém na start nativních aplikací a spouští *smss.exe*.

SMSS (*Session Manager*) je zodpovědný za spuštění uživatelského prostředí. Spouští grafický subsystém (*Win32k.sys*) a přihlašovací proces (*Winlogon*).

11.6 Přihlašovací sekvence, *Winlogon.exe*

Soubor *Winlogon.exe* zprostředkovává přihlášení uživatele. Spouští proces *Lsass* (odpovídá za autentizaci uživatele) a *services.exe*.

Proces *Winlogon* koordinuje přihlášení. V rámci přihlašování spouští uživatelův první proces, obsluhuje odhlášení a řídí různé další operace týkající se zabezpečení, včetně zadávání hesel během přihlášení, změny hesel a uzamykání či odemykání pracovní stanice.

Proces *Winlogon* používá při ověřování jména a hesla uživatelského účtu grafickou identifikační a autentizační knihovnu GINA (*Graphical Identification and Authentication*).

Windows dovolují nahradit standardní GINA knihovnu jinými, (v klíči *HKLM\Software\Microsoft\Windows\CurrentVersion\WinLogon\GinaDLL*) a umožňují systému používat rozdílné mechanismy pro identifikaci uživatelů. Výrobci software tak mohou dodat vlastní GINA knihovnu, která používá pro identifikaci uživatelů například zařízení na rozpoznávání otisků prstů a jejich hesla získává ze zašifrované databáze.

Přihlašování uživatele začíná v okamžiku, kdy uživatel stiskne sekvenci *Ctrl + Alt + Delete*. Po jejím stisknutí zavolá proces *Winlogon* knihovnu GINA, pro autentizaci uživatele. Proces *Winlogon* vytvoří pro uživatele jedinečný místní přihlašovací identifikátor SID. V případě, že je uživatel úspěšně přihlášen, dostane se identifikátor SID do tokenu přihlašovacího procesu a to je krok, který chrání přístup k pracovní ploše.

Uživatel je ověřen, *Winlogon* vyhledá v registru klíč a hodnoty *HKLM\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\Winlogon\Userinit* a spustí *Userinit.exe*

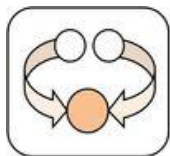
- zavádí uživatelský profil,
- a spustí program *Explorer.exe (... \Winlogon\Shell)*.

Po spuštění *Exploer.exe* *Userinit.exe* končí (proto u procesu *Explorer.exe* není nikdy vidět rodičovský proces).

Po přihlášení uživatele se aktuální stav se uloží jako „*Last known good configuration*“. Start systému je tak dokončen. Je aplikována User a Computer policy a startují programy, dávky a nástroje z různých míst, např.:

- HKCU\Software\Policies\Microsoft\Windows\System\Scripts
- HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Runonce
- HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\policies\Explorer\Run
- HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
- HKCU\Software\Microsoft\WindowsNT\CurrentVersion\Windows\Run
- HKCU\Software\Microsoft\Windows\CurrentVersion\Run
- HKCU\Software\Microsoft\Windows\CurrentVersion\RunOnce
- programy v C:\Winnt\Profiles\All Users\Start Menu\Programs\StartUp

Shrnutí kapitoly



Po zapnutí počítače BIOS provede POST test, načte a zkontroluje MBR. Je-li MBR v pořádku, řízení předá Partition Loaderu (zavaděč prvního stupně). Ten zajistí vyhledání zavaděcího záznamu pro spuštění zavaděče druhého stupně BootMGR.

Bootovací sekvence začíná po načtení zavaděcího programu BootMGR (Windows 7) nebo NTLDR (NT Loader) do paměti.

V rámci bootovací sekvence se provádí

- inicializace,
- výběr OS,
- detekce HW,
- výběr HW konfigurace.

Činnost zavaděče je ukončena načtením souborů

- *Ntoskrnl.exe*: jádro systému, přebírá řízení startu
- *Hal.dll* (Hardware Abstraction Layer)

Windows 7 přináší do bootování změny: BootMGR načítá informace z BCD. BCD (Boot Configuration Data) nahrazuje soubor *boot.ini*. Je to databáze konfiguračních parametrů pro zavádění různých operačních systémů platformy MS Windows. Po výběru OS spustí *winload.exe* (místo *Ntdetect.com*), který provede detekci a konfiguraci HW a na konec spustí *Ntoskrnl.exe*.

Ntoskrnl.exe je považován za mini jádro systému a spolu se souborem *Hal.dll* v této fázi startu počítače inicializují výkonné subsystémy exekutivy, ovladače zařízení, připravují systém na start nativních aplikací a spouští *smss.exe*.

SMSS (Session Manager) je zodpovědný za spuštění uživatelského prostředí. Spouští grafický subsystém (*Win32k.sys*) a přihlašovací proces *Winlogon.exe*.

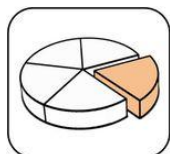
Při startu OS probíhá komunikace s registry – bez údajů z registru (při jeho poškození) by start systému včetně přihlášení uživatele nebyl možný.

Kontrolní otázky a úkoly



- 1) Popište před bootovací sekvenci.
- 2) Popište jednotlivé kroky bootovací sekvence.
- 3) Čím se liší bootovací sekvence ve Windows 7 od předchozích?
- 4) Popište přihlašovací proces

Použitá literatura a jiné zdroje:



- [1] BABINEC, Pavel, Martin OSOVSKÝ, Filip JURNEČKA, Jakub DOBROVOLNÝ, Vít BUKAČ, Martin DEUTSCH a Pavel PISKAČ. Výukové materiály technologií MS: Windows 7 Tutoriál [online]. Ústav výpočetní techniky Masarykovy univerzity, © 2010 [cit. 2012-04-15]. Dostupné z: <http://kurzy.ucn.muni.cz/Win7/>
- [2] Boot Configuration Data Editor Frequently Asked Questions. Technet [online]. April 25, 2007 [cit. 2012-04-15]. Dostupné z: [http://technet.microsoft.com/en-us/library/cc721886\(WS.10\).aspx](http://technet.microsoft.com/en-us/library/cc721886(WS.10).aspx)
- [3] EFI System partition. In: *Wikipedia: the free encyclopedia* [online]. San Francisco (CA): Wikimedia Foundation, May 2006, 3 December 2011 [cit. 2012-04-15]. Dostupné z: http://en.wikipedia.org/wiki/EFI_System_partition

12 Linux: Konfigurace OS

Obsah hodiny



Obsahem této popis možností konfigurace OS Linux.

Cíl hodiny



Po prostudování budete schopni:

- popsat možnosti programování v shellu,
- orientovat se v možnostech konfigurace OS Linux,
- orientovat se v adresáři /etc a /proc a /dev.

Klíčová slova



Skripty, Konfigurační soubory, Konfigurace shellu, Adresář /etc, /dev, Souborový systém /proc

12.1 Skripty

Konfigurace jednotlivých programů Unixových operačních systémů se definuje prostřednictvím **konfiguračních souborů**. Někdy jsou označovány jako „*ini-files*“ (inicializační soubory) nebo „*rc files*“ (řídící soubory) nebo jako „*dot files*“ (soubory, jejichž jména začínají tečkou). Pozor, jména souborů začínající tečkou nejsou normálně příkazem *ls* zobrazena, je nutné přidat volbu *-a* (*all*), která zajistí zobrazení všech souborů, tedy i skrytých.

Řada konfiguračních souborů jsou skripty nebo mají formu tabulky (databáze). Skripty jsou soubory, které obsahují příkazy shellu. V MS Windows se takové soubory označují jako dávkové a mají příponu *.BAT*. Skripty jsou sice výrazně pomalejší než kompilovaný program, ale snadno se vytvářejí a modifikují.

V Linuxu jsou skripty srovnatelné s kompilovatelnými programy. Tvorba skriptů je vlastně programováním v příkazovém interpretu. Ve skriptech lze používat proměnné systémové i uživatelské, lokální i globální, jednoduché i složené (pole), řídící příkazy pro vytváření podmínek a cyklů, funkce.

12.2 Konfigurace příkazového interpretu bash

Pro uživatele je konfigurace systému omezena na konfiguraci příkazového procesoru, shellu.

Existuje několik různých způsobů, jak příkazový procesor neboli shell bash může uživatel spustit.

- Přihlašovací - **login-shell** se automaticky spouští po přihlášení uživatele do systému.
- **Interactive shell** je jakýkoliv příkazový procesor, který se prezentuje příkazovým řádkem. I shell, jenž se spustí bezprostředně po přihlášení se do systému interaktivní. Jiným příkladem interaktivního příkazového interpretu je program *xterm* spuštěný z prostředí X Window.

Existují také **neinteraktivní příkazové interprety**. Tyto procesory se používají k vykonávání skriptů. Pro inicializaci příkazového interpretu se používají tyto skripty:

- *.bash_profile* - spouští se při přihlášení uživatele
- *.bashrc* – spouští se při každém spuštění bash

.bash_profile

Tyto soubory jsou dva. Jeden je uložen v adresáři */etc* a nastavuje jednotné prostředí pro všechny uživatele. Druhý je v domovském adresáři každého uživatele. Uživatel je jeho vlastníkem a může ho editovat.

Do souboru *.bash_profile* se zadávají pouze příkazy, které se mají spouštět při přihlášení se do systému, je to tedy konfigurační soubor pro přihlašovací shell.

Vložením příkazu „*source ~/.bashrc*“. Příkaz *source* „sdělí“ příkazovému procesoru, že má jeho argument interpretovat jako skript. To znamená, že při každém spuštění skriptu *.bash_profile* se spustí skript také *.bashrc*.

.bashrc

Je konfigurační soubor pro neinteraktivní shell bash. Spouští se při každém spuštění bash. Uživatel si do něj nejčastěji ukládá *aliasy* a vlastní nastavení proměnných.

Alias (přezdívka, druhé jméno) je možnost definovat si vlastní příkaz. Vytváří se příkazem *alias*:

alias jméno_příkazu="příkaz/příkazy včetně parametrů"

Příklad: Vytvoření *aliasu* pro příkaz *ls* s parametrem *-la* pro dlouhý výpis včetně skrytých souborů, spojený rourou s příkazem *less* pro stránkovaný výpis:

```
alias lsl="ls -la|less"
```

V souboru *.bashrc* se definují další důležitá konfigurační nastavení prostřednictvím systémových proměnných (*environment variables*). Jejich hodnotu si může uživatel přizpůsobit svým potřebám.

Např. proměnná *PATH* obsahuje adresářů, ve kterých se automaticky vyhledávají programy ke spouštění. K původní hodnotě *PATH* si uživatel může přidat svůj vlastní adresář se skripty:

```
PATH=$PATH://home/pepa/bin
```

V příkazové řádce by to vypadalo takto:

```
/home/pepa# echo $PATH
/home/pepa# /bin:/usr/local/bin:/usr/bin/X11
/home/pepa# PATH=$PATH:/home/pepa/bin
```

Do *PATH* pomocí *=* nastavíme nejprve původní hodnotu proměnné *PATH* (*\$PATH*) a přidáme svůj adresář. Své adresáře z důvodu bezpečnosti uvádíme vždy jako poslední.

```
/home/pepa# echo $PATH
/home/pepa#
/bin:/usr/local/bin:/usr/bin/X11:/home/pepa/bin
```

12.3 Adresář /etc

Konfigurace OS, všech jeho služeb je uložena v textových souborech, které jsou uloženy převážně v adresáři */etc*. Mají většinou formu skriptů, případně tabulky (např. */etc/passwd*, */etc/fstab*, */etc/inittab*). Oprávnění je editovat má pouze správce systému, tedy uživatel *root*.

Adresář */etc* obsahuje hlavní konfigurační soubory OS a dále je v něm řada podadresářů, které obsahují konfiguraci pro jednotlivé aplikace, služby. Název těchto adresářů odpovídá názvu služby. Např. adresář *mc* obsahuje konfigurační soubory pro *mc* (*Midnight Commander*), *apache* obsahuje konfiguraci *webového serveru*.

Některé důležité soubory z adresáře */etc*:

Skripty nebo adresáře skriptů, které se spouští při startu, nebo v případě, že se mění úroveň běhu systému:

```
/etc/rc      /etc/rc.      d /etc/rc?.d
```

<i>/etc/passwd</i>	Databáze uživatelů systému s informacemi o uživatelských i systémových účtech.
<i>/etc/shadow</i>	Zašifrovaná hesla a omezení pro hesla, jako např. doba platnosti hesla.
<i>/etc/fstab</i>	Seznamy FS připojovaných automaticky při startu příkazem <code>mount -a</code> . Soubor <code>fstab</code> má typicky svou vlastní manuálovou stránku v sekci 5.
<i>/etc/mtab</i>	Seznam aktuálně připojených FS.

Seznam aktuálně připojených souborových systémů. Jeho obsah po zavedení systému a připojení určených souborových systémů prvotně nastavují inicializační skripty, v běžném provozu pak automaticky příkaz `mount`. Používá se v případech, kdy je potřeba zjistit, které souborové systémy jsou připojené, například při zadání příkazu `df`.

<i>/etc/group</i>	Soubor popisuje pracovní skupiny.
<i>/etc/inittab</i>	Konfigurační soubor procesu <code>init</code> .
<i>/etc/security</i>	Soubor identifikuje zabezpečené terminály, tedy terminály, ze kterých se může přihlašovat superuživatel.
<i>/etc/shells</i>	Seznam shellů
<i>/etc/hosts</i>	Obsahuje seznam známých počítačů (v lokální síti).
<i>/etc/services</i>	Překládá názvy síťových služeb na číslo portu/protokolu.
<i>/etc/inetd.conf</i> , <i>/etc/xinetd.conf</i>	soubory pro konfiguraci superserveru pro síťové služby.

12.4 Adresář */dev*

Adresář */dev* obsahuje speciální soubory všech zařízení. Speciální soubory jsou pojmenované podle určitých konvencí. Speciální soubory se vytváří v průběhu instalace operačního systému, v běžném provozu pak skriptem `/dev/MAKEDEV`.

Pokud ve skriptech odkazujeme na zařízení, tak vždy právě přes tyto speciální soubory.

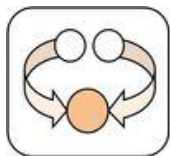
12.5 Souborový systém */proc*

Systém souborů */proc* je vlastně imaginárním souborovým systémem. Ve skutečnosti na disku neexistuje. Místo toho jej v paměti vytváří jádro systému. Ze systému souborů */proc* lze získávat různé aktuální informace o systému (původně o procesech – z toho je odvozeno jeho jméno).

Některé programy zobrazují informace načtené ze souborů */proc*. Například program *free* zobrazuje informace z */proc/meminfo*.

<i>/proc/1</i>	Adresář s informacemi o procesu číslo 1. Každý z procesů má v adresáři <i>/proc</i> vlastní podadresář, jehož jméno je stejné jako identifikační číslo procesu.
<i>/proc/cpuinfo</i>	Různé informace o procesoru. Například typ, výrobce, model, výkon a podobně.
<i>/proc/device</i>	Seznam ovladačů zařízení konfigurovaných pro aktuálně běžící jádro systému.
<i>/proc/dma</i>	Informuje o tom, které kanály DMA jsou právě využívány.
<i>/proc/filesystems</i>	Souborové systémy konfigurované v jádru systému.
<i>/proc/interrupts</i>	Informuje o tom, která přerušení jsou využívána a kolikrát nastala.
<i>/proc/ioports</i>	Informuje o tom, které ze vstupně-výstupních portů se momentálně využívají.
<i>/proc/kcore</i>	Obráz fyzické paměti systému. Má velikost odpovídající velikosti fyzické paměti systému. Ve skutečnosti ale samozřejmě nezabírá takovéto množství paměti, protože jde o soubor generovaný „na požádání“, tedy pokaždé jenom v okamžiku, kdy k němu různé programy přistupují.
<i>/proc/meminfo</i>	Informace o využití paměti, jak fyzické, tak virtuální.
<i>/proc/modules</i>	Informuje o tom, které moduly jádra jsou právě zavedeny v paměti.
<i>/proc/net</i>	Informace o stavu síťových protokolů.
<i>/proc/uptime</i>	Informuje o tom, jak dlouho systém běží.
<i>/proc/version</i>	Verze jádra systému.

Shrnutí kapitoly



Konfigurace jednotlivých programů Unixových operačních systémů se definuje prostřednictvím konfiguračních souborů. Někdy jsou označovány jako „ini-files“ (inicializační soubory) nebo „rc files“ (řídící soubory) nebo jako „dot files“ (soubory, jejichž jména začínají tečkou).

Řada konfiguračních souborů v Linuxu má formu skriptů nebo tabulky (databáze). Skripty jsou soubory, které obsahují příkazy shellu.

Konfigurace OS, všech jeho služeb je uložena v textových souborech, které jsou uloženy převážně v adresáři `/etc`. Oprávnění je editovat má pouze správce systému, tedy uživatel `root`.

Adresář `/etc` obsahuje hlavní konfigurační soubory OS a dále je v něm řada podadresářů, které obsahují konfiguraci pro jednotlivé aplikace, služby.

Adresář `/dev` obsahuje speciální soubory všech zařízení.

Systém souborů `/proc` je pouze virtuální. V paměti jej vytváří jádro systému. Ze systému souborů `/proc` lze získávat různé aktuální informace o systému.

Kontrolní otázky a úkoly



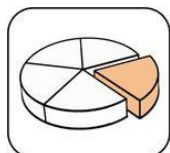
- 1) Jakým způsobem se konfiguruje OS a služby OS v unixových systémech?
- 2) Jakou formu mají konfigurační soubory v Linuxu?
- 3) Kde je uložena většina konfiguračních souborů?
- 4) Co je obsahem adresáře `/dev`?
- 5) Co je to `/proc`?

Otázky k zamyšlení



- 1) V čem je výhoda textových konfiguračních souborů?

Použitá literatura a jiné zdroje:



- [1] /KOLEKTIV AUTORŮ. Linux: Dokumentační projekt. Brno: Computer Press, a.s., 2008. ISBN 978-80-251-1525-1. Dostupné z: <http://www.root.cz/knihy/linux-dokumentacni-projekt-4-vydani/>

- [2] SHAH, Steve. Administrace systému Linux: jak porozumět svému počítači : podrobný průvodce začínajícího administrátora. 2. vyd. Praha: Grada, 2003, 533 s. ISBN 80-247-0641-5.

13 MS Windows: Registry

Obsah hodiny



Obsahem této hodiny je popis registru v MS Windows.

Cíl hodiny



Po prostudování budete schopni:

- charakterizovat registr a jeho úlohu při konfiguraci systému,
- orientovat se v jeho struktuře,
- popsat hlavní klíče a jejich funkci.

Klíčová slova



Registr, Klíč, Hkey_Local_Machine, Hkey_Current_Config, Hkey_Classes_Root, Hkey_Current_Users

13.1 Co je to registr

Veškerá nastavení (konfigurace systému, služeb, aplikací, politik, účtů, atd.) se ukládají do registru. Registr nahrazuje většinu textových konfiguračních souborů používaných ve starších systémech (INI ve Windows 3.x, MS-DOS: *Autoexec.bat* a *Config.sys*). Je to databáze všech systémových informací a nastavení jako např.:

- profily jednotlivých uživatelů,
- aplikace nainstalované v počítači a typy dokumentů, které mohou jednotlivé aplikace vytvářet,
- nastavení stránek vlastností složky a ikony aplikací,
- informace o hardwaru existujícím v systému, o používaných portech.

Informace uložené v registru systém Windows neustále používá během všech operací. Každá změna v systému (například instalace nové aplikace, přidání nebo naopak odebrání hardware) se promítne do registru. Registr se odpovídajícím způsobem automaticky upraví.

Registr má hierarchickou, stromovou strukturu. Tvoří ho podregistry, tj. skupiny skupiny klíčů, podklíčů a hodnot. Jejich kořen je umístěn na vrcholu hierarchické struktury registru. Obsah podregistru je popsán

jedním souborem a souborem s příponou LOG, tyto soubory jsou uloženy ve složkách

- *c:\Windows\System32\Config*
- *c:\Documents and Settings\jméno_uživatele.*

Podregistry se nazývají také soubory registru nebo soubory s protokolem registru.

Většina souborů registru (*DEFAULT*, *SAM*, *SECURITY*, *SOFTWARE* a *SYSTEM*), kromě souboru pro podregistr *HKEY_CURRENT_USER*, je standardně uložena ve složce:

%SystemRoot%\System32\Config.

HKEY_CURRENT_USER: "%SystemRoot%\Profiles\Uživatelské_jméno.

Ve Windows řady s DOS jádrem mělo uložení registrů v souborech jednodušší organizaci. Registry tvořily dva soubory:

- *SYSTEM.DAT*,
- *USER.DAT*.

Registr v 64bitových verzích systémů Windows XP, Windows Server 2003, Windows Vista, Windows 7 je rozdělen do 32bitových a 64bitových klíčů. Mnoho 32bitových klíčů má stejné názvy jako jejich 64bitové protějšky a naopak.

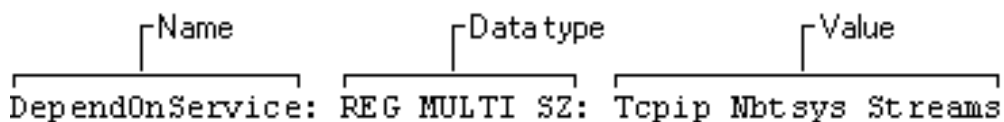
Registry udržuje komponenta jádra, jejich změna se provádí automaticky prostřednictvím grafických utilit. Aplikace, uživatelé a správce konfigurují nastavení přes ovládací panely. Správce má pro přímý vstup k dispozici Editor registrů (*regedit.exe*) a další nástroje, které slouží k optimalizaci, opravě registrů (*Tweak nástroje*).

13.2 Struktura registru

Registr obsahuje klíče a podklíče. Klíče jsou něco jako adresáře (složky). Každý klíč nebo podklíč registru může obsahovat data nazývaná položky. V některých položkách jsou uloženy informace platné pouze pro určitého uživatele, v jiných údaje vztahující se na všechny uživatele daného počítače.

Položka má tři části. Tyto tři části položky se vždy zobrazují v následujícím pořadí:

- název hodnoty,
- datový typ hodnoty,
- vlastní hodnota.



Obrázek 13-1: Položka klíče

V registru se používají hodnoty různých datových typů, ukládají a zobrazují se většinou binárně, některé jako text.

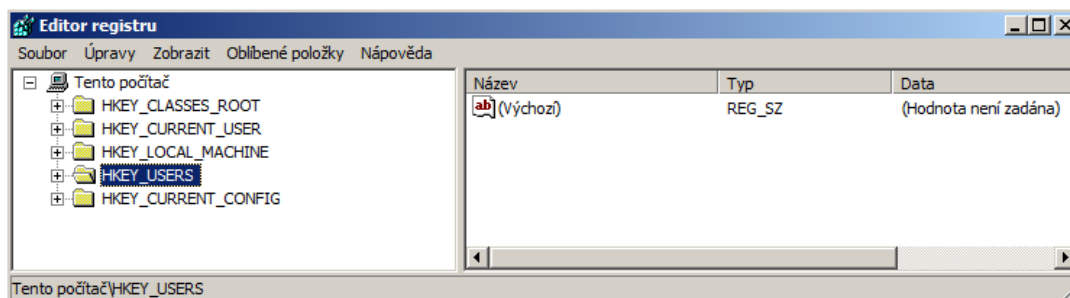
REG_BINARY	Neformátovaná binární data. Většina informací o hardwaru se ukládá ve formě binárních dat a <i>Editor registru</i> je zobrazuje v šestnáctkovém formátu.
REG_DWORD	Údaje reprezentované číslem o délce 4 bajty. Tento typ je využíván velkým množstvím parametrů ovladačů zařízení a služeb. <i>Editor registru</i> je zobrazuje v binárním, šestnáctkovém nebo desítkovém formátu.
REG_EXPAND_SZ	Datový řetězec proměnné délky. K tomuto typu dat patří proměnné vyhodnocované v okamžiku, kdy si program nebo služba příslušná data vyžádá.
REG_MULTI_SZ	Řetězec s více než jednou hodnotou. Tohoto typu jsou zpravidla hodnoty tvořené seznamem několika údajů určených k přímému zobrazování v uživatelském rozhraní. Jednotlivé položky jsou odděleny mezerami, čárkami nebo jinými znaky.
REG_SZ	Textový řetězec pevné délky.
REG_FULL_RESOURCE_DESCRIPTOR	Sada vnořených polí určená k ukládání seznamu prostředků hardwarové součásti nebo ovladače.

Tabulka 1: Datové typy v registrech

Registr se člení na dva podstromy, které se dále větví. Aby bylo vyhledávání informací v registru snadnější, zobrazují nástroje *Editoru registru* pět podstromů, přičemž tři z nich jsou aliasy jiných částí registru.

- *Hkey_Local_Machine* → informace globálního charakteru o instalovaném HW, nastavení aplikací:
 - *Hkey_Current_Config* → aktuální konfigurace,
 - *Hkey_Classes_Root* → nastavení programů.

- *Hkey_Users* → info o všech přihlášených uživateli, nastavení platná pro jednotlivé uživatele:
 - *Hkey_Current_Users* → ukazuje do *Hkey_Users* na aktuálně přihlášeného uživatele.



Obrázek 13-2: Editor registru - výpis základních klíčů

HKEY_LOCAL_MACHINE

Klíč *HKEY_LOCAL_MACHINE*, zkráceně HKLM, sdružuje informace o konfiguraci počítače (HW i SW) platného pro všechny uživatele. Konfigurace zde uložené mají globální charakter a nahrávají se už při bootování systému. K informacím přistupují jak různé aplikace, tak uživatelé.

Obsahuje informace o místním počítačovém systému včetně údajů o hardwaru a operačním systému, jako je například typ sběrnice, systémová paměť, ovladače zařízení a ovládací data pro spouštění systému.

HKEY_CURRENT_CONFIG

Tento klíč je částí *HKEY_LOCAL_MACHINE* a ukazuje na podstrom *HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Hardware Profiles\Current*.

Obsahuje informace o hardwarovém profilu používaném místním počítačem při spuštění systému. Tyto informace slouží ke konfiguraci nastavení, například ovladačů zařízení, které mají být načteny, a rozlišení obrazovky.

HKEY_CLASSES_ROOT

Zde uložené informace zajišťují asociaci souborů s aplikacemi. To znamená, že se při otevření souboru spustí správná aplikace. Jsou uloženy ve dvou klíších:

- *HKEY_LOCAL_MACHINE\Software\Classes* obsahuje výchozí nastavení, které lze použít pro všechny uživatele místního počítače.
- *HKEY_CURRENT_USER\Software\Classes* obsahuje nastavení, které platí pouze pro interaktivního uživatele a přepíše výchozí nastavení.

Klíč *HKEY_CLASSES_ROOT* slučuje informace z těchto dvou zdrojů, zobrazuje je a poskytuje programům. Pozor! Změny je třeba provádět v příslušných klíčích.

HKEY_USERS

HKEY_USERS, zkráceně HKU obsahuje uživatelské profily jednotlivých uživatelů. V *Default* je varianta, která se použije při prvním přihlášení nového uživatele.

Jeho podklíčem je *HKEY_CURRENT_USER*. Obsahuje profil uživatele, který je právě interaktivně (nikoli vzdáleně) přihlášen, včetně proměnných prostředí, připojení k sítím, nastavení tiskáren a programových předvoleb.

Jedná se o nastavení právě přihlášeného uživatele, například konfigurace jednotlivých aplikací, seznam některých programů, které se spouštějí ihned po přihlášení, nastavení Ovládacích panelů apod.

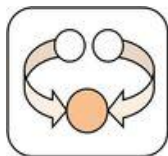
Tento podstrom je aliasem podstromu **HKEY_USERS** a ukazuje na podstrom **HKEY_USERS\Default** zabezpečení aktuálního uživatele.

13.3 Zabezpečení registru

Registr obsahuje citlivá data o počítači a o aplikacích a souborech, které jsou v něm uloženy. Uživatel se zlými úmysly může prostřednictvím registru vážně poškodit počítač. Proto je důležité udržovat vysokou úroveň zabezpečení registru.

Registru je standardně přidělena vysoká úroveň zabezpečení. Správci mají úplný přístup k celému registru, zatímco jiní uživatelé mají obecně úplný přístup ke klíčům vztahujícím se k jejich vlastním uživatelským účtům (jako je klíč *HKEY_CURRENT_USER*) a přístup jen pro čtení ke klíčům vztahujícím se k počítači a jeho softwaru. Uživatelé nemají přístup ke klíčům vztahujícím se k účtům jiných uživatelů. Uživatel s příslušnými oprávněními k danému klíči může provádět změny oprávnění přístupu k tomuto klíči a ke klíčům v něm obsaženým.

Shrnutí kapitoly



Registr je centrální systémová databáze, udržovaná komponentou jádra. Má hierarchickou strukturu. Je určen k ukládání informací potřebných ke konfiguraci systému, aplikací a hardwarových zařízení pro jednoho nebo více uživatelů.

Registr obsahuje klíče a podklíče. Klíče jsou něco jako adresáře (složky). Jejich obsahem jsou jednotlivé položky – hodnoty nebo další klíče. Pro práci s registry se používají speciální programy.

Registr se člení na několik základních klíčů, které se dále větví. Dva ze základních klíčů jsou hlavní a ostatní jsou vlastně odkazy na důležité větve v nich:

- *Hkey_Local_Machine* → informace globálního charakteru o instalovaném HW, nastavení aplikací
 - *Hkey_Current_Config* → aktuální konfigurace
 - *Hkey_Classes_Root* → nastavení programů
- *Hkey_Users* → info o všech přihlášených uživatelích, nastavení platná pro jednotlivé uživatele
 - *Hkey_Current_Users* → ukazuje do *Hkey_Users* na aktuálně přihlášeného uživatele

Kontrolní otázky a úkoly



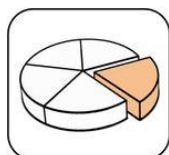
- 1) Co je to registr?
- 2) Jaká je funkce registru?
- 3) Jaké hlavní klíče tvoří registr a co je v nich uloženo?

Otázky k zamyšlení



- 1) Jaké jsou výhody a nevýhody registrů v MS Windows v porovnání s textovými konfiguračními soubory v OS Linux?

Použitá literatura a jiné zdroje:



- [1] Nástroje pro konfiguraci a správu: Registr [online]. © 2012 [cit. 2012-04-15]. Dostupné z: [http://technet.microsoft.com/cs-cz/library/cc778047\(v=ws.10\).aspx](http://technet.microsoft.com/cs-cz/library/cc778047(v=ws.10).aspx)

14 Windows: práce s registry

Obsah hodiny



Obsahem této hodiny je seznámení s nástroji pro práci s registry.

Cíl hodiny



Po prostudování budete schopni:

- orientovat se v možnostech úpravy registrů,
- charakterizovat nástroje pro práci s registry.

Klíčová slova



Regedit, Tweak nástroje

Registr Windows je v podstatě jedno velké a rozsáhlé bludiště plné obtížně čitelných konfiguračních údajů. Změny se provádí automaticky, působí je aplikace (instalace, odinstalování), uživatelé. Aplikace, uživatelé včetně správce konfiguruji nastavení přes ovládací panely. Kromě toho má správce pro přímý vstup k dispozici *Editor registrů* (*regedit.exe*) a další nástroje, které slouží k optimalizaci, opravě registrů (*Tweak nástroje*).

14.1 Editor registrů

Editor registru (standardně *REGEDIT.EXE*, *REGEDIT32.EXE*) je program, který přímo zobrazuje stromovou strukturu této systémové databáze, podobně jako třeba Průzkumník Windows. Umožňuje prohlížet složky – klíče a soubory – hodnoty klíčů registru.

Editor registru je nástroj určený pro pokročilé uživatele. Používá se nejen ke zobrazení, ale i ke změně nastavení systémového registru, k jeho zálohování nebo obnově.

Registr lze otevírat z příkazové řádky zadáním *regedit.exe*. Příkazový řádek se v tomto případě otevírá se zvýšeným oprávněním přes nabídku *Spustit jako správce (Run As)*.

Změny registru obvykle není nutné provádět a ani se to nedoporučuje. Jsou v něm totiž obsaženy složité systémové informace, které jsou životně důležité pro počítač. Nesprávná změna registru, poškození registru může

mít vážné následky pro OS, aplikace a může způsobit nefunkčnost počítače.

Někdy dochází k problémům, které vyžadují ruční zásah do registru. Důrazně se doporučuje před každým takovým zásahem registr zálohovat. (Např. programem *backup*). Změny je vhodné provádět pouze u známých hodnot. Je proto nutné si vždy předem zjistit, jakým způsobem postupovat. Úprava registru vyžaduje přesné znalosti, nelze postupovat intuitivně.

Pro účely řešení případných potíží je vhodné průběžně evidovat seznam provedených změn.

14.2 Funkce regedit

Běžně je možno vyhledávat a provádět různé změny klíčů a hodnot:

- Nalezení řetězce, hodnoty nebo klíče,
- Přidání klíče registru,
- Přidání hodnoty do položky klíče registru,
- Změna hodnoty,
- Odstranění klíče nebo hodnoty registru,
- Přejmenování klíče nebo hodnoty registru,
- Zkopírování názvu klíče registru.

Dále *regedit* umožňuje:

- Vzdálené připojení k registru a jeho správu,
- Obnovení registru,
- Export, import registru nebo jeho částí,
- Načtení a uvolnění podregistru.

Vzdálená správa

Příkaz *Připojit síťový registr* v nabídce umožňuje vzdálené připojení k registru a jeho správu. Musí být zapnuta služba *Vzdálený registr*.

Obnovení registru

Pokud jsou některé klíče nebo hodnoty v klíči registru *HKLM\System\CurrentControlSet* odstraněny nebo jim jsou přiřazeny nesprávné hodnoty, bude pravděpodobně nutné registr obnovit, aby bylo možné dále používat počítač. Je třeba:

- Spustit program *Editor registru*;
- Přes *Start* vypnout systém;
- Spustit počítač, po zobrazení zprávy *Vyberte operační systém, který chcete spustit* stisknout klávesu F8;

- Vybrat položku *Poslední známá funkční konfigurace*. Aby byly funkční klávesy se šipkami na numerické klávesnici, je třeba vypnout režim NUM LOCK;
- Spustit OS.

Export, import registru nebo jeho částí

Editor registru nabízí řadu příkazů, které jsou určeny především pro účely údržby systému.

Editor registru může přes nabídku v *soubor/export* vyexportovat registr do textového souboru nebo do souboru podregistru. Soubory registru lze ukládat ve formátu systému Windows, jako registrační soubory, binární soubory podregistru nebo jako textové soubory. Soubory registru se ukládají s příponou REG a textové soubory s příponou TXT. Se soubory registru vytvořenými při exportu lze pracovat pomocí textového editoru.

Nabídka *soubor/importovat* v Editoru registru umožňuje importovat všechny typy souborů registru včetně textových souborů a souborů podregistru.

Načtení a uvolnění podregistru

Příkazy *Načíst podregistr* a *Uvolnit podregistr* umožňují dočasné stažení části systému do jiného počítače za účelem údržby. Mají vliv pouze na klíče *HKEY_USERS* a *HKEY_LOCAL_MACHINE* a budou aktivní, pouze pokud jsou tyto předdefinované klíče vybrány.

Když se do registru načte podregistr, stane se podregistr podklíčem jednoho z těchto klíčů.

Aby mohl být podregistr načten nebo obnoven, je třeba jej nejprve uložit jako klíč.

14.3 Řízení přístupu k registru

Vzhledem k tomu, že členové skupiny *Administrators* mají k registru úplný přístup, měli by být v této skupině pouze uživatelé, kteří tento přístup skutečně potřebují. Jinou možností je pomocí *Editoru registru* nastavit oprávnění přístupu k určitým klíčům a podstromům nebo odebrat *Editor registru* z počítačů uživatelů, kterým chcete zabránit v provádění změn v registru.

Editor je vhodné spouštět z účtu *Administrator* pouze v případě, že je potřeba zobrazit nebo změnit klíče, ke kterým jinak není přístup.

Ke spuštění *Editoru registru* z účtu *Administrator* nebo z účtu jiného uživatele je lepší se přihlásit jako člen skupiny *Users* a používat příkaz *Spustit jako*.

14.4 Další nástroje pro práci s registry

Další nástroje, které slouží buď k optimalizaci, čištění registru nebo opravení registru. Jsou to speciální programy, které obecně procházejí záznamy registru a vyhledávají ukazatele na neexistující soubory, osiřelé záznamy a další nesrovnalosti. Po dokončení skenování nabízí možnost opravy formou smazání podezřelých klíčů (CCleaner, freeware).

Čistící nástroje je třeba používat velmi opatrně. Nevhodně smazaný klíč, může způsobit vážné problémy. Na druhou stranu pokud nástroj dokáže vyhledat a smazat ten správný klíč, může to nestabilnímu systému velice prospět.

Některé nástroje umožňují pohodlnější práci s obsahem registru. Je možné pořídit je buď jako komerční software nebo freeware či shareware. Někdy se označují často jako Tweak nástroje (patří sem i TweakUI od Microsoftu).

Regeditx (Freeware)

Rozšíření standardního regeditu. Umožňuje rychlejší práci s klíči registru pomocí záložek, historie. Obsahuje adresní řádek, do kterého lze nakopírovat adresu hledaného klíče a rychle se na něj dostat. Podporuje zkratky názvů hlavních klíčů. Vyhledávání je několikanásobně rychlejší díky možnosti indexace Registru.

Registry workshop

Registry Workshop je pokročilý editor registru. Kromě všech standardních funkcí má řadu dalších, které umožňují pracovat s registrem rychleji a efektivněji. Např. funkce pro porovnání registrů mezi počítači, zálohování a obnovu, defragmentaci, undo funkce, kontextové navigační menu, historie, adresní řádek, funkce drag & drop a další.

Registrar Registry Manager (Verze Lite je free, jinak komerční)

Pokročilý a velmi kvalitní editor registru. Poskytuje uživatelsky přívětivé rozhraní, které umožňuje rychle najít klíče a hodnoty. Při procházení registru lze používat navigační tlačítka, funkci drag & drop. K dispozici má adresní řádek pro okamžitý přístup ke klíči registru. Umožňuje přidávat poznámky ke klíčům a jejich hodnotám. Mezi další funkce patří informace o klíčích a celkovém počtu podklíčů a hodnot, zálohování a obnova registru, otevření a editace vzdáleného registru, porovnání registru, defragmentace, monitoring aktivity v registru, editování monitorovaných položek. Podporuje zkratky (např. HKCU, HKLM), obsahuje různé tipy pro úpravy registru.

Registry Mechanic

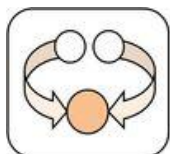
Program pro optimalizaci a čištění registru. Používá vyspělý algoritmus pro detekci problémů s integritou registru - s neplatnými či poškozenými

položkami. Na závěr skenování vytvoří seznam nalezených problémů, které lze následně podle vlastního výběru opravit, ignorovat nebo ponechat. Umožňuje defragmentaci registru a vytvoření záloh opravovaných položek registru.

WinASO Registry Optimizer (Shareware)

Kvalitní program k optimalizaci a čištění registru Windows. Je to profesionální produkt. Jeho pokročilý skenovací algoritmus může otestovat celý registr během několika sekund a objevit zastaralé a neplatné položky, jakož i další chyby registru. Zobrazí je přehledně ve výsledné zprávě a je možno si vybrat položky k opravě. Po opravě se vytvoří automaticky záloha opravených položek pro pozdější případnou obnovu. Program obsahuje funkce pro ochranu soukromí - smazání historie vaší aktivity na počítači, smazání neaktivních zástupců programu, utility pro optimalizaci systému, defragmentaci registru, odinstalování programů, spravuje i programy spouštěné po startu.

Shrnutí kapitoly



Aplikace, uživatelé včetně správce konfigurují nastavení přes ovládací panely. Kromě toho má správce pro přímý vstup k dispozici *Editor registrů* (*regedit.exe*) a další nástroje, které slouží k optimalizaci, opravě registrů (*Tweak* nástroje).

Editor registru je nástroj určený pro pokročilé uživatele. Používá se ke zobrazení a změně nastavení systémového registru, k jeho zálohování nebo obnově.

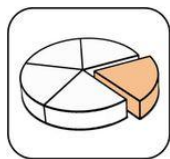
Změny registru obvykle není nutné provádět a ani se to nedoporučuje. Jsou v něm totiž obsaženy složité systémové informace, které jsou životně důležité pro počítač. Nesprávná změna registru by mohla způsobit nefunkčnost počítače.

Někdy však dojde k problémům, které vyžadují ruční zásah do registru. Důrazně se doporučuje před každým takovým zásahem registr zálohovat. Úprava registru vyžaduje přesné znalosti, nelze postupovat intuitivně.

Kontrolní otázky a úkoly



- 1) Jak se provádí změny v registru?
- 2) Jaké nástroje se používají ruční změny v registru?
- 3) Jaké jsou funkce editoru registru?
- 4) Proč se nedoporučuje ručně zasahovat do registru?

***Použitá literatura a jiné zdroje:***

- [1] Editor registru. Microsoft TechNet [online]. © 2012 Microsoft [cit. 2012-04-17]. Dostupné z: <http://technet.microsoft.com/cs-cz/library/cc755256.aspx>
- [2] Registr. Microsoft TechNet [online]. © 2012 Microsoft [cit. 2012-04-17]. Dostupné z: <http://technet.microsoft.com/cs-CZ/library/a39b9bc9-89ec-4cfb-b31e-144613ad63c8>

15 Konfigurace síťového rozhraní, sítě

Obsah hodiny



Obsahem této hodiny je popis síťového rozhraní a jeho konfigurace, IP adresování.

Cíl hodiny



Po prostudování budete schopni:

- charakterizovat síťové rozhraní z hlediska HW,
- popsat adresování definované protokolem IPv4,
- orientovat se v adresách protokolu IPv6,
- popsat konfiguraci síťového rozhraní.

Klíčová slova



NIC, MAC adresa, IPv4, IPv6, IP adresa, Síťové rozhraní, Síťová adresa, Síťová maska, Broadcastová adresa, Loopback, Unicast, Anycast, Multicast

15.1 Síťové rozhraní

Aby byla vůbec možná komunikace s ostatními zařízeními v síti, je obvykle nutné mít v počítači nějaké síťové zařízení – síťovou kartu.

Síťová karta - Network Interface Controller, zkratka NIC je aktivní zařízení, které umožňuje vzájemnou komunikaci počítačů v počítačové síti.

Síťová karta má v paměti firmware. Připravuje a převádí data na elektrické nebo optické signály tak, aby mohly být přenášeny po přenosovém mediu. Kontroluje tok dat mezi dvěma koncovými uzly (síťovými kartami). Karty odesílajícího a přijímajícího počítače se dohodnou na vlastnostech komunikace (např.: musí najít společnou přenosovou rychlost). Po stanovení všech detailů pro komunikaci zahájí obě karty vysílání a přijímání dat.

V lokálních sítích se většinou používají ethernetové síťové karty. Každá ethernetová síťová karta má od výrobce stanoven jedinečný 6B identifikátor - MAC adresu (fyzická nebo hardwarová adresa).

- 3B kód výrobce,
- 3B identifikace u výrobce.

MAC adresu lze nastavit pomocí speciálního programu přímo v EEPROM síťové karty nebo pomocí ovladače.

Síťové karty musí být podporované jádrem. Jádro OS musí nejprve síťová zařízení (síťové karty) rozpoznat. Aby OS kartu „viděl“, musí mít pro ni zaveden funkční ovladač. Pak teprve může aplikacím poskytnout jednotné rozhraní pro přístup k prostředkům síťové karty. Síťové rozhraní lze poté nakonfigurovat.

Základem konfigurace síťového rozhraní je přiřazení logické adresy, tj. IP adresy a masky sítě.

15.2 IP adresy

Síťová komunikace je řízena sadou TCP/IP protokolů. Jsou standardem pro komunikaci v rozsáhlých počítačových sítích a jsou implementovány i v sítích lokálních. Umožňují tak propojování sítí, směrování na základě IP adresy. IP adresy definuje protokol IP:

- IPv4: adresa má 32 bitů, jsou stále běžně používané,
- IPv6: adresa má 128 bitů, jsou podporované OS, ale teprve se zavádějí.

Kromě síťového protokolu TCP/IP existují v OS další síťové protokoly, které ale většinou fungují pouze v lokálních sítích:

- NetBIOS, NetBEUI (MS Windows),
- IPX/SPX (Novell NetWare).

IP adresa IPv4

IP adresa je logická adresa zařízení v počítačové síti (na 3. vrstvě podle OSI modelu), je definována protokolem IPv4. Má velikost 4 byte = 32 bitů. Nejčastěji se zapisuje v desítkové soustavě, kdy jednotlivé byte mohou logicky nabývat hodnot od 0 – 255 a jsou odděleny tečkou. IP adresa tedy může nabývat hodnot 0.0.0.0 až 255.255.255.255 (ne všechny adresy je možno v praxi použít), což je adresní rozsah IP sítí a internetu.

Například: 192.44.118.192

IP adresy jsou logicky dvousložkové, obsahují

- adresu sítě jako celku,
- adresu uzlu v rámci dané sítě, tj. adresu konkrétního síťového rozhraní v počítači uvnitř sítě.

V rámci každé sítě se vždy přidělují IP adresy, které mají stejnou první - síťovou část - tedy tzv. síťovou adresu. Aby bylo možné poznat, která část adresy to je, přidává se k IP adrese síťová maska.

Síťová maska je speciální adresa, která obsahuje binárně v síťové části adresy pouze jedničky a v části pro jednotlivé počítače jen nuly. Určuje, která část IP adresy je adresa sítě – v této části má samé jedničky.

Zadává se prefixem, tj. IP adresa/ počet jedniček, tj. jako počet jedniček v masce za IP adresou:

10.240.5.8/26

Binárně: 11111111.11111111.11111111.11000000

Na základě síťové masky je možné spočítat IP adresu sítě a to provedením bitového součinu IP adresy a masky. Dále lze určit IP adresu broadcastovou pro všesměrové vysílání:

Adresa uzlu 10.240.5.8

00001010.11110000.00000101.00001000

Maska 255.255.255.192

11111111.11111111.11111111.11000000

Síťová adr. 10.240.5.0

00001010.11110000.00000101.00000000

Broadcast 10.240.5.63

00001010.11110000.00000101.00111111

Broadcastová adresa je také zvláštní. Je to adresa, která v části pro jednotlivé počítače má samé jedničky. Je používána pro posílání paketů určených pro všechny stanice v síti.

IP adresy, jako je síťová maska, adresa sítě, adresa broadcastová, se řadí mezi adresy speciální, které nelze použít pro adresování síťového rozhraní. Další z takovýchto adres jsou adresy 127.0.0.0 nebo 127.0.0.1. Jsou to adresy pro loopback, neboli zpětnovazebnou smyčku. Jsou určeny k testovacím účelům pro síťový SW. Zasláním dat na tuto adresu nebudou data vysílána přes síťové rozhraní do sítě.

IP adresy IPv6

IPv6 adresa má 128 bitů, obvykle se zapisuje v hexadecimální notaci, kde se jednotlivé části oddělují dvojtečkou. Je poměrně dlouhá, takže se zkracuje např.:

- odstraněním po sobě jdoucích nul zleva (nelze vynechat nuly na konci),
- vynecháním po sobě jdoucích políček se samými nulami.

Nezkrácená IP: 1088:00F9:0000:0000:0000:AB0C:7C11:0800

po zkrácení: 1088:F9::AB0C:7C11:800

Typy adres v IPv6:

- Unicast,
- Anycast,
- Multicast.

Unicast adresa reprezentuje jednotlivé síťové rozhraní. Paket zaslaný na unicast adresu je doručen konkrétnímu počítači.

Anycast adresa je jedna adresa přiřazena více zařízením – rozhraním. Datagram je pak nasměrován, z hlediska směrování, vždy na "nejbližší" stanici s danou anycastovou adresou.

Multicast adresa je skupinová adresa, kde adresáty jsou všichni členové příslušné skupiny. Speciální multicastové adresy plně nahrazují broadcasty, které se už v IPv6 nepoužívají.

15.3 Subnetting

Classless Inter-Domain Routing (CIDR) je aktuální adresní schéma a mechanismus pro přidělování adres sítě Internet. Před zavedením CIDR byly adresy rozděleny do tříd a koncovým sítím připojeným k Internetu se v závislosti na jejich velikosti přidělovala adresa sítě třídy A, B nebo C. Každá třída měla pevně stanovenou hranici síťové části.

Třída A:

- 1.x.x.x – 126.x.x.x
- první oktet je pro adresování sítí: 126 velkých sítí, tj. 28, v každé z nich až 65 534 uzlů, tj. 224 -2

Třída B:

- 128.0.x.x – 191.255.x.x
- první dva oktety pro adresování sítí: 16384 sítí středních, tj. 2¹⁴, v každé z nich až 65534 adres uzlů, tj. 2¹⁶-2

Třída C.

- 192.0.0.x – 223.255.255.x
- první tři oktety pro adresování sítí: více než dva milióny sítí malých, tj. 2^{21} , v každé z nich až 254 adres uzlů, tj. 2^8-2

CIDR přinesl do adresace dva nové principy:

- délka adresy sítě je libovolná,
- adresy se přidělují hierarchicky.

Libovolná délka síťové části adresy umožňuje adresování podsítí (subnetting). Základní myšlenkou je, že pro podsítě v rámci jedné sítě, není potřeba přidělovat několik celých adres, ale stačí jedna adresa. V adrese pak stačí posouvat hranici adresy sítě doprava, podle potřeby tak vytvářet síťové adresy pro podsítě. Masky sítě pak jednoznačně určuje, kolik bitů bude síťová adresa mít. Stírají se tak hranice mezi třídami a síťová maska je pak pro konfiguraci nezbytná.

Např. Jedna adresa třídy C s maskou danou prefixem 30 může být rozdělena na 64 podsítí: z posledního oktetu je 6 bitů přidáno k síťové části a lze je použít k vytvoření 2^6 podsítí, v každé bude $2^2 - 2$ uzlů. IP adresa se může měnit pouze v posledních dvou bitech.

V následující tabulce jsou zobrazeny všechny adresy pro síť 192.168.5.12/30, maska binárně 11111111.11111111.11111111.11111100.

IP adresa	Binárně	Typ
192.168.5.12	11000000.10101000.00000101.000011 00	network ID
192.168.5.13	11000000.10101000.00000101.000011 01	uzel
192.168.5.14	11000000.10101000.00000101.000011 10	uzel
192.168.5.15	11000000.10101000.00000101.000011 11	broadcast

Tabulka 2: Příklad subnettingu

15.4 Adresy rezervované pro privátní sítě

IP adresy, které se používají pro přístup na Internet a pro komunikaci v rámci Internetu se označují jako veřejné a musí být unikátní. Tvoří hlavní část adresního rozsahu internetu a tyto adresy jsou routovatelné v rámci celého Internetu.

Sítě bez přímé konektivity, privátní sítě, používají IP adresy privátní. Jsou unikátní v rámci LAN sítí. Pomocí techniky NAT (Network Address Translation) se při komunikaci mimo LAN překládají na adresu veřejnou. (stačí pak jedna veřejná adresa). Stejně privátní adresy se tak mohou nacházet na mnoha místech v internetu, ale nemohou spolu přímo komunikovat.

V zásadě lze říct, že privátní sítě mohou používat libovolné IP adresy. Nicméně je vhodné používat i tam, kde síť není připojena k internetu takové IP adresy, které byly k tomuto účelu vyhrazeny:

- Třída A: 10.0.0.0 – 10.255.255.255
- Třída B: 172.16.0.0 – 172.31.255.255
- Třída C: 192.168.0.0 – 192.168.255.255

15.5 Konfigurace sítě

Každé síťové rozhraní, musí mít svou:

- IP adresu,
- masku sítě,
- broadcast adresu.

Pro přístup do jiné sítě nebo na internet musí znát IP adresu zařízení, které připojení zprostředkuje. Toto zařízení se nazývá gateway (brána) a má také svou IP adresu:

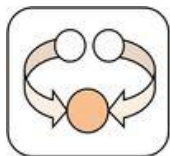
- IP adresu brány - Gateway

Každý počítač má kromě IP adresy také symbolické jméno (doménové jméno). Aby bylo možné komunikovat podle jména, musí být jméno převedeno na IP adresu (například z dev.gentoo.org udělat 64.5.62.82). Služba, která se o to stará, se nazývá name service, poskytují ji DNS servery (nameservy), proto je nutné zadat také adresu DNS serverů:

- IP adresy DNS serverů

V některých případech slouží gateway také jako nameserver. Pokud ne, zadávají se nameservy poskytované ISP.

Shrnutí kapitoly



Pro komunikaci v síti, je nutné mít v počítači síťovou kartu (NIC). Typ karty závisí na použité technologii. V lokálních sítích je nejčastější technologií ethernet. Každá ethernetová karta má od výrobce nastavenou MAC adresu. Síťové karty musí mít podporu v jádru OS, musí mít funkční ovladač. Pak OS kartu vidí a může být nakonfigurováno síťové rozhraní, protokol TCP/IP. Základem konfigurace je nastavení IP adresy, masky sítě a broadcast adresy.

Pro konfiguraci se běžně používají se IP adresy 32 bitové, definované protokolem IPv 4. Mají dvě části – adresu sítě a adresu uzlu v síti. Kolik bitů tvoří síťovou část, určuje maska sítě (jedničky=síťová adresa). Zadává se často ve tvaru IP/počet jedniček v masce nebo desítkově.

Při konfiguraci síťového rozhraní v podsítích se využívá subnetting.

Při konfiguraci sítě se nastavuje pro síťové rozhraní

- IP adresa
- Maska sítě
- Broadcast adresa
- IP adresa brány – Gateway
- IP adresy DNS serverů

Pro konfiguraci lze použít i adresy nově definované protokolem IPv6.

Kontrolní otázky a úkoly



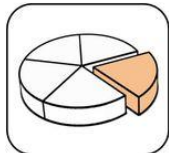
- 1) Co je NIC, jakou má funkci?
- 2) Co je základem konfigurace síťového rozhraní?
- 3) Jaké síťové protokoly se používají v lokálních sítích?
- 4) Co je to MAC adresa
- 5) Jak je definovaná IP adresa v protokolu IPv4 a IPv6?
- 6) Co je to subnetting?
- 7) Co je to maska sítě?
- 8) Jaké adresy nelze použít pro adresování uzlů?
- 9) Co je to Gateway?
- 10) Jaká je funkce DNS serveru při konfiguraci sítě?

Otázky k zamyšlení



1) Proč je nutný přechod k adresám definovaným protokolem IPv6?

Použitá literatura a jiné zdroje:



- [1] DOSTÁLEK, Libor a Alena KABELOVÁ. Velký průvodce protokoly TCP/IP a systémem DNS. 3. aktualiz. a rozš. vyd. Brno: Computer Press, 2005, 542 s. ISBN 80-722-6675-6.

16 Linux: konfigurace síťového rozhraní

Obsah hodiny



Obsahem této hodiny je popis konfigurace sítě v OS Linux.

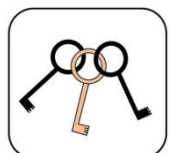
Cíl hodiny



Po prostudování budete schopni:

- popsat vytvoření vazby mezi síťovou kartou a modulem ovladače,
- popsat parametry síťového rozhraní,
- orientovat se v konfiguraci sítě.

Klíčová slova



Ovladače, moduly, modprobe, modprobe.conf, ifconfig

16.1 Detekce ovladače pro síťovou kartu

Jádro v současných Linuxových distribucích obvykle obsahuje všechny potřebné ovladače, které jsou automaticky aktivovány podle zjištěných připojených zařízení.

Ovladače pro síťovou kartu jsou obvykle realizovány jako zaveditelné moduly. Pokud je síťová karta připojena přes PCI-Express (popř. PCI) sběrnici, není potřeba modulu předávat další informace, protože si všechny dokáže zjistit sám (příkaz `lspci` vypíše seznam zařízení připojených na PCI sběrnici, podrobnější výpis: `lspci -v`). V případě ISA karet je obvykle potřeba ovladači, tj. modulu sdělit alespoň I/O adresu.

Jádro Linuxu spolupracuje s démonem *hal*, který umožňuje zavádět moduly současných zařízení zcela automaticky¹³ bez zásahu uživatele.

¹³ Např.: po zasunutí Flash paměti do USB slotu je automaticky zaveden modul pro práci s USB mass storage zařízením. Následně je detekován použitý typ systému souborů na Flash paměti (FAT, NTFS, jffs2 a podobně) a zaveden modul nebo více modulů, které z něj dokážou číst soubory a adresáře.

Potřebný modul je obvykle detekován při instalaci nebo lze použít nějaký automatický nástroj, který provede autotetekci a zapíše do konfiguračního souboru jména zařízení a k nim příslušné moduly (v distribuci Fedora je to např. program *kudzu*, spouští se při startu systému nebo ručně).

Automatické nástroje zjišťují identifikaci zařízení v tabulce */lib/modules/2.6.x-y.z¹⁴/modules.pcimap* a hledají modul pro ovladač. Seznam modulů je v adresáři */lib/modules/2.6.x-y.z/kernel/drivers/net*. Zjištěné asociace mezi zařízením a potřebným modulem zapíší do souboru */etc/modprobe.conf*.

U starších zařízení, kde nelze automaticky vše pro připojení zjistit, je nutné vytvořit vazbu mezi zařízením a modulem ručně. Tyto vazby (aliasy) se zapisují do souboru */etc/modprobe.conf* (v jádrech 2.4.x a starších v souboru */etc/modules.conf*).

/etc/modprobe.conf:

```
alias eth0 3c59x
```

```
alias eth1 ne2k-pci
```

Při práci se zařízením (např. síťová karta na ISA sběrnici), je pak modul na základě tohoto souboru zaveden buď automaticky nebo může být před použitím zařízení zaveden do jádra ručně příkazem *modprobe* včetně parametrů.

```
modprobe ne io=0x300
```

16.2 Konfigurace sítě

Když OS síťovou kartu rozpozná, aktivuje příslušný ovladač, je možno přistoupit ke konfiguraci síťového rozhraní, sítě.

Pro základní konfiguraci v Linuxové síti stačí nastavit pro každé síťové rozhraní:

- individuální IP adresu,
- masku sítě,
- pro přístup do jiné sítě se nastavuje IP adresa brány,
- IP adresa DNS serveru (nameserver) pro překlad IP adres na doménové jméno.

Konfigurace se provádí řádkovým příkazem v příkazovém interpretu nebo textovými či grafickými utilitami, které mají k dispozici jednotlivé distribuce. Univerzálním a základním nástrojem pro konfiguraci je příkaz *ifconfig*.

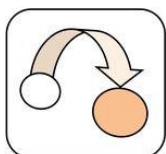
¹⁴ 2.6.x-y.z je číslo verze právě používaného jádra, lze zjistit příkazem `uname -r`

Veškerá konfigurace sítě je uložena v konfiguračním souboru a provádí se při spuštění systému prostřednictvím rc-skriptů.

Automatická detekce nastavení sítě

Pokud v síti existuje funkční DHCP server, konfigurace síťových rozhraní se provede automaticky. Nastaví se síťová rozhraní lo (loopback) a eth0. DHCP (Dynamic Host Configuration Protocol) totiž umožňuje automatické nastavení všech se sítí souvisejících údajů.

Příkazem `/sbin/ifconfig -a` lze vypsat informace o nastavení všech síťových rozhraní, např. o eth0:



```
# /sbin/ifconfig eth0
eth0
Link encap:Ethernet HWaddr 00:50:BA:8F:61:7A
inet addr:192.168.0.2 Bcast:192.168.0.255
Mask:255.255.255.0
inet6 addr: fe80::50:ba8f:617a/10 Scope:Link
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:1498792 errors:0 dropped:0 overruns:0 frame
:0
TX packets:1284980 errors:0 dropped:0 overruns:0 carri
er:0collisions:1984 txqueuelen:100
RX bytes:485691215 (463.1Mb) TX bytes:123951388 (118.2Mb
)
Interrupt:11 Base address:0xe800
```

Ruční konfigurace sítě

Pokud síť nefunguje, je nutno přistoupit k ruční konfiguraci. Nastavení sítě sestává ze tří kroků:

- Přiřazení IP adresy pro síťové rozhraní, síťové masky a broadcastu pomocí *ifconfig*.

```
ifconfig eth0 IP_ADDD broadcast BROADCAST netmask NETMASK up
ifconfig eth0 up nahození rozhraní
ifconfig eth0 down shození rozhraní
```

- Nastavení routování (směrování) na bránu pomocí *route*.

```
route add default gw GATEWAY
```

- Zápis IP adresy nameserverů do souboru (např. do /etc/resolv.conf).

```
nameserver NAMESERVER1
```

```
nameserver NAMESERVER2
```

16.3 Nastavení sítě pomocí nástroje ip

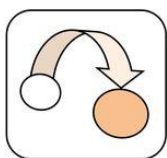
Nástroj *ip* bývá součástí moderních distribucí, pokud není, stačí nainstalovat balíček *iproute2*.

Prvním parametrem příkazu *ip* je vždy „modul“, se kterým pracuje síťové rozhraní, IP adresa, směrovací tabulka, ARP tabulka apod.:

```
ip link          # operace se síťovými rozhraními
ip addr          # operace s IP adresami
ip route         # operace se směrovací tabulkou
ip neigh         # operace s ARP tabulkou
ip rule          # operace se směrovacími pravidly
```

Každý z těchto modulů má svou specifickou syntaxi, k dispozici je nápověda: *ip help* nebo *ip modul help* a samozřejmě *man ip*

Přiřazení IP adresy pro síťové rozhraní a síťové masky ve formátu CIDR¹⁵, broadcastu:



```
ip addr add IP_ADDR brd NETMASK dev eth0
ip link set dev eth0 up           # nahození rozhraní
ip link set dev eth0 down        # shození rozhraní
```

Nastavení routování (směrování) na bránu:

```
ip route add default via GATEWAY
```

¹⁵ CIDR je zkratka z Classless InterDomain Routing. Původně byly IPv4 adresy rozděleny do tříd A, B, C a D, tento systém však nepočítal s masivním rozvojem Internetu a záhy mu začalo hrozit vyčerpání nových unikátních adres. Adresovací schéma CIDR umožňuje jedné IP adrese označit celý rozsah. CIDR IP adresa vypadá jako běžná IP adresa, avšak končí lomítkem a číslem – počet jedniček v masce sítě, například 192.168.0.0/16. CIDR je popsáno v RFC 1519.

16.4 Konfigurační soubory (Gentoo)

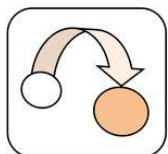
/etc/conf.d/hostname.....jméno počítače, hostname:

```
hostname="tux"
```

/etc/conf.d/net.....jméno domény

```
dns_domain_lo="domacisit"
```

/etc/conf.d/net.....konfigurace sítě



```
# This blank configuration will automatically use DHCP
for any net.*
```

```
# scripts in /etc/init.d. To create a more complete
configuration,
```

```
# please review /etc/conf.d/net.example and save your
configuration
```

```
# in /etc/conf.d/net (this file :]!).
```

```
# Pro DHCP
```

```
config_eth0=( "dhcp" )
```

```
# Pro statickou IP adresu zapsanou ve formátu CIDR
```

```
config_eth0=( "192.168.0.7/24" )
```

```
routes_eth0=( "default via 192.168.0.1" )
```

```
# Pro statickou IP adresu zapsanou pomocí masky sítě
```

```
config_eth0=( "192.168.0.7 netmask 255.255.255.0" )
```

```
routes_eth0=( "default gw 192.168.0.1" )
```

/etc/hostspro převod (resolving) jmen strojů na IP adresy,
používá se jako doplněk služby DNS.

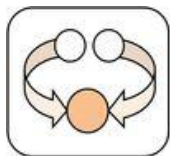
```
127.0.0.1      tux.domacisit tux localhost
```

Lze přidat informace o dalších počítačích, pouze
pevné IP adresy

```
192.168.0.5    jan.domacisit jan
```

```
192.168.0.6    iva.domacisit i
```

Shrnutí kapitoly



Jádro v současných Linuxových distribucích obvykle obsahuje všechny potřebné ovladače, které jsou automaticky aktivovány podle zjištěných připojených zařízení. Ovladače pro síťovou kartu jsou obvykle realizovány jako zaveditelné moduly. Potřebný modul je detekován při instalaci, pomocí nástroje, který provede autodetekci nebo ručně. Do konfiguračního souboru `/etc/modprobe.conf` se zapisuje jméno zařízení a k němu příslušný modul.

Po aktivaci ovladače se provádí konfigurace síťového rozhraní, sítě. Pro základní konfiguraci v Linuxové síti stačí nastavit pro každé síťové rozhraní:

- individuální IP adresu
- masku sítě
- pro přístup do jiné sítě se nastavuje IP adresa brány
- IP adresa DNS serveru (nameserver) pro překlad IP adres na doménové jméno.

Konfigurace se provádí automaticky (pokud je funkční DHCP server) nebo ručně: řádkovým příkazem v příkazovém interpretu nebo textovými či grafickými utilitami, které mají k dispozici jednotlivé distribuce.

Univerzálním a základním nástrojem pro konfiguraci je příkaz `ifconfig` a v současných distribucích lze použít nástroj `ip`.

Kontrolní otázky a úkoly



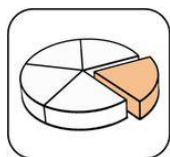
- 1) Jak se detekuje ovladač síťové karty a asociuje zaveditelný modul?
- 2) Jaká je základní konfigurace síťového rozhraní?
- 3) Jakým způsobem se provádí konfigurace síťového rozhraní?

Otázky k zamyšlení



- 1) Vyhledejte a porovnejte postup konfigurace síťového rozhraní v distribuci Gentoo a Debian.

Použitá literatura a jiné zdroje:



- [1] KERSLAGER, Milan. Síťová rozhraní: Síťové služby v Linuxu. Www.pslib.cz [online]. 28. 9. 2007, 4. 6. 2009 [cit. 2012-02-26]. Dostupné z: http://www.pslib.cz/ke/S%C3%AD%C5%A5ov%C3%A1_rozhran%C3%AD#cite_note-0
- [2] VERMEULEN, Sven, Roy MARPLES, Daniel ROBBINS, Chris HOUSER a Jerry ALEXANDRATOS. Gentoo Linux alpha Handbook: Konfigurace sítě v Gentoo. Rorbuilder.info [online]. [2006], 21. říjen 2007 [cit. 2012-02-26]. Dostupné z: <http://rorbuilder.info/doc/cs/handbook/handbook-alpha.xml?part=4&chap=1>
- [3] DOČEKAL, Michal. Správa Linuxového serveru: Nastavení sítě pomocí nástroje ip. LinuxEXPRES [online]. Brno: QCM, 31. leden 2012 [cit. 2012-02-26]. Dostupné z: <http://www.linuxexpres.cz/praxe/sprava-linuxoveho-serveru-nastaveni-site-pomoci-nastroje-ip>
- [4] SHAH, Steve. Administrace systému Linux: jak porozumět svému počítači : podrobný průvodce začínajícího administrátora. 2. vyd. Praha: Grada, 2003, 533 s. ISBN 80-247-0641-5.

17 MS Windows: konfigurace síťového rozhraní

Obsah hodiny



Obsahem této hodiny je popis konfigurace sítě v OS Windows.

Cíl hodiny



Po prostudování budete schopni:

- orientovat se v možnostech nastavení síťového rozhraní,
- popsat nastavení síťového rozhraní ve Windows.

Klíčová slova



Centrum síťových připojení, Příkaz ifconfig, Příkaz netsh

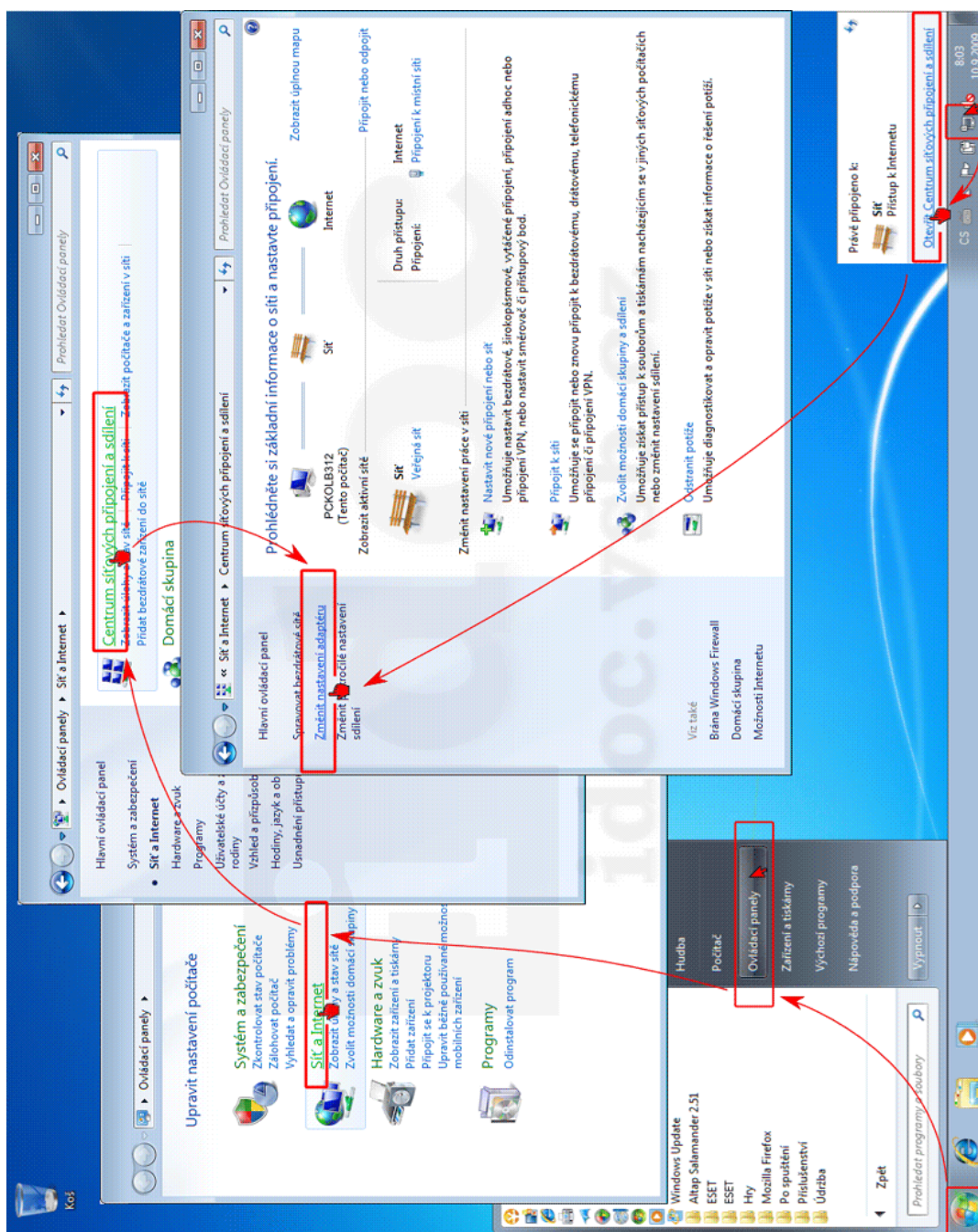
17.1 Konfigurace síťové karty v MS Windows

Pro konfiguraci síťové karty v prostředí MS Windows rovněž platí, že je třeba nejprve nainstalovat ovladač síťové karty. Ovladač může být součástí databáze ovladačů Windows, která obsahuje velkým množstvím ovladačů síťového HW různých výrobců. Pokud ovladač není nalezen v databázi, lze jej do systému doinstalovat. Ovladač je software dodávaný výrobcem karty. Instaluje se podle pokynů výrobce. Samotná HW konfigurace síťové karty se provádí pomocí správce zařízení.

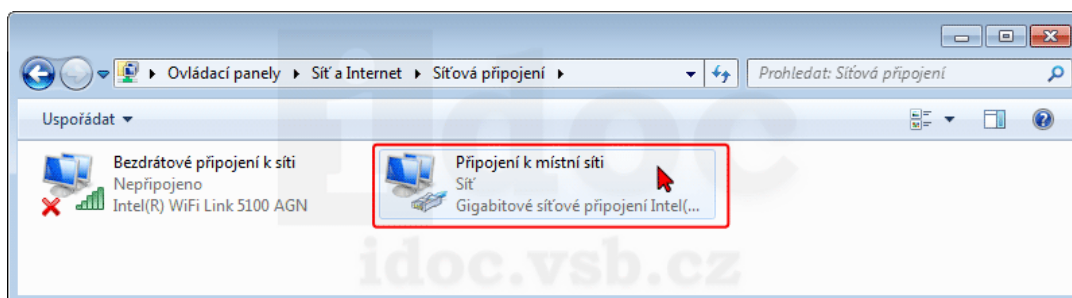
Podobně jako v Linuxu, máme dvě možnosti: nastavit automatickou konfiguraci síťového rozhraní protokolem DHCP nebo ručně (staticky). Jako výchozí bývá nastavena možnost automatické konfigurace.

17.2 Nastavení síťového rozhraní

Nejprve je třeba vyhledat základní informace o síti s možností nastavení připojení v Centru síťových připojení: Tlačítko Start – Ovládací panely – Síť a Internet – Centrum síťových připojení a Sdílení.

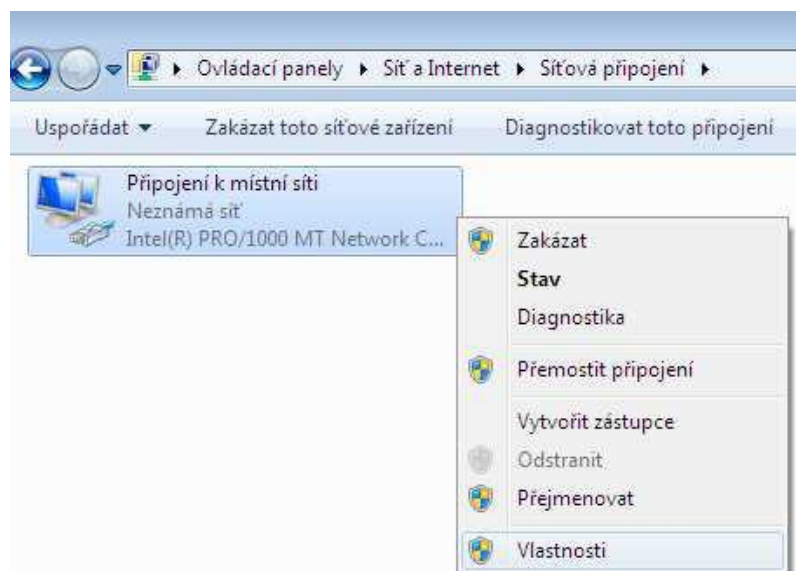


Obrázek 17-1: Centrum síťových připojení

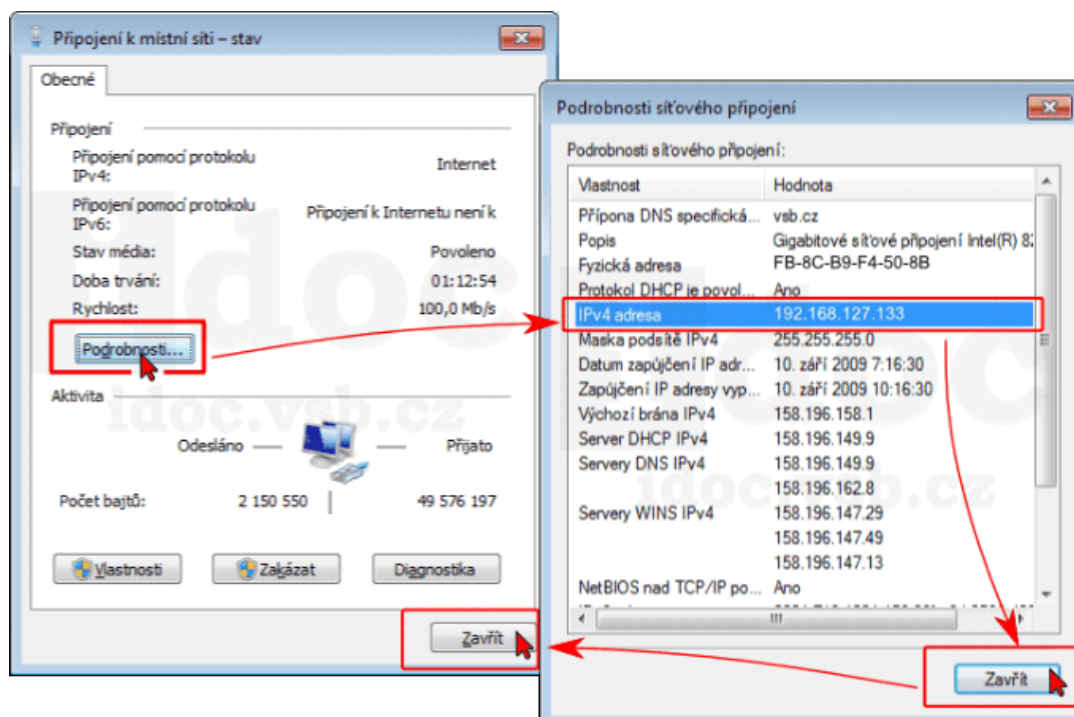


Obrázek 17-2: Windows 7: Nastavení síťového rozhraní

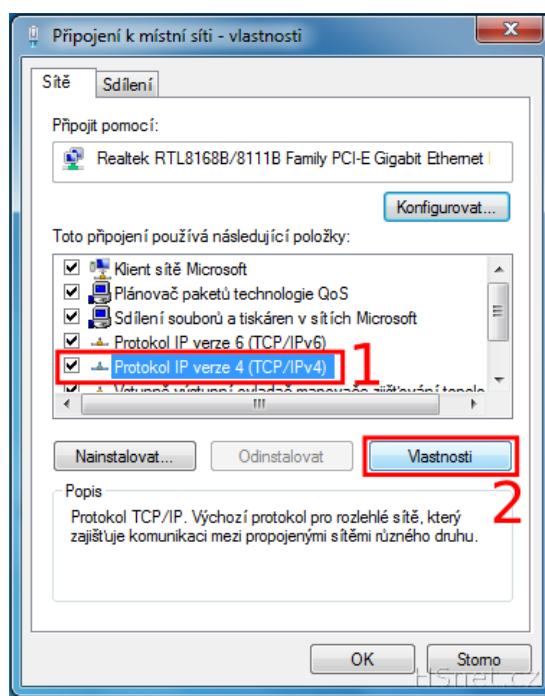
V Centru síťových připojení je odkaz Změnit nastavení adaptéru. Po kliknutí se otevře seznam dostupných síťových rozhraní v počítači (síťová připojení) a je možno vybrat síťové rozhraní pro konfiguraci. Seznam síťových připojení lze jednoduše vyvolat spuštěním příkazu *ncpa.cpl*. Dalším krokem je nastavení vlastností vybraného síťového připojení: kontextové menu Vlastnosti.



Obrázek 17-3: Podrobnosti o konfiguraci síťového rozhraní

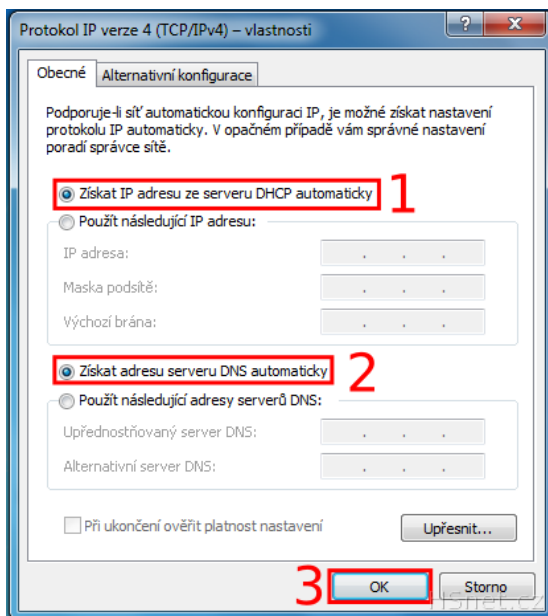


Obrázek 17-4: Podrobnosti síťového připojení



Obrázek 17-5: Windows 7: Protokol IP - vlastnosti

Další nastavení je shodné se staršími OS Windows. Na kartě jsou k dispozici protokoly, které umožňují síťovou komunikaci včetně protokolu TCP/IP (1). Jejich konfigurace je schovaná ve Vlastnostech (2). Po rozkliknutí se objeví následující okno:



Obrázek 17-6: Konfigurace síťových protokolů

Jsou zde dvě možnosti konfigurace:

- automaticky přes DHCP server (1),
- ručně (2).

Pokud se zde vybere možnost získat IP adresu ze serveru DHCP(1), je IP adresa, maska podsítě i výchozí brána nastavena DHCP serverem automaticky. Pro připojení na Internet je nutné zadat pouze adresy DNS serverů, ale i ty lze získat automaticky.

17.3 Síťové rozhraní a příkazová řádka

Kromě grafického rozhraní se pro konfiguraci síťového prostředí využívají i nástroje, které má k dispozici příkazový interpret. Základním příkazem pro diagnostiku a konfiguraci je v MS Windows příkaz *ipconfig*. Příkaz *ipconfig* neumožňuje statickou konfiguraci protokolu TCP/IP, ale s jeho pomocí je možno zobrazovat aktuální konfiguraci síťových připojení, obnovovat (popř. uvolňovat) nastavení přidělené serverem DHCP a vyprazdňovat DNS cache.

Pro komplexní nastavení síťových připojení pomocí příkazové řádky slouží příkaz *netsh*. Samotným spuštěním příkazu *netsh* se spustí příkazový interpret Network Shell disponující sadou příkazů umožňující velice detailní nastavení celého síťového prostředí Windows (síťové rozhraní, firewall, NAT, routování, ...).

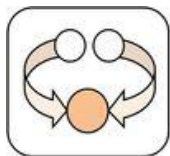
Příklad statické konfigurace síťového připojení TCP/IP pomocí *netsh*:

```
netsh interface ip set address name="LAN" static
192.168.0.100 255.255.255.0 192.168.0.1 1
```

zobrazení aktuální konfigurace:

```
netsh interface ip show config
```


Shrnutí kapitoly



Pro konfiguraci síťové karty v prostředí MS Windows rovněž platí, že je třeba nejprve nainstalovat ovladač síťové karty.

Samotná HW konfigurace síťové karty se provádí pomocí správce zařízení.

- Automatická konfiguraci síťového rozhraní protokolem DHCP
- Ruční - statické nastavení.

Je třeba najít seznam dostupných síťových rozhraní v počítači (síťová připojení) přes *Centrum síťových připojení a Sdílení/Změnit nastavení adaptéru*. Po kliknutí se otevře a je možno vybrat síťové rozhraní pro konfiguraci.

Seznam síťových připojení lze jednoduše vyvolat spuštěním příkazu *ncpa.cpl*.

Dalším krokem je nastavení vlastností vybraného síťového připojení: v kontextovém menu *Vlastnosti*.

Na kartě jsou k dispozici protokoly, které umožňují síťovou komunikaci včetně protokolu TCP/IP. Jejich konfigurace je ve *Vlastnostech*.

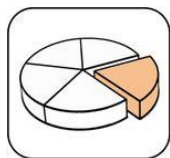
Kromě grafického rozhraní se pro konfiguraci síťového prostředí využívají i nástroje, které má k dispozici příkazový interpret. Základním příkazem pro diagnostiku a konfiguraci je v MS Windows příkaz *ipconfig*

Pro komplexní nastavení síťových připojení pomocí příkazové řádky slouží příkaz *netsh*.

Kontrolní otázky a úkoly



- 1) Jakým způsobem se provádí konfigurace síťového rozhraní?
- 2) Co je třeba v rámci konfigurace nastavit protokolu TCP/IP?
- 3) Jakým způsobem lze zobrazit seznam dostupných síťových rozhraní?
- 4) Jaké nástroje pro konfiguraci síťových připojení se používají v příkazovém interpretu?
- 5) Jakými způsoby lze zjistit konfiguraci síťového rozhraní?

Použitá literatura a jiné zdroje:

- [1] Nastavení připojení v Microsoft Windows 7 a Microsoft Windows Vista.
In: HSNET [online]. [2010] [cit. 2012-06-16]. Dostupné z:
<http://hsnet.cz/nastaveni-pripojeni-v-ms-windows-vista-a-ms-windows-7/>
- [2] Nastavení připojení v Microsoft Windows 7 a Microsoft Windows Vista.
In: InNET Vysoká škola báňská - Technická univerzita Ostrava [online].
© 2012 [cit. 2012-06-16]. Dostupné z:
http://idoc.vsb.cz/cs/okruhy/cit/pc/sitova_pripojeni/t_cp_ip/

18 Autentizace a autorizace uživatele

Obsah hodiny



Obsahem této hodiny autentizace a autorizace uživatele, se zaměřením na různé metody autentizace.

Cíl hodiny



Po prostudování budete schopni:

- popsat princip autentizace a autorizace uživatele,
- definovat bezpečné heslo a pravidla pro jeho vytvoření,
- orientovat se v různých metodách autentizace,
- popsat princip autorizace uživatele.

Klíčová slova



Autentizace, Autorizace, Bezpečné heslo, Biometrie

18.1 Autentizace na základě hesla

Autentizace uživatele je proces identifikace uživatele při vstupu do systému na základě zadaného jedinečného identifikačního údaje. Slouží k jednoznačnému určení uživatele. Takovým údajem je nejčastěji heslo, které uživatel zadává při přihlášení do systému po zadání uživatelského jména. Uživatelské jméno je údaj veřejný, ale heslo je privátní údaj, který zná pouze uživatel.

Heslo je obecný prostředek k autentizaci uživatele. Slouží pro ochranu přístupu k nejrůznějším systémům a informacím, do kterých by se neměl dostat nikdo nepovolaný. Pokud uživatel prokáže znalost hesla, je pokládán za oprávněného.

Heslo je použitelné pouze tehdy, není-li ostatním uživatelům známé, proto uživatel musí držet heslo v tajnosti. Musí si heslo pamatovat. Heslo by nemělo být nikde zapsané.

Heslo je v zašifrované podobě uloženo v databázi systému. Po jeho zadání v procesu přihlašování se provede kontrola – ověření správnosti hesla proti údaji v databázi.

V databázi spolu s heslem jsou uloženy ještě další údaje s dalšími parametry hesla, např. délka, doba platnosti hesla. K heslu v systému nemá přístup ani administrátor, pokud uživatel své heslo zapomene, administrátor mu nastaví nové. Povinností uživatele je si heslo změnit.

Jak je to ale s heslem administrátora? Heslo je obecně informace velmi citlivá, zejména, jedná-li se o heslo administrátora. Co když je administrátor z nějakého důvodu nedostupný, nikdo další nemá jeho oprávnění a při tom obzvláště jeho heslo nikdo nesmí znát? Na tuto situaci by se mělo pamatovat při definování pravidel bezpečnostní politiky firmy. Přístupové heslo administrátora se chrání jako velmi citlivé informace ve firmě. Může být např. uloženo v zapečetěné obálce a uzamčeno v trezoru.

18.2 Bezpečné heslo

Hesla představují základ ochrany proti neoprávněnému přístupu k organizaci.

Slabá hesla usnadňují útočníkům snadný přístup k počítačům i sítí, zatímco odhalení silných hesel je poměrně složité i pomocí softwaru odhalujícího hesla. Nástroje k odhalení hesel jsou neustále zlepšovány a výkon počítačů používaných k tomuto účelu se stále zvyšuje. Software odhalující hesla používá jednu ze tří následujících metod:

- inteligentní odhadování,
- slovníkové útoky,
- násilné automatizované útoky, které zkouší všechny možné kombinace znaků.

Automatizovanou metodou lze odhalit jakékoli heslo, pokud je k dispozici dostatek času. Odhalení silného hesla je však mnohem složitější než v případě slabého hesla. Zabezpečený počítač má nastavená silná hesla pro všechny uživatelské účty.

Slabé heslo:

- není v podstatě žádné heslo,
- obsahuje vaše uživatelské jméno, skutečné jméno či název firmy,
- obsahuje slovo, které je možné nalézt ve slovníku.

Například: Heslo je slabé heslo.

Délka hesla Použité znaky		4	5	6	7	8
		Kombinací 100 hesel/sec	Kombinací 100 hesel/sec	Kombinací 100 hesel/sec	Kombinací 100 hesel/sec	Kombinací 100 hesel/sec
0-9	10 znaků	10 000 2 minuty	100 000 16 minut	1 000 000 3 hodiny	10 000 000 1 den	100 000 000 11 dní
a-z; 0-9	36 znaků	731 161 616 5 hodin	380 204 032 7 dní	2×10^9 8 měsíců	8×10^{10} 25 let	3×10^{12} 900 let
a-z; A-Z; 0-9	62 znaků	147 763 336 2 dny	916 132 832 3 měsíce	5×10^{10} 18 let	4×10^{12} 1000 let	2×10^{14} 70 000 let
a-z; A-Z; 0-9; ščáěě...;@#\$%^*?!...	85 znaků	522 006 25 6 dní	443 705 312 1 rok	3×10^{11} 120 let	3×10^{13} 10 000 let	3×10^{15} 800 000 let

Obrázek 18-1: Hesla o různé délce a čas pro jejich prolomení

Bezpečné heslo je takové, které není snadno zjistitelné, uhodnutelné nebo jinak snadno zneužitelné. Pro vytvoření bezpečného hesla platí řada pravidel.

Heslo by nemělo vzniknout z nějakého údaje o nás či našem okolí, například:

- vlastní jméno či jméno někoho z rodiny, jméno psa, milenky apod.
- rodné číslo či datum narození
- č. domu, adresa, telefonní číslo...
- heslo, 1234...
- známé hlášky, obměny jednoduchých slov, data narození

Heslo mělo používat nejen běžné znaky, ale rovněž číslice, speciální znaky. Čím je větší množinu znaků použitých v hesle, tím je složitější heslo prolomit.

K dispozici je 10 číslic, 26 základních písmen abecedy (a-z), ty lze zdvojnásobit použitím velkých a malých písmen, dále můžeme přidat znaky s diakritikou a nakonec i interpunkční znaménka (. , ; - ? ! ...) a spoustu speciálních znaků (@ # & \$ ^ _ * ...). Dohromady tedy máme k dispozici přes 80 znaků relativně snadno použitelných na běžné klávesnici.

U speciálních znaků je třeba opatrnosti, servery nepodporují z bezpečnostních důvodů použití určitých speciálních znaků (např. \$, &, \, /, ', <, >, ", , , ~)

Nejbezpečnější hesla jsou „nesmyslné“ kombinace znaků. Tady je ale poměrně nepříjemné, že takové heslo je dost obtížně zapamatovatelné a pokud ho pravidelně nepoužíváme, brzy ho zapomeneme. Napsat si heslo někde na papírek není také dobrý nápad. Proto je dobré si vymyslet k heslu nějakou mnemotechnickou pomůcku. I ta ale musí zůstat stejně tajná jako heslo samotné.

Podtrženo, sečteno, silné heslo:

- obsahuje nejméně sedm znaků,
- neobsahuje vaše uživatelské jméno, skutečné jméno či název firmy,
- neobsahuje slovo, které je možné nalézt ve slovníku,
- výrazně se liší od předchozích hesel. Hesla lišící se pouze v čísle, například *Heslo1*, *Heslo2*, *Heslo3* atd., nejsou silná.
- Obsahuje znaky: velká písmena, malá písmena číslice a symboly nacházející se na klávesnici

18.3 Jiné způsoby autentizace

Autentizace uživatele může být uskutečněna i na základě jiných identifikačních údajů než je heslo, k autentizaci mohou být použity speciální aplikace (například bezpečnostní či adresářové servery), hardwarová zařízení (čipové karty).

PIN

Mezi nejběžněji používanou patří autentizace na základě PINu. PIN (osobní identifikační číslo) je posloupnost číslic. Používá se například při výběru peněz z bankomatu. PIN je obvykle čtyřciferný.

Chytré karty

Je to karta, která má na čipu nebo magnetickém proužku uloženy informace. Jedná se o autentizační zařízení, na kterém jsou uloženy národně uživatele, opravňující jej k přístupu.

Podobají se platebním kartám a mají v sobě uloženy veřejné/soukromé klíče a hesla. Technika uložení dat může být jednoduchá jako na magnetickém pásku, nebo složitá jako integrovaný obvod vpracovaný do karty, který funguje jako miniaturní počítač.

Ve vysoce zabezpečeném prostředí samotné karty neumožní přístup automaticky. Uživatel musí kartu vložit do čtečky, a než mu bude povolen přístup, musí ještě zadat další údaje.

18.4 Pokročilé způsoby identifikace a ověřování

Biometrie

Jedná se o vyšší úroveň zabezpečení, a to identifikaci pomocí:

- otisku prstu,
- podle oční sítnice,
- podle obličeje,
- podle mapy žil na dlani ruky,
- podle DNA,

- dynamiky stisku kláves,
- charakteristiky hlasu,
- charakteristiky písma.

Statistická pravděpodobnost, že dva lidé budou mít stejné biometrické údaje (otisky prstů, obraz sítnice oka, DNA, vzorek hlasu ...) je tak malá, že je tato technika poskytuje nespornou identifikaci uživatelů.

Všechny systémy fungují na principu porovnání se vzorkem uloženým v databázi. Někdy se kombinuje více metod najednou.

Systém rozlišení otisku prstu se často používá ve spojení se zabezpečením pomocí chytrých karet. Uživatelé jsou sejmuty vzorky otisku prstů a uloženy do databáze.

V okamžiku, kdy uživatel chce použít počítač, musí přiložit prst (nebo celou ruku) na plochu čtecího zařízení. Takto sejmutý obraz je porovnán s otiskem uloženým v databázi a výsledkem je buď povolení, nebo zamítnutí přístupu.

Obraz sítnice nebo duhovky se snímá pomocí světelného paprsku o malém výkonu. Paprsek přečte vzorek ze sítnice nebo duhovky oka, provede se počítačová analýza vzorku a opět porovnání v databázi. O těchto vzorcích se říká, že jsou ještě unikátnější, než otisky prstů nebo DNA.

Ověření hlasového vzorku pracuje na principu unikátních vzorků lidského hlasu. Uživatel musí do databáze nejprve nahrát heslo nebo frázi, podle které bude dále identifikován. Pro přihlášení do systému musí uživatel do patřičného zařízení říci heslo nebo frázi, která je porovnána se vzorkem v databázi. Zohledněny jsou faktory jako výška hlasu, rychlost a intenzita. Technika hlasového vzorku není považována za tak přesnou, obvykle používá v situacích, kdy musí být ověření provedeno pomocí telefonní linky.

Známou firmou v oblasti výroby a kvality biometrických technologií je společnost SUPREMA INC, výhradním distributorem jejich produktů u nás je Biometrie s.r.o. Zabývá se prodejem, instalací a servisem biometrických přístupových a docházkových terminálů, které jsou certifikované NBÚ na stupeň utajení 2-4. (<http://www.biometrie.cz/>).

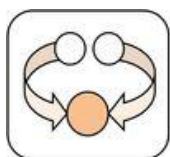
18.5 Autorizace uživatele

Po identifikaci uživatele a jeho vstupu do systému je další činnost uživatele v OS řízena na základě autorizovaného přístupu k souborům adresářům.

Autorizací se rozumí proces ověření přístupových oprávnění uživatele vstupující do informačního systému. Tento proces ve většině případů navazuje na proces autentizace.

Podstatou autorizace je ověřit, zda daný uživatel má oprávnění provést příslušnou akci, například vložení nového záznamu do seznamu dodavatelů apod.

Shrnutí kapitoly



Autentizace uživatele je proces identifikace uživatele při vstupu do systému na základě zadaného jedinečného identifikačního údaje. Identifikačním údajem může být heslo, PIN, biometrické údaje.

Autentizace je založena porovnání zadaného nebo nasnímaného údaje se vzorkem uloženým v databázi.

V OS probíhá autentizace na základě hesla. Heslo je privátní velmi citlivá informace, kterou uživatel musí chránit. Pro vytvoření hesla platí řada pravidel, jejich dodržení může zabránit prolomení hesla.

Autorizací je proces ověření přístupových oprávnění uživatele vstupující do informačního systému. Navazuje na proces autentizace. Podstatou je ověření oprávnění provést příslušnou akci.

Kontrolní otázky a úkoly



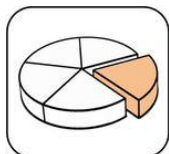
- 1) Popište princip autentizace pomocí hesla?
- 2) Jaké pravidla je třeba dodržovat při vytváření hesla?
- 3) Jaké jsou další metody autentizace uživatele?
- 4) Na jakém principu fungují všechny metody autentifikace?
- 5) Co je autorizace uživatele?

Otázky k zamyšlení



- 1) Kde se můžeme setkat s použitím biometrických metod autentifikace?

Použitá literatura a jiné zdroje:



- [1] SROUBEK, Jirka. Bezpečné heslo: Kvalita hesla. In: Wikipedia: the free encyclopedia [online]. San Francisco (CA): Wikimedia Foundation, 2001-02-06 [cit. 2012-02-04]. Dostupné z: http://cs.wikipedia.org/wiki/Bezpečné_heslo
- [2] BITTO, Ondřej. Šifrování a biometrika aneb tajemné bity a dotyky. Vyd. 1. Kralice na Hané: Computer Media, 2005, 168 s. ISBN 80-866-8648-5.
- [3] Silná hesla. Technet.microsoft.com [online]. © 2012 [cit. 2012-04-06]. Dostupné z: [http://technet.microsoft.com/cs-cz/library/cc756109\(v=ws.10\).aspx](http://technet.microsoft.com/cs-cz/library/cc756109(v=ws.10).aspx)

19 Linux: proces přihlašování, organizace a správa účtů,

Obsah hodiny



Obsahem této hodiny je průběh procesu přihlašování uživatele a organizace a správa účtů v OS Linux.

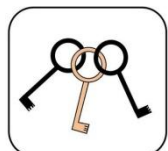
Cíl hodiny



Po prostudování budete schopni:

- popsat proces přihlášení uživatele,
- popsat organizaci účtů,
- popsat práci s heslem,
- orientovat se v konfiguračních souborech pro správu účtu,
- vytvořit a modifikovat účet uživatele,
- orientovat se v logovacích souborech pro monitorování přihlašování

Klíčová slova



Login, Účet uživatele, Heslo, Logování

19.1 Přihlášení uživatele

O přihlášení, čili autentizaci a autorizaci uživatele se stará program *login*. Kontroluje, zda bylo zadáno správné uživatelské jméno a přístupové heslo a provádí počáteční nastavení uživatelského prostředí nastavením oprávnění a spuštěním interpretu příkazů.

Příkaz *login* vyzve uživatele k zadání *login name* – přihlašovacího jména uživatele a *password* – hesla uživatele. Poté následuje ověření uživatele (autentizace uživatele) přes soubor */etc/passwd*.

Nastaví se UID, GID, proměnné HOME, PATH, SHELL, TERM, MAIL, LOGNAME, domovský adresář, a uživateli se obvykle spustí *shell*. Při přihlášení se zobrazí uživateli zprávy správce systému ze souboru */etc/motd* ("messages of the day").

Další soubory, které se načítají při přihlášení uživatele, mu umožňují nastavit pracovní prostředí:

- */etc/profile*, globální nastavení pro všechny uživatele
- *~/bash_rc*, nastavení vlastností příkazového interpretu při každém jeho spuštění
- *~/bash_profile*, nastavení „soukromého“ profilu uživatele
- */etc/issue*

Obsah posledního souboru se vypíše ještě před vlastním přihlášením, obvykle obsahuje základní informace o systému, např. verzi jádra, název pc.

Program *login* zapisuje všechny neúspěšné pokusy o přihlášení do systémového "log" souboru (pomocí programu *syslog*). Zaznamenává úspěšné i neúspěšné pokusy o přihlášení superuživatele. Oba druhy záznamů jsou užitečné při pátrání po případných "vetřelcích".

Přihlášení uživatelé jsou zapsáni v souboru */var/run/utmp*. Tento soubor je platný jenom do dalšího znovuzavedení nebo zastavení systému, protože v průběhu zavádění systému se jeho obsah vymaže. Příkazy *who*, *w* a další podobné se dívají právě do souboru */var/run/utmp* a zjišťují, kdo je k systému připojený.

Všetchna úspěšná přihlášení jsou zaznamenána do souboru */var/log/wtmp*. Tento soubor se může bez omezení zvětšovat, proto je potřeba jej pravidelně mazat (například po týdnu).

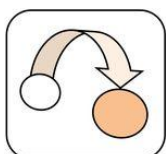
Soubor *wtmp* lze procházet příkazem *last*.

Oba soubory *utmp* i *wtmp* mají binární formát (viz manuálová stránka *utmp*), takže je nelze prohlížet bez speciálních programů.

19.2 Uživatelský účet

Každý uživatel v Linuxu má svůj účet, který zahrnuje přihlašovací jméno, heslo a domácí adresář a v širším smyslu všechny soubory, které uživatel vlastní. Účet jednoznačně definuje uživatele a jeho pracovní prostředí, včetně všech souborů, které danému uživateli náleží.

Uživatelské i systémové účty jsou definovány v jednoduché databázi v podobě textového souboru */etc/passwd*, kde je na každém řádku uveden jeden účet. Jeho prostřednictvím se provádí správa účtů. Jsou v něm uloženy všechny informace nutné pro autentizaci uživatele.



```
$ cat /etc/passwd

root:x:0:1:Super-User:/root:/sbin/sh
daemon:x:1:1::/:
```

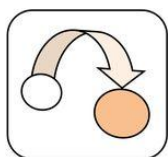
```
bin:x:2:2::/usr/bin:
sys:x:3:3::/:
listen:x:37:4:Network Admin:/usr/net/nls:
nobody:x:60001:60001:Nobody:/:
noaccess:x:60002:60002:No Access User:/:
nobody4:x:65534:65534:SunOS 4.x Nobody:/:
honza:x:1001:10:Honza:/home/honza:/bin/ksh
```

Soubor `/etc/passwd` obsahuje záznamy o sedmi položkách. Jednotlivé položky jsou od sebe odděleny dvojtečkou:

Login name:password:UID:GID:komentář:/home/adresář:/implicitní/shell

- Uživatelské jméno (*login name*) skupina 3-8 znaků.
- Heslo (*password*). Pokud je zapnutý systém stínových hesel, je uloženo v zakódované podobě v souboru `/etc/shadow`.
- Uživatelské číslo UID (*user identification*).
- Primární (základní) skupina uživatele GID (*primary group identification*). Každý uživatel je členem alespoň jedné skupiny uživatelů členství v dalších skupinách je uloženo v souboru `/etc/group`.
- Doplňující uživatelské údaje jméno, příjmení, telefon ...
- Domovský adresář (*home directory*).
- Příkazový interpret (nebo program), který se spustí po přihlášení. Většinou je zde `/bin/bash`, tj. *shell* - interpret příkazů.

Do souboru může zapisovat pouze uživatel `root`, až na dvě výjimky. Uživatel si může v tomto souboru vyplnit pole vyhrazené pro informace o uživateli příkazem `chfn`:



```
lenka@home ~ $ chfn
```

Changing the user information for lenka

Enter the new value, or press ENTER for the default

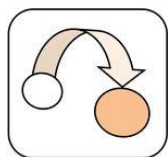
Full Name:

Room Number []:

Work Phone []:

Home Phone []:

Nebo si může vybrat jiný shell (ze seznamu v `/etc/shells`) a to pomocí příkazu `chsh`:



```
lenka@home ~ $ chsh
```

Changing the login shell for lenka

Enter the new value, or press ENTER for the default

```
Login Shell [/bin/bash]:
```

19.3 Vytvoření a modifikace účtu

Pro vytvoření a modifikaci účtu jsou v Linuxu k dispozici řádkové příkazy nebo utility v textovém či grafickém rozhraní. Nejefektivnější je použití řádkových příkazů, zejména když vytváříme nebo měníme více účtů najednou. Výhodou příkazové řádky je možnost zjednodušit si tuto činnost skriptem.

Příkazy pro práci s účty, provádí zápis do `/etc/passwd` a `/etc/group`:

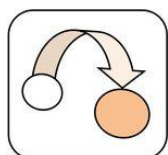
- `useradd` vytvoření účtu
- `usermod` modifikace účtu
- `userdel` zrušení účtu: odstraní uživatele, včetně domovského adresáře a mailové schránky,

useradd

Vytvoří uživatele včetně jeho domovského adresáře `/home/<uživatel>` (zkopíruje sem obsah adresáře `/etc/skel`), mailové schránky `/var/spool/mail/<uživatel>` a přiřadí uživateli primární skupinu téhož názvu. Při vytváření nového účtu se vychází z údajů uvedených v `/etc/default/useradd` a `/etc/login.defs`.

Příkazy pro práci se skupinami, provádí zápis do `/etc/group`

- `groupadd` vytvoření skupiny
- `groupmod` změna skupiny
- `groupdel` zrušení skupiny
- `groups` vypíše skupiny, do nichž je uživatel zařazen



Další příkazy:

id

Vypíše UID a GID uživatele včetně všech jeho skupin

```
lenka@home~ $ id
```

```
uid=1002(lenka)
```

```
gid=1004(lenka) groups=1004(lenka),1001(homenet)
```

mkpasswd

Vytvoří náhodné heslo: o min. délce 9 znaků, pro vygenerování hesla použije minimálně: dvě velká písmena, dvě malá písmena, dvě číslice, jeden speciální znak. Uvedené implicitní nastavení lze změnit pomocí voleb.

```
lenka@home~ $ mkpasswd
```

```
Password:
```

```
JKF7ALyXMcFoo
```

change <uživatel>

Změní nastavení platnosti účtu a hesla uživatele. Ne zadají-li se v příkazu žádné volby, pracuje interaktivně; výchozí hodnoty platnosti hesel uživatelů jsou uvedeny v */etc/login.defs*

19.4 Heslo v Linuxu

Hesla nastavuje root při vytváření uživatelského účtu. Root může pomocí příkazu *passwd* s parametrem jméno uživatele nastavit pro heslo uživatele další vlastnosti. Provádí se zápis do */etc/shadow*. Výchozí hodnoty jsou uvedeny v */etc/login.defs*:

- -d nastaví účet bez hesla,
- -n <DD> určí min. platnost hesla v řádu dní,
- -x <DD> určí max. platnost hesla v řádu dní,
- -w <DD> určí počet dní k varování uživatele před koncem platnosti hesla,
- -l uzamkne účet,
- -u odemkne účet,
- -S <uživatel> vypíše informace o nastavení hesla uživatele (stav hesla: „PS“ = heslo přiřazeno, „NP“ = žádné heslo, „LK“ = účet uzamčen, datum poslední změny hesla, min. a max. platnost hesla v řádu dní, varovací období před vypršením hesla a doba mezi koncem platnosti hesla a uzamčením účtu v řádu dní);

Uživatel si po tomto prvotním nastavení heslo mění příkazem *passwd*. Tento příkaz pracuje interaktivně. Uživatel je vyzván k zadání stávajícího hesla. Nejprve proběhne autentizace uživatele a teprve pak může uživatel heslo změnit.

V Linuxu se při zadávání hesla neobjevují žádné znaky. Při zadávání hesla program kontroluje, zda pro heslo nebyl použit výraz ze slovníku, zda heslo není příliš jednoduché nebo shodné či podobné s login name.

Heslo je uschováno v souboru */etc/shadow* (kvůli ochraně proti útoku hrubou silou na použitou jednosměrnou šifru). Soubor je přístupný pouze uživateli root.

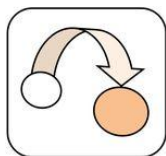
Soubor `/etc/shadow` obsahuje hesla v zašifrované podobě (MD5) a údaje o platnosti a expiraci hesla (viz. příkaz `passwd`)

```
username:pwd_hash: .. expiration data ..
```

Uživatel může zjistit údaje o svém hesle příkazem `passwd` s volbou `-S`

```
lenka@home ~ $ passwd -S
```

```
lenka P 06/17/2009 0 99999 7 -1
```

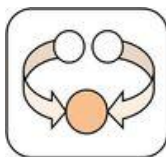


19.5 Logování přihlašování uživatele

Informace o přihlašování uživatelů se zapisují do logovacího souboru v adresáři `/var/log`:

- `last`
- `/var/log/lastlog` - vypíše časové údaje o přihlášení všech / daného uživatele do systému za poslední období (od vytvoření souboru `/var/log/wtmp`)
- `lastlog`
- `/var/log/lastlog` - vypíše seznam všech uživatelů v systému a čas jejich posledního přihlášení včetně jména terminálu
- `lastb`
- `/var/log/btmp` - vypíše časové údaje nezdařených pokusů o přihlášení všech / daného uživatele do systému za poslední období (od vytvoření souboru `/var/log/btmp`)
- `faillog`
- `/var/log/faillog` - vypíše pozitivní záznamy o neúspěšném přihlášení všech uživatelů

Shrnutí kapitoly



Autentizace uživatele se po přihlášení uživatele provádí prostřednictvím souboru `/etc/passwd` a `/etc/shadow`. Při přihlášení se spouští skripty, které nastaví pracovní prostředí uživatele.

Soubor `/etc/passwd` obsahuje informace o uživatelských účtech, `/etc/shadow` obsahuje zašifrovaná hesla a omezení platná pro hesla. Pro vytvoření a modifikaci účtu jsou v Linuxu k dispozici řádkové příkazy nebo utility v textovém či grafickém rozhraní.

Účty a hesla nastavuje root při vytváření uživatelského účtu. Root může pomocí příkazu `passwd` s parametrem jméno uživatele nastavit pro heslo uživatele další vlastnosti.

Monitorování přihlašování uživatele se provádí prostřednictvím logovacích souborů v adresáři `/var/log`.

Kontrolní otázky a úkoly



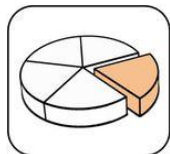
- 1) Jak probíhá přihlášení uživatele a jeho autorizace v systému?
- 2) Popište soubor /etc/passé.
- 3) K jakému účelu se používá soubor /etc/shadow?
- 4) Jak se nastavuje a mění heslo?
- 5) Co je to základní neboli primární skupina uživatele?
- 6) Kde jsou informace o skupinách?
- 7) Lze monitorovat přihlašování uživatelů a jak?
- 8) Kdo může zapisovat do /etc/passwd?

Otázky k zamyšlení



- 1) Proč soubor /etc/shadow není pro běžné uživatele přístupný?

Použitá literatura a jiné zdroje:



- [1] DOOKIE. Účty a práva. Linuxvbashi.cz [online]. 2011-01-13, 2011-01-13 [cit. 2012-02-04]. Dostupné z: <http://linuxvbashi.cz/ucty-a-prava>
- [2] KOLEKTIV AUTORŮ. Linux: Dokumentační projekt. Brno: Computer Press, a.s., 2008. ISBN 978-80-251-1525-1. Dostupné z: <http://www.root.cz/knihy/linux-dokumentacni-projekt-4-vydani/>
- [3] SHAH, Steve. Administrace systému Linux: jak porozumět svému počítači : podrobný průvodce začínajícího administrátora. 2. vyd. Praha: Grada, 2003, 533 s. ISBN 80-247-0641-5.

20 Linux: přístupová práva

Obsah hodiny



Obsahem této hodiny je vysvětlení problematiky přístupových práv v Linuxu.

Cíl hodiny



Po prostudování budete schopni:

- popsat přístupová práva: typy, kategorie uživatelů,
- orientovat se v možnostech nastavení práv,
- charakterizovat práva speciální možnosti jejich využití,
- vysvětlit význam a použití ACC.

Klíčová slova



Mod, Kategorie uživatelů, Speciální práva, Sticky Bit, SGID Bit, SUID Bit, Příkaz chmod, Příkaz umask, ACL, Maska

20.1 Základní přístupová práva

V Linuxu existuje právě jeden superuživatel zvaný *root*. Některé činnosti může provádět pouze tento uživatel. Normální uživatel v Linuxu má jen nezbytné minimum práv. K běžné práci není žádoucí ani potřebné mít *root* práva. *Root* uživatel se správně využívá jen k administraci systému a to převážně jen prostřednictvím dočasného zvyšování práv (příkaz *sudo*).

Uživatelé v Linuxu jsou organizováni do skupin. Skupině se přidělují práva, která se přenášejí na všechny členy skupiny. Uživatel může být členem několika skupin, ale pouze jedna skupina je základní, je uvedena v */etc/passwd*. Všechny skupiny jsou popsány v souboru */etc/group*.

Každý soubor, program v Linuxu má svého vlastníka – uživatele a skupinu. Vlastníkem je většinou ten uživatel, který soubor vytvořil (*root* může vlastnictví přidělit jinému uživateli) a zároveň skupina uživatele – vlastníka (většinou je to základní skupina, lze změnit). Práva se pak definují pro vlastníka: uživatele, členy skupiny a zbytek světa.

Každý uživatel je identifikovaný svým UID a je členem minimálně základní skupiny. Skupina je identifikována GID. Ke každému souboru tedy existují dvě čísla, která charakterizují uživatele. Každý soubor, adresář vytvořený uživatelem je vlastněn uživatelem - UID a má přidělenou skupinu (základní) – GID.

Přístupová práva v Unixových systémech a tedy i v Linuxu jsou uložena v inode, v prvních 12-ti bitech (*mod*). Dělí se na práva speciální (první tři bity v modu) a základní (9 bitů v modu).

Speciální práva jsou tři: *Sticky Bit*, *SUID Bit*, *SGID Bit*.

Základní práva jsou rozdělena do tří typů: *čtení*, *zápis* a *spouštění souboru* nebo *průchod adresářem*. Jsou vždy definována pro tři kategorie uživatelů: *vlastníci* (*u*, *user*), *skupiny* (*g*, *group*) a *ostatní* (*o*, *other*).

Práva speciální	Binárně	Oktalově	Symbol	Práva základní	Binárně	Oktalově	Symbol
Sticky Bit	001	1	t	execute	001	1	x
SGID Bit	010	2	s	write	010	2	w
SUID Bit	100	4	s	read	100	4	r

Tabulka 3: Přístupová práva

Rozlišuje se, zda jde o soubor nebo adresář. Pro soubor se operace definují následovně:

Pro soubory:

- r soubor je povoleno číst
- w do souboru je povoleno zapisovat
- x soubor (binární nebo skript) je povoleno spustit

Pozor na právo *x* – *exekute*! Spustitelnost souboru v Linuxu není dána příponou, ale právě tímto přístupovým právem.

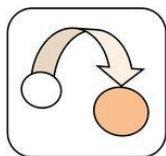
Pro adresáře:

- r adresář je povoleno vypsát
- w do adresáře je povoleno zapisovat, vytvářet a rušit soubory
- x do adresáře je možno vstoupit (pomocí *cd*)

Přístupová práva se dále specifikují pro tři různé kategorie uživatelů:

- u vlastník (user) co s objektem může vlastník provádět
- g skupina (group) co s objektem mohou provádět uživatelé skupiny
- o ostatní (others) co s objektem mohou provádět ostatní

Změna přístupových práv se provádí příkazem `chmod`. Budťo symbolicky, tj. pomocí symbolů (kategorie operace práva) nebo absolutně jako součet oktalových hodnot zapnutých práv pro jednotlivé kategorie. Práva může měnit jen vlastník souboru nebo uživatel *root*.



Symbolicky: `chmod u=rwx,g=rx,o=r soubor`

Absolutně: `chmod 751 soubor`

751 znamená $7=4(r)+2(w)+1(x)$ $5=4(w)+1(x)$ $1=1(x)$

20.2 Speciální přístupová práva: t-bit a s-bit

S-Bit

Procesy v Linuxu běží pod UID, toho, kdo má přístup ke zdrojům (souborům, zařízením atd.). Při spuštění procesu se generuje reálné UID a GID, které je shodné s UID a GID uživatele, který proces spustil.

Efektivní UID, GID určuje přístup k souborům - jaké operace smí vykonat proces. Většinou je (efektivní) EUID a EGID stejné jako (reálné) RUID a RGID.

SUID (Set User ID) je speciální právo, které se nastavuje pro spustitelné soubory. Pokud soubor má nastavený SUID Bit (S-Bit) a je spuštěn, nastaví se EUID na vlastníka souboru nikoli na uživatele, který ho spustil.

Program spuštěný uživatelem má stejná práva, jako uživatel sám. To znamená, že může modifikovat jen ty soubory, k nimž má uživatel právo zápisu. V případě, že má soubor nastavený S-Bit, získá uživatel, který ho spustil, práva vlastníka. To představuje bezpečnostní riziko.

S-Bit se nastaví takto:

```
chmod 4755 program nebo chmod u+s program
```

Existuje několik případů, kdy je nutné, aby uživatelem spuštěný program běžel pod jiným účtem (zpravidla s vyššími právy). Typickým příkladem je příkaz `passwd` pro změnu hesla uživatele. Ten musí modifikovat soubor `/etc/shadow`, kde jsou uloženy hashe hesel. Tento soubor není, z pochopitelných důvodů, zapisovatelný pro běžné uživatele. Program `passwd` má nastaven S-Bit a vlastní jej uživatel *root*. Program po svém spuštění má práva uživatele *root*, přestože jej spustil jiný uživatel.

```
ls -l /bin/passwd
```

```
-rws--x--x 1 root root 32108 čec 11 14:30 /bin/passwd
```

Programu je přiřazen SUID-Bit *root* a uživatel ho může spouštět ze svého neprivilegovaného účtu. Program po svém spuštění má práva uživatele *root*, přestože jej spustil jiný uživatel a tak může modifikovat všechny soubory jako *root*.

Existuje také podobný SGID-Bit, který mění skupinu. Není tolik používán u souborů, ale u adresářů, kdy po aplikaci tohoto příznaku patří všechny nově vytvořené soubory do určené skupiny a ne do uživatelské základní. Nastaví se příkazem `chmod g+s` a výpis vypadá následovně:

```
drwxr-sr-x  3 root users      4096 zář  1 23:14 foo
```

t-bit (sticky bit)

Soubor, který je uložený v adresáři, do něhož mají všichni povolen zápis, může také kdokoliv smazat. Někdy je vhodné, aby jej mohl mazat pouze vlastník souboru a nikdo jiný.

Sticky (lepkavý) bit se nastavuje příkazem `chmod +t` nebo `chmod 1777` a ve výpisu příkazu `ls` je vidět takto:

```
drwxrwxrwt  39 root  root      3704 zář  6 21:15 tmp
```

Tím způsobem je možno nastavit danému adresáři sticky bit. V takto ošetřeném adresáři bude moci soubory mazat jenom jejich vlastník.

20.3 Umask

Příkaz `umask` nastavuje implicitní (default) práva, která má soubor a adresář při vytvoření. V Linuxu se totiž práva nedědí, nastaví se pomocí masky.

Příkaz `umask` je obdobou příkazu `chmod`, ale pracuje s opačnými bity a je pro všeobecné - globální nastavení práv.

Aby se nové soubory ukládaly s právy 750, musí se použít `umask` takto: od čísla 7 se odečte každé číslo u: 0 ($7 - 7 = 0$), g: 2 ($7 - 5 = 2$) a 7, o: 0 ($7 - 0 = 0$).

```
umask 027 xxx
```

Nový adresář `xxx` pak bude vytvořený s přístupovými právy nastavenými na 750.

20.4 ACC: access list, rozšířená práva

ACL (access control list, seznam pro řízení přístupu) je obecně seznam oprávnění připojený k nějakému objektu (např. souboru). Seznam určuje, kdo nebo co má povolení přistupovat k objektu a jaké operace s ním může provádět. Oprávnění nastavená ACL se dědí.

ACL jsou součástí jádra a mají podporu ve většině Linuxových souborových systémů. Pro souborový systém `ext3`, `ext4` se musí ACL aktivovat při připojování, v souboru `/etc/fstab` použitím volby `-o acl`.

Pro práci s ACL se používají příkazy (utilit) *getfacl* a *setfacl*. Každý záznam, tj. řádek seznamu má tři položky, oddělené dvojtečkou:

typ:uid/gid:práva nebo *user:jméno uživatele:práva*

Typem může být *user*, *group*, *other* nebo *mask*. User specifikuje práva pro uživatele, *group* pro skupinu, *other* pro ostatní uživatele. Pomocí *mask* lze specifikovat masku práv. Maska práv se příliš nepoužívá, utilita *setfacl* ji automaticky při nastavování práv dopočítává jako sjednocení jednotlivých práv.

Místo *uid/gid* je možno použít jméno uživatele. U některých záznamů se tento údaj nevyplňuje (položka se nevynechá, ale zůstane prázdná). Neuvádí se u typů *other*, *mask* a u nastavení práv *user* a *group* pro vlastnickou skupinu či uživatele.

ACL záznamy se přidávají příkazem *setfacl* s parametrem *-m*., zobrazují se příkazem *getfacl soubor*. Záznamy mají tvar:

user: jméno uživatele:práva

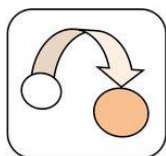
Záznamy bez uživatele nebo skupiny se zadávají:

mask::"práva".

Práva se uvádějí ve tvaru *rw*x, jako u základních práv.

Minimální ACL

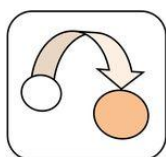
Obsahují záznamy *user* - *u*, *group* - *g*, *other* – *o*, což jsou klasická základní práva:



```
[root@centos]# getfacl soubor
# file: soubor
# owner: ondra
# group: uživatele
user::rw-
group::r--
other::---
```

Rozšířené ACL

Přidávají další záznamy s právy pro další uživatele nebo skupiny, v tomto příkladu přidáme *rw* pro uživatele *karel*:



```
[root@centos]# setfacl -m user:karel:rw soubor
[root@centos]# getfacl soubor
# file: soubor
# owner: ondra
```

```
# group: uživatelé
user::rw-
user:karel:rw-
group::r--
mask::rw-
other::---
```

Maska

Maska je filtr práv. Maska určuje maximální možná práva, která může dostat uživatel nebo skupina definovaná v ACL. Nevztahuje se na vlastníka. Změnou masky souboru lze najednou všem uživatelům a skupinám definovaným v ACL zakázat všechny přístupy.

Ve výpisu je vidět, že přibyl záznam pro uživatele karel a záznam pro masku. Že jsou použita rozšířená práva, lze zjistit výpisem `ls -l`. Ve výpisu je za právy uveden znak '+':

```
[root@centos]# ls -l
-rw-rw----+ 1 ondra uživatelé    0 Nov 19 16:08 soubor
```

Záznam z ACL lze zrušit pomocí volby `-x`:

```
setfacl -x user:karel soubor
```

Shrnutí kapitoly



Model přístupových práv v Unixových systémech je velmi jednoduchý. Každý soubor má svého vlastníka a skupinu, do které patří. Oprávnění mohou být různá pro vlastníka, skupinu a ostatní uživatele. Přístupová práva jsou tři, právo číst (r, jako read), právo zapisovat (w, jako write) a právo vykonat kód, tedy spouštět (x, jako eXecute).

Kromě výše uvedených práv existují ještě tři práva speciální: sticky bit, setuid bit a setgid bit.

Pokud se pro adresář nastaví sticky bit, bude moci soubory mazat jenom jejich vlastník.

Nastavením setuid bitu pro spustitelný soubor bude možno soubor spustit s vyšším oprávněním, jako by ho spustil uživatel, který ho vlastní. SGID bit na souborech ovlivňuje vlastnictví skupiny u nových souborů a adresářů.

Práva se v Linuxu nedědí, ale nastavují se na základě masky příkazem *umask*.

ACL (access control list, seznam pro řízení přístupu) je seznam oprávnění připojený k souboru, adresáři. Určuje, kdo (uživatel, skupina) má povolení přistupovat k objektu a jaké operace s ním může provádět. ACC rozšiřují klasická práva vlastníka a skupiny o práva dalších uživatelů, skupin, o masku práv.

Pro práci s ACL se používá *getfacl* a *setfacl*.

Kontrolní otázky a úkoly



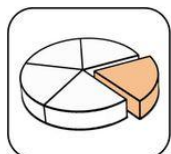
- 1) Charakterizujte model přístupových práv v Linuxu
- 2) Jak nastavujeme přístupová práva
- 3) Co umožňují práva speciální?
- 4) Co je to ACL a jak se liší od základních práv?
- 5) Jaké záznamy jsou v ACL?

Otázky k zamyšlení



- 1) Jaké jsou rozdíly v nastavování práv v jednotlivých OS?
- 2) Lze aplikovat práva z Linuxu ve Windows a opačně?

Použitá literatura a jiné zdroje:



- [1] Přístupová práva. [online]. [cit. 2012-01-29]. Dostupné z:
<http://www.abclinuxu.cz/ucebnice/zaklady/principy-prace-se-systemem/pristupova-prava>
- [2] CRHONEK, Tomáš. ACL prakticky: Bezpečnost. Abclinuxu.cz [online]. 11.12.2008 [cit. 2012-02-04]. Dostupné z:
<http://www.abclinuxu.cz/clanky/bezpecnost/acl-prakticky#maska>
- [3] PALÁT, Pavel. ACL v Linuxu. Linuxzone.cz [online]. 16. 09. 2003 [cit. 2012-02-04]. Dostupné z:
<http://www.linuxzone.cz/index.phtml?idc=839&ids=29>
- [4] VYCHODIL, Vilém. Operační systém Linux: příručka českého uživatele. 1. vyd. Brno: Computer Press, 2003, 260 s. ISBN 80-722-6333-1.
- [5] SHAH, Steve. Administrace systému Linux: jak porozumět svému počítači : podrobný průvodce začínajícího administrátora. 2. vyd. Praha: Grada, 2003, 533 s. ISBN 80-247-0641-5.

21 OS Windows: Organizace a správa účtů

Obsah hodiny



Obsahem této hodiny popis organizace a správy účtů v OS Windows.

Cíl hodiny



Po prostudování budete schopni:

- popsat pracovní skupinu a doménu,
- charakterizovat místní uživatelské účty,
- charakterizovat doménové uživatelské účty,
- orientovat se ve výchozích účtech.

Klíčová slova



Pracovní skupina, Doména, Místní a doménový účet (konto)

21.1 Pracovní skupiny a domácí skupiny, domény

Pracovní skupina

Obvykle ve skupině nebývá více než dvacet počítačů. Všechny počítače jsou rovnocenné, žádný z počítačů nemá kontrolu nad jiným počítačem. Všechny počítače musí být ve stejné místní síti nebo podsíti.

Každý počítač má sadu uživatelských účtů. Pro přihlášení do počítače pracovní skupiny, je nutné v něm mít uživatelský účet. Pracovní skupina není chráněna heslem.

Uživatelské účty umožňují více osobám sdílet jeden počítač. Každá osoba může mít samostatný účet s vlastními nastaveními a předvolbami, například s vlastním pozadím plochy nebo spořičem obrazovky. Uživatelské účty kontrolují, ke kterým souborům a programům mají uživatelé přístup, a jaké typy změn v počítači mohou provádět.

Doména

Jeden či více počítačů jsou servery. V doméně mohou být tisíce počítačů. Počítače mohou být v různých místních sítích. Prostřednictvím

serverů správci sítě řídí zabezpečení a oprávnění všech počítačů v doméně. Usnadňuje to provádění změn, protože změny jsou automaticky provedeny ve všech počítačích. Uživatelé domény musí zadat heslo nebo jiné pověření při každém přístupu do domény.

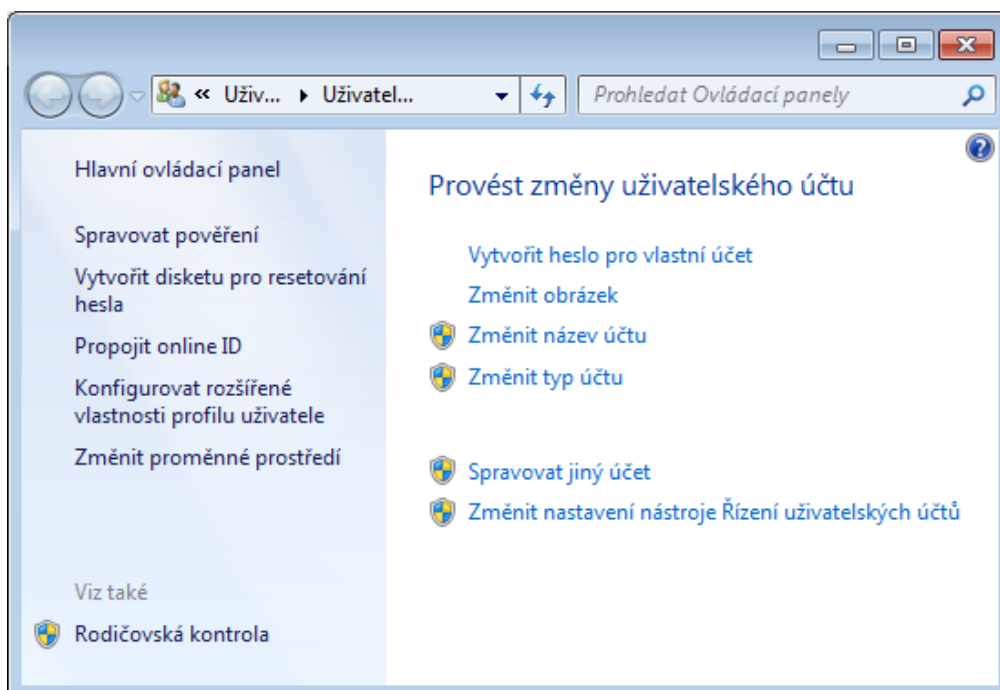
Uživatelský účet v doméně, umožňuje se přihlásit ke kterémukoli počítači v doméně.

21.2 Místní a doménové uživatelské účty

Pro komunikaci v rámci pracovních skupin ve Windows musí mít každý uživatel ve všech počítačích, na nichž pracuje, vytvořen uživatelský účet. Přístup těchto účtů je omezen na lokální prostředky. Jedná se o takzvané místní uživatelské účty. Každý počítač má svou vlastní databázi účtů (kont).

Fyzicky jsou účty uloženy v Security Accounts Manager (SAM) databázi. Přidat nebo zrušit lokálního uživatele lze přes Ovládací panely (pouze základní činnosti), pomocí konzoly Správa počítače, Lokal Users and Groups.

Princip místních uživatelských účtů je vhodný pro malé sítě typu peer-to-peer, kde není problém spravovat několik málo počítačů a uživatelů a není problém s konfigurací pro každého z nich. Jinak je to při správě větších sítí, kdy se spravuje velké množství účtů.



Obrázek 21-1: Přístup k účtům přes ovládací panely.

Ve větších počítačových sítích typu klient server se používají doménové účty (konta) uživatelů a skupin (někdy také označované jako globální účty a globální skupiny).

Doménové uživatelské účty jsou vytvořené v databázi Active Directory. Místo přihlášení na počítač přes místní uživatelský účet, se provádí přihlašování přes doménový účet do domény. V doméně existuje jeden centrální server (takzvaný řadič domény), na kterém je uložena databáze uživatelů a skupin domén. Výhody:

- centralizovaná správa,
- centralizovaná autentizace uživatele, jedním přihlášením (Single Sign On) lze získat přístup ke všem zpřístupněným síťovým zdrojům v síti (v doménách). Oprávnění uživatelé se mohou přihlásit k počítačům v i bez toho, aby na nich měli vytvořené místní uživatelské účty.

V případě domén jsou sice vyšší pořizovací náklady, ale je snazší a efektivnější správa a zabezpečení. Správa účtů se provádí přes konzolu Active Directory Users And Computers.

V databázi uživatelů a skupin u obou typů účtů existují účty

- výchozí a
- účty vytvořené správcem - standardní uživatelské účty.

Všechny uživatelské účty jsou identifikované plně kvalifikovaným přihlašovacím jménem. Ve Windows 7 jsou tyto jména složena ze dvou částí:

- uživatelské jméno – jméno uživatele účtu,
- jméno počítače nebo jméno domény – počítač nebo doména, v které uživatelský účet existuje.

Např. Pro uživatele Lenka, účet byl vytvořený na počítači PC1, je plně kvalifikované přihlašovací jméno PC1\Lenka

Z lokálního účtu nelze přistupovat ke sdíleným zdrojům v doméně, ale z doménového účtu je možné specifikovat přístup k lokálním zdrojům. Plně kvalifikované doménové jméno může být definováno dvěma způsoby:

- UPN (User Principal Name) ve tvaru Uživatelské jméno@úplné jméno domény (Lenka@domena1.cz),
- Pre-Windows 2000 logon name ve tvaru jméno domény\Uživatelské (domena1\Lenka).

Klíčovým identifikátorem uživatelského účtu je bezpečnostní identifikátor SID. SID (Security Identifier) je alfanumerický řetězec generovaný při vytváření objektu účtu. Je sestavený z předpony tvořené ID počítače nebo

domény a z jedinečného ID uživatele. Windows 7 používá tyto identifikátory při rozpoznávání uživatelských účtů.

21.3 Uživatelské účty a účty počítačů v doméně

Nejen uživatel, ale také každý počítač musí mít v Active Directory (AD) doméně svůj účet počítače. Jedná se o rozšíření základního typu user (user class) na typ computer (computer class). Rozšíření přidává jen několik atributů jako je například operatingSystem, operatingSystemVersion a operatingSystemServicePack.

Uživatelské účty a účty počítačů ve službě Active Directory reprezentují fyzické entity (například počítač nebo osobu). Uživatelské účty se v případě některých aplikací mohou používat také jako vyhrazené účty služeb.

Uživatelské účty a účty počítačů (a skupiny) jsou někdy označovány jako zaregistrované objekty zabezpečení. Zaregistrované objekty zabezpečení jsou objekty adresáře, kterým je automaticky přiřazeno ID zabezpečení (SID) a které lze použít pro přístup k prostředkům domény. Uživatelský účet nebo účet počítače je možné použít k těmto akcím:

- ověřování identity uživatele nebo počítače,
- povolení nebo odepření přístupu k prostředkům domény,
- správa ostatních zaregistrovaných objektů zabezpečení.

21.4 Výchozí uživatelské účty

Výchozí uživatelské účty jsou vytvářeny automaticky při instalaci systému. Jedná se o

- účet Správce, člen skupiny Administrators,
- účet Guest, člen skupiny Guest,
- účet HelpAssistant.

Účet Správce, čili administrátorský účet dovoluje provádět změny, které ovlivní také ostatní uživatele. Administrátorský účet patří mezi určitá privilegia, ve výchozím nastavení je zakázán, je třeba ho povolit. Pokud je povolen, získá účet Správce plnou kontrolu nad počítačem a může uživatelům podle potřeby přiřazovat uživatelská práva a oprávnění řízení přístupu. Tento účet lze použít pouze pro úkoly vyžadující pověření pro správu (např. konfigurace systémových nastavení, instalace softwaru, přistupovat ke všem datům, ...). U tohoto účtu je nutné nastavit silné heslo.

Účet Správce je členem skupiny Administrators, z této skupiny jej nelze odstranit ani odebrat, ale může být přejmenován nebo zakázán. Dokonce i v případě, kdy byl účet Správce zakázán, je možné ho stále v nouzovém

režimu používat k přístupu k počítači. Na místním počítači mají členové skupiny Administrators oprávnění Úplné řízení.

Z důvodu zabezpečení se nedoporučuje připojovat se k počítači s pověřením správce. I když je uživatel přihlášen k počítači bez oprávnění správce, má možnost použít příkaz *Spustit jako správce* a provést tak úlohy, které požadují vyšší úroveň oprávnění, než je standardní uživatelský účet.

Účet Guest slouží uživatelům, kteří v počítači nemají skutečný účet. Pozor! Účet Guest nevyžaduje heslo a tím se stává bezpečnostním rizikem. Ve výchozím nastavení je účet Guest zakázán, lze jej však povolit, nedoporučuje se. U účtu Guest lze nastavit stejná práva a oprávnění jako u jiných uživatelských účtů.

Ve výchozím nastavení je účet Guest členem skupiny Guest, která umožňuje uživateli přihlásit se k počítači. Další práva a oprávnění musí skupině Guests udělit člen skupiny Administrators.

Standardní uživatelský účet umožňuje uživateli používat většinu funkcí počítače, mimo pro provádění změn ovlivňujících ostatní uživatele nebo zabezpečení počítače (k těmto operacím se vyžaduje oprávnění od správce).

Uživatel, který má zřízen standardní účet, může užívat většinu programů nainstalovaných v počítači, ale nemůže instalovat nebo odinstalovat software ani hardware, odstraňovat soubory nutné k provozu počítače nebo měnit nastavení počítače ovlivňující ostatní uživatele. Při používání standardního účtu mohou některé programy před provedením určitých úloh vyžadovat zadání hesla správce.

21.5 Vytvoření místního uživatelského účtu

Správa počítače/Systémové nástroje/Místní uživatelé a skupiny/Uživatelé

K této operaci je potřeba mít pověření pro účet Správce na místním počítači nebo být na místním počítači členem skupiny Správce (Administrators).

Uživatelské jméno se nesmí shodovat s žádným jiným uživatelským jménem nebo názvem skupiny, které počítač spravuje. Jméno uživatele může obsahovat nanejvýš 20 velkých či malých písmen a dalších znaků, kromě následujících:

" / \ [] : ; | = , + * ? < > @

Uživatelské jméno se nemůže skládat pouze z teček (.) nebo mezer.

V polích *Heslo* a *Potvrzení hesla* lze zadat heslo o maximální délce 127 znaků. Pokud jsou ovšem v síti i počítače se systémy Windows 95 a Windows 98, nemělo by být heslo delší než 14 znaků, jinak nebude pravděpodobně možné přihlásit se na síť z počítačů se systémy Windows 95 a Windows 98.

Novému uživateli je vhodné přiřadit přihlašovací skript a domovský adresář.

Přiřazení přihlašovacího skriptu a domovského adresáře

Správa počítače\Systémové nástroje\Místní uživatelé a skupiny\Uživatelé

Po výběru uživatele ve *Vlastnostech* se na kartě *Profil* zadá do pole *Přihlašovací skript* název souboru a relativní cesta ke skriptu.

Místní přihlašovací skripty musí být uloženy do sdílené složky (či do podsložek sdílené složky) s názvem *Netlogon*. Jestliže složka ve výchozím nastavení neexistuje, je nutné ji vytvořit. Pokud je přihlašovací skript uložený v podsložce složky *Netlogon*, je nutné před názvem souboru zadat relativní cestu k dané složce:

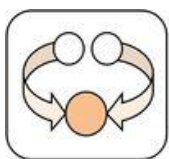
Přihlašovací skript Startup.bat je uložený v adresáři \\PC1\Netlogon\skripty, do pole Přihlašovací skript se zadá skripty\Startup.bat.

Pro nastavení místní domovské složky, se na kartě *Profil* zadá cesta k domovskému adresáři do pole *Místní cesta* (např.: *c:\uživatelé\marie.*)

Jestliže je domovská složka ve sdíleném prostředku, je třeba kliknout na možnost *Připojit*, dále na příslušné písmeno jednotky a poté zadat síťovou cestu (např.: *\\airedale\uživatelé\pavelr.*). Je nutné nejprve vytvořit sdílený prostředek a nastavit oprávnění, která uživateli povolí přístup.

Pokud není přiřazena žádná domovská složka, přiřadí systém k uživatelskému účtu výchozí místní domovskou složku.

Shrnutí kapitoly



Za účelem sdílení prostředků se počítače v síti se sdružují do skupin, max. dvacet počítačů. Všechny počítače jsou rovnocenné, žádný z počítačů nemá kontrolu nad jiným počítačem. Všechny počítače musí být ve stejné místní síti nebo podsíti.

Každý počítač má sadu uživatelských účtů. Pro přihlášení do počítače pracovní skupiny, je nutné v něm mít uživatelský účet. Pracovní skupina není chráněna heslem.

Pro komunikaci v rámci pracovních skupin ve Windows musí mít každý uživatel ve všech počítačích, na nichž pracuje, vytvořen uživatelský účet. Přístup těchto účtů je omezen na lokální prostředky. Jedná se o takzvané místní uživatelské účty. Každý počítač má svou vlastní databázi účtů (kont). Princip místních uživatelských účtů je vhodný pro malé sítě typu peer-to-peer.

Ve větších počítačových sítích typu klient server se počítače sdružují do domén. Počítače mohou být v různých místních sítích. Uživatelé používají doménové účty (konta) uživatelů a skupin (někdy také označované jako globální účty a globální skupiny). Prostřednictvím serverů správci sítě řídí zabezpečení a oprávnění všech počítačů v doméně – centralizovaná správa účtů. Uživatelský účet v doméně, umožňuje se přihlásit ke kterémukoli počítači v doméně.

Doménové uživatelské účty jsou vytvořené v databázi Active Directory. Místo přihlášení na počítač přes místní uživatelský účet, se provádí přihlašování přes doménový účet do domény. V doméně existuje jeden centrální server (takzvaný řadič domény), na kterém je uložena databáze uživatelů a skupin domén.

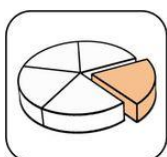
V databázi uživatelů a skupin u obou typů účtů existují účty

- výchozí a
- účty vytvořené správcem - standardní uživatelské účty.

Kontrolní otázky a úkoly



- 1) Co je to pracovní skupina?
- 2) Co je to doména?
- 3) Jaké účty se používají v pracovní skupině a co umožňují?
- 4) Jaké účty jsou v doméně a co umožňují?
- 5) Kde je v doméně uložena databáze uživatelů a skupin domén?
- 6) Jaké se vytvářejí výchozí účty?



Použitá literatura a jiné zdroje:

- [1] Místní uživatelé a skupiny. *Technet.microsoft.com* [online]. © 2012 [cit. 2012-04-06]. Dostupné z: [http://technet.microsoft.com/cs-cz/library/cc786411\(v=ws.10\).asp](http://technet.microsoft.com/cs-cz/library/cc786411(v=ws.10).asp)
- [2] Principy skupin. *Technet.microsoft.com* [online]. © 2012 [cit. 2012-04-08]. Dostupné z: [http://technet.microsoft.com/cs-cz/library/cc776995\(v=ws.10\).aspx](http://technet.microsoft.com/cs-cz/library/cc776995(v=ws.10).aspx)
- [3] Uživatelské účty a účty počítačů. In: Windows server [online]. © 2012 Microsoft [cit. 2012-05-12]. Dostupné z: [http://technet.microsoft.com/cs-cz/library/cc759279\(v=ws.10\).aspx](http://technet.microsoft.com/cs-cz/library/cc759279(v=ws.10).aspx)
- [4] Vytvoření uživatelského účtu. In: Windows [online]. Microsoft Corporation, © 2012 Microsoft Corporation [cit. 2012-05-12]. Dostupné z: <http://windows.microsoft.com/cs-cz/Windows7/Create-a-user-account>
- [5] ČERVENKA, Petr. VŠB OSTRAVA. Počítačové kurzy: Windows server 2008. [2012]. [cit. 2012-05-12].

22 OS Windows: Skupiny a zvláštní identity

Obsah hodiny



Obsahem této hodiny je popis skupin a zvláštních identit ve Windows.

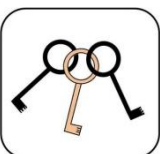
Cíl hodiny



Po prostudování budete schopni:

- charakterizovat lokální skupiny,
- charakterizovat doménové skupiny a jejich rozdělení,
- orientovat ve vytváření skupiny,
- orientovat se ve skupinách výchozích,
- charakterizovat zvláštní identity.

Klíčová slova



Skupiny lokální, Skupiny doménové, Skupiny výchozí, Zvláštní identity

22.1 Uživatelské skupiny lokální a doménové

Skupina je soubor účtů uživatelů a počítačů, kontaktů a jiných skupin, které lze spravovat jako jednu jednotku. Uživatelé a počítače patřící ke konkrétní skupině jsou označováni jako členové skupiny.

Použití skupin může zjednodušit správu díky tomu, že lze najednou přiřadit společnou sadu oprávnění a práv k mnoha účtům namísto jejich přiřazování k jednotlivým účtům.

Skupiny uživatelů se vytvářejí z důvodu přidělování přístupových práv k prostředkům více uživatelům. Správce přiděluje oprávnění skupině a uživatel po přidělení do skupiny oprávnění zdědí. Takže správce jednoduchým vložením uživatele do konkrétní skupiny, přidělí uživateli všechna uživatelská práva přiřazená ke skupině a všechna oprávnění přiřazená ke skupině u libovolného sdíleného prostředku.

Existují tři typy skupin:

- Lokální skupiny – jsou vytvořené a spravované na lokálním počítači.
- Bezpečnostní skupiny (Security Groups) – mají asociovaný bezpečnostní identifikátor. Jsou to doménové objekty.
- Distribuční skupiny – jsou používány pouze jako distribuční seznamy pro e-mailové aplikace (bez práv, identifikátoru).

Podobně jako uživatelé, mají skupiny svůj bezpečnostní identifikátor SID.

Lokální skupiny jsou zřízeny na konkrétních počítačích, nelze je využívat na jiných počítačích. Neměly by se používat na počítačích zařazených do domény, nelze je totiž centrálně spravovat.

Lokální skupiny nemohou být členem jiných skupin. Členem lokální skupiny mohou být pouze lokální konta.

Dále se skupiny dělí podle rozsahu působnosti:

- Místní doménové skupiny (Domain Local Groups) zajišťují přístup k síťovým zdrojům v dané doméně. Do místních skupin lze přidat místní uživatelské účty, uživatelské účty domény, účty počítače nebo skupinové účty.
- Univerzální skupiny zajišťují přístup k síťovým zdrojům v různých doménách, používají se vyjíměčně.
- Globální skupiny se používají k rozčlenění doménových uživatelských účtů (obvykle podle pracovního zařazení). Členové globálních skupin získají práva až díky zařazení své globální skupiny do lokální doménové skupiny.

Skupiny s místním rozsahem usnadňují definování a správu přístupu k prostředkům v jedné doméně. Tyto skupiny mohou obsahovat následující členy:

- účty z libovolné domény,
- globální skupiny z libovolné domény,
- univerzální skupiny z libovolné domény,
- místní doménové skupiny, ale pouze ze stejné domény, jako je nadřazená místní doménová skupina,
- libovolnou kombinaci výše uvedených možností.

Je vhodné, aby jména skupin začínala DL (doménové skupiny), U (univerzální skupiny), G (globální skupiny) a dále obsahovala řetězec charakterizující účel skupiny, pro lepší orientaci mezi skupinami.

22.2 Postup tvorby skupin

1. Zorganizovat uživatele globálních skupin, např. podle útvaru, funkce.

G_Reditelstvi, G_Provoz1, G_Ucetni...

2. Vytvořit lokální doménové skupiny v doménách, podle toho, co nabízejí ke sdílení

DL_FakturyR (R - přístup do faktur jen čtení), DL_FakturyF (F – plný přístup k fakturám)

3. Přiřadit globální skupiny do lokálních doménových skupin.

Do DL_FakturyR přiřadit G_Reditelstvi a G_Provoz1, do DL_FakturyF přiřadit G_Ucetni

4. Přidělit práva a oprávnění.

22.3 Výchozí skupiny

Při instalaci se vytvářejí předdefinované skupiny – výchozí skupiny. Po instalaci většina nemá žádné členy. Na serveru jsou to skupiny:

- Administrators (členem je účet Administrator, po zařazení do domény skupina Domain Admins),
- Backup operators,
- Guests (členem je účet Guest, po zařazení do domény skupina Domain Guests),
- Power Users,
- Replikator,
- Users (pozor, pouze na stanici je členem Administrator, na serveru není, po zařazení do domény skupina Domain Users),
- Account operators,
- Print operators,
- Domain Admins,
- Domain Guests,
- Domain Users.

Výchozí skupiny pro domény jsou umístěny v kontejnerech Builtin a Users. Kontejner Builtin obsahuje skupiny definované s místním rozsahem domény. Kontejner Users obsahuje skupiny definované s globálním rozsahem a skupiny definované s místním rozsahem domény.

Skupiny obsažené v těchto kontejnerech lze přesunout do jiných skupin nebo organizačních jednotek v rámci domény, ale nelze je přesunout do jiných domén.

22.4 Místní (lokální) skupiny

Administrators. Členové této skupiny mají oprávnění k plnému řízení počítače a mohou podle potřeby přiřazovat uživatelům uživatelská práva a oprávnění řízení přístupu. Účet Správce je výchozím členem této skupiny. Po připojení počítače k doméně je k této skupině automaticky přidána skupina Domain Admins. Tato skupina má oprávnění k úplnému řízení počítače a z tohoto důvodu je přidání uživatelů do této skupiny potřeba pečlivě zvážit.

Guests. Členům této skupiny se při přihlášení vytvoří dočasný profil. Tento profil je po odhlášení člena odstraněn. Účet Guest (ve výchozím nastavení zakázán) je také výchozím členem skupiny.

Users. Členové této skupiny mohou provádět běžné úlohy, jako např. spouštět aplikace, používat místní a síťové tiskárny nebo zamykat počítače. Členové této skupiny nemohou sdílet adresáře ani vytvářet místní tiskárny. Ve výchozím nastavení mezi členy této skupiny patří skupiny Domain Users, Authenticated Users a Interactive. Z tohoto důvodu se každý uživatelský účet vytvořený v doméně stane členem této skupiny.

Power Users. Ve výchozím nastavení nemají členové této skupiny jiná uživatelská práva a oprávnění než ta, která jsou součástí standardního uživatelského účtu. V předchozích verzích systému Windows byla skupina Power Users navržena tak, aby dala uživatelům zvláštní práva správce a taková oprávnění, která by jim umožnila provádět běžné systémové úlohy. V současné době Windows má již standardní uživatelský účet ve své vlastní podstatě schopnost provádět základní běžné konfigurační úlohy (jako např. změna časových pásem).

Skupina Backup Operators. Členové této skupiny mohou zálohovat a obnovovat soubory v počítači bez ohledu na oprávnění, která tyto soubory chrání. Právo provádět zálohování má totiž přednost před všemi oprávněními k souboru. Členové této skupiny nemohou měnit nastavení zabezpečení.

Další výchozí skupiny

- Remote Desktop Users – vzdálený přístup,
- Skupina Cryptographic Operators – kryptografické operace,
- Skupina Distributed COM Users – přístup k objektům modelu DCOM,
- Skupina IIS_IUSRS - je využívána službou Internet Information Services,
- Network Configuration Operators - nastavení protokolů TCP/IP,
- Performance Monitor Users – monitorování čítače výkonu,

- Performance Log Users – správa čítače výkonu, protokoly a výstrahy,
- Replicator - podporuje funkce replikace,
- Offer Remote Assistance Helpers - vzdálenou pomoc uživatelům.

22.5 Doménové skupiny

Doménové skupiny v kontejneru Builtin

Account Operators. Členové této skupiny mohou vytvářet, upravovat a odstraňovat účty uživatelů, skupin a počítačů umístěných v kontejnerech Users nebo Computers a v organizačních jednotkách v doméně.

Administrators. Členové této skupiny mají oprávnění k úplnému řízení všech řadičů domény.

Users. Členové této skupiny mohou provádět většinu běžných úkolů, například spouštět aplikace, používat místní a síťové tiskárny nebo zamykat server. Ve výchozím nastavení mezi členy této skupiny patří skupiny Domain Users, Authenticated Users a Interactive. Každý uživatelský účet vytvořený v dané doméně se tedy stane členem této skupiny.

Další skupiny:

- Guests,
- Backup Operators,
- Print Operators,
- Remote Desktop Users,
- Incoming Forest Trust Builders,
- Network Configuration Operators,
- Performance Monitor Users,
- Performance Log Users,
- Pre-Windows 2000 Compatible Access,
- Replicator,
- Server Operators.

Doménové skupiny v kontejneru Users (typ Global)

Domain Admins. Členové této skupiny mají oprávnění k úplnému řízení domény. Ve výchozím nastavení je tato skupina členem skupiny Administrators ve všech řadičích domény, všech pracovních stanicích domény a všech členských serverech domény v době, kdy jsou připojeny k doméně. Ve výchozím nastavení je účet správce členem této skupiny.

Domain Computers. Tato skupina obsahuje všechny pracovní stanice a servery připojené k doméně. Ve výchozím nastavení se každý vytvořený účet počítače automaticky stává členem této skupiny.

Domain Controllers. Tato skupina obsahuje všechny řadiče domény v doméně.

Domain Guests. Tato skupina obsahuje všechny hosty domény.

Domain Users. Tato skupina obsahuje všechny uživatele domény. Ve výchozím nastavení se každý vytvořený uživatelský účet v doméně automaticky stává členem této skupiny. Tato skupina může představovat všechny uživatele v doméně. Pokud například mají mít všichni uživatelé v doméně přístup k tiskárně, lze přiřadit oprávnění pro tiskárnu k této skupině (nebo přidat skupinu Domain Users k místní skupině na tiskovém serveru, který má oprávnění pro tuto tiskárnu).

Cert Publishers. Členové této skupiny jsou oprávněni publikovat certifikáty pro uživatele a počítače.

DnsAdmins. Členové skupiny mají přístup ke správě služby DNS Server.

DnsUpdateProxy. Členy této skupiny jsou klienti služby DNS, kteří mohou provádět dynamické aktualizace jménem jiných klientů, například serverů DHCP.

22.6 Zvláštní identity

Servery se systémem Windows Server 2008 R2, Windows Server 2008 nebo Windows Server 2003 obsahují kromě skupin v kontejneru Users a Builtin několik zvláštních identit. Tyto identity jsou pro zjednodušení obecně označovány jako skupiny. Tyto speciální skupiny nemají specifická členství, která je možné upravovat. V závislosti na okolnostech však představují různé uživatele v různých okamžicích. Zvláštní identity tvoří následující skupiny.

Anonymous Logon. Tato skupina představuje uživatele a služby, kteří získávají přístup k počítači a jeho prostředkům pomocí sítě bez použití názvu účtu, hesla nebo názvu domény. V počítačích se systémem Windows NT a nižších verzí je skupina Anonymous Logon výchozím členem skupiny Everyone. V počítačích se systémem Windows Server 2008 R2, Windows Server 2008 nebo Windows Server 2003 není skupina Anonymous Logon ve výchozím nastavení členem skupiny Everyone.

Authenticated Users. Všichni uživatelé (i počítače) mající platný účet v počítači nebo v doméně (uživatelé z různých domén) a byli někým autentifikováni, nepatří zde Guest.. Brání anonymnímu přístupu ke zdrojům.

Everyone. Tato skupina představuje všechny aktuální uživatele sítě, včetně uživatelů Guest a uživatelů z jiných domén. Při každém přihlášení uživatele do sítě je uživatel automaticky přidán do skupiny Everyone.

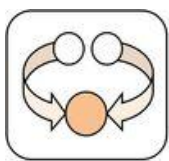
Network. Tato skupina představuje uživatele, kteří aktuálně přistupují k danému prostředku prostřednictvím sítě, nikoli pomocí místního přihlášení k počítači, kde je prostředek umístěn. Vždy, když uživatel získá přístup k dané prostředku prostřednictvím sítě, je tento uživatel automaticky přidán do skupiny Network.

Interactive. Tato skupina představuje všechny uživatele, kteří jsou aktuálně přihlášení k určitému počítači a přistupují k danému prostředku umístěnému v tomto počítači. Nezískávají tedy přístup k prostředku pomocí sítě. Vždy, když uživatel získá přístup k danému prostředku v počítači, ke kterému je aktuálně přihlášen, je tento uživatel automaticky přidán do skupiny Interactive.

Dialup. Uživatelé právě připojení přes modem.

Ačkoli je možné přiřadit zvláštním identitám práva a oprávnění k prostředkům, nelze členství zvláštních identit měnit nebo prohlížet. Pro zvláštní identity nelze použít rozsah skupin. Uživatelé jsou do těchto zvláštních identit přiřazováni automaticky při přihlášení nebo získání přístupu k určitému prostředku.

Shrnutí kapitoly



Skupina je soubor účtů uživatelů a počítačů, kontaktů a jiných skupin, které lze spravovat jako jednu jednotku. Uživatelé a počítače patřící ke konkrétní skupině jsou označováni jako členové skupiny.

Správce přiděluje oprávnění skupině a uživatel po přidělení do skupiny oprávnění zdědí.

Existují tři typy skupin:

- lokální skupiny,
- bezpečnostní skupiny,
- distribuční skupiny.

Dále se skupiny dělí podle rozsahu působnosti:

- Místní doménové skupiny (Domain Local Groups) zajišťují přístup k síťovým zdrojům v dané doméně. Do místních skupin lze přidat místní uživatelské účty, uživatelské účty domény, účty počítače nebo skupinové účty.
- Univerzální skupiny zajišťují přístup k síťovým zdrojům v různých doménách, používají se vyjíměčně.
- Globální skupiny se používají k rozčlenění doménových uživatelských účtů (obvykle podle pracovního zařazení). Členové globálních skupin získají práva až díky zařazení své globální skupiny do lokální doménové skupiny.

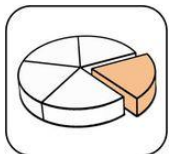
Při instalaci se vytvářejí předdefinované skupiny – výchozí skupiny. Po instalaci většina nemá žádné členy.

Servy se systémem Windows Server obsahují kromě skupin několik zvláštních identit. Tyto identity jsou pro zjednodušení obecně označovány jako skupiny. Tyto speciální skupiny nemají specifická členství, která je možné upravovat. V závislosti na okolnostech však představují různé uživatele v různých okamžicích.

Kontrolní otázky a úkoly



- 1) Charakterizujte skupiny ve Windows OS.
- 2) Jaké jsou tři typy skupin ve Windows OS?
- 3) Jak se skupiny ve Windows dělí podle rozsahu působnosti?
- 4) Jaký se doporučuje postup tvorby skupin?
- 5) Co jsou to zvláštní identity?
- 6) Uveďte příklady výchozích skupin a zvláštních identit?

Použitá literatura a jiné zdroje:

- [1] Místní uživatelé a skupiny. *Technet.microsoft.com* [online]. © 2012 [cit. 2012-04-06]. Dostupné z: [http://technet.microsoft.com/cs-cz/library/cc786411\(v=ws.10\).asp](http://technet.microsoft.com/cs-cz/library/cc786411(v=ws.10).asp)
- [2] Principy skupin. *Technet.microsoft.com* [online]. © 2012 [cit. 2012-04-08]. Dostupné z: [http://technet.microsoft.com/cs-cz/library/cc776995\(v=ws.10\).aspx](http://technet.microsoft.com/cs-cz/library/cc776995(v=ws.10).aspx)
- [3] Správa skupin. *Technet.microsoft.com* [online]. únor 2009 [cit. 2012-04-08]. Dostupné z: <http://technet.microsoft.com/cs-cz/library/dd861324.aspx>
- [4] ČERVENKA, Petr. VŠB OSTRAVA. Počítačové kurzy: Windows server 2008. [2012]. [cit. 2012-05-12].

23 OS Windows: Práva a oprávnění

Obsah hodiny



Obsahem této hodiny je vysvětlení pojmů práva a oprávnění.

Cíl hodiny



Po prostudování budete schopni:

- popsat práva a oprávnění,
- orientovat se oprávněních souborů a složkách,
- vysvětlit pojem dědičnost,
- popsat UAC.

Klíčová slova



Oprávnění, Práva, Dědičnost, Primitivní oprávnění, UAC

23.1 Práva a oprávnění

Pod souhrnným označením oprávnění si většina uživatelů představí sadu pravidel pro přístup k datům, sdíleným prostředkům nebo speciálním funkcím systému. Windows však rozlišují **oprávnění a práva**. Oprávnění (anglicky permission) je možnost přistupovat k některému objektu vybraným způsobem.

Právo (right) dovoluje provést některou systémovou akci – přidat nového uživatele, změnit nastavení plochy, určit systémové datum apod.

Oprávnění určuje vlastník prostředku. Např. u souboru má možnost nastavit a změnit oprávnění jak správce, tak vlastník souboru, kterým může být jeho autor. Vlastník prostředku pak konkrétní oprávnění přidělí jednotlivým uživatelům nebo skupině.

23.2 Oprávnění k souborům a složkám

Oprávnění se nastavuje přes položku *Properties (Vlastnosti)* v místní nabídce na kartě *Security*. Na kartě se nastavují permission (oprávnění). Tato oprávnění jsou vlastně kombinací „primitivních oprávnění“ (dále PO), jakési balíčky oprávnění namíchané pro nejobvyklejší případy použití.

- **Full Controll**, úplné řízení (Modify+PO Change Permissions, Také Ownership, Delete Subfolders and Fields),
- **Modify**, měnit (Read&Execute+Write+PO Delete),
- **Read&Execute**, číst a spouštět (Read+PO Traverse Folder/Execute File),
- **Read**, číst (PO, ve kterých je slovo Read),
- **Write**, zapisovat (PO, ve kterých je slovo Write),
- **List Folder Contents**, zobrazovat obsah složky (Read&Execute, pouze pro složky, nedědí se na soubory).

Nejvyšším oprávněním v rámci NTFS je Full Controll, úplné řízení, které uživatelům dovoluje měnit oprávnění, spouštět soubory, listovat složkami, upravovat soubory apod. Důležité také je, že oprávnění úplného řízení umožní uživateli převzít vlastnictví složky, čehož lze s výhodou využít například při připojení disku z jiného počítače.

Další oprávnění kromě úplného řízení mají u souborů a složek intuitivní pojmenování, jedná se o oprávnění měnit, číst a spouštět, zapisovat, nebo pouze číst.

Popsaná přístupová oprávnění NTFS by mohla v určitých případech kolidovat, a tak se řídí některými důležitými pravidly.

- Oprávnění jsou kumulativní – výsledné oprávnění je kombinací oprávnění dané skupiny, kam uživatel patří, a přímo oprávnění, která jsou spojena s jeho účtem.
- Oprávnění k souboru mají vyšší váhu než oprávnění k dané složce. Toto pravidlo jde dokonce do extrému: pokud má uživatel ke složce úplné řízení, ale konkrétnímu souboru v ní pouze čtení, nebude moci soubor zapisovat!

Řízení přístupu je proces ověřování uživatelů, skupin a počítačů pro přístup k objektům v síti pomocí oprávnění, uživatelských práv a auditu objektů.

Primitivní oprávnění (*karta permissions/tlačítko edit*)

- Traverse Folder/Execute File, Procházet složkou/ Spouštět soubory,
- List Folder/Read Data, Zobrazovat obsah složky/Číst data.
- Read Attributes,
- Read Extended Attributes,
- Create Files/Write Data,
- Create Folders/Append Data (nutný pro uložení dokumentu po změně),
- Write Attributes, (nutný pro uložení dokumentu po změně),
- Write Extended Attributes, (nutný pro uložení dokumentu po změně),
- Delete Subfolders and Fields (pouze pro složku),

- Delete (umožňuje i přejmenování),
- Read Permissions (zobrazení karty Security, bez možnosti změn),
- Change Permissions (zobrazení karty Security, zpřístupnění tlačítka *Add a Advanced*),
- Take Ownership (zobrazení karty Security, zpřístupnění tlačítka *Advanced*).

23.3 Dědičnost

Při vytváření standardně složka nebo soubor zdědí oprávnění složky, ve které se nachází. Dědění je možné zrušit (*karta Permissions*). Ruší se všechna oprávnění pro všechny uživatele a skupiny.

Předávání oprávnění pouze zčásti – jen některým souborům a složkám se realizuje přes kartu s *Triviálními právy*.

Při kopírování se mění vlastnictví složky a souboru – obojí se vlastně znovu vytvoří a tak dědí oprávnění z cílové složky. Pozor! Při přesunu v rámci svazku se zachovává původní vlastník i oprávnění.

23.4 Řízení uživatelských účtů – UAC

Nástroj *Řízení uživatelských účtů* je funkce systému Windows, která pomáhá zabránit neoprávněným změnám v počítači. Dříve než se provedou akce, které by mohly ovlivnit chod počítače nebo změnit nastavení ovlivňující ostatní uživatele, systém požádá o povolení nebo heslo správce.

Díky žádostem o ověření před spuštěním akcí může nástroj *Řízení uživatelských účtů* zabránit tomu, aby se nainstaloval škodlivý software (malware) a či spyware, případně aby provedl nepovolené změny v počítači.

Je-li potřeba k dokončení úlohy povolení nebo heslo, zobrazí nástroj *Řízení uživatelských účtů* jednu z následujících zpráv:



K pokračování této akce potřebuje systém Windows vaše povolení.

Funkce systému Windows nebo program, který může ovlivnit ostatní uživatele, potřebuje ke spuštění vaše povolení.



Program potřebuje vaše povolení, aby mohl pokračovat.

Program, který není součástí systému Windows, potřebuje ke spuštění vaše povolení. Má platný digitální podpis označující název programu a vydavatele.



Neznámý program požaduje přístup k tomuto počítači.

Neznámý program je program bez platného digitálního podpisu vydavatele, který umožňuje ujistit se, že program je tím, za co se vydává.



Tento program je blokován.

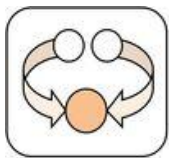
Tento program byl zablokován správcem, aby nemohl být v počítači spuštěn. Pro spuštění, je třeba oprávnění správce. Jedná o funkci, která má za úkol zvýšit bezpečnost celého systému.

UAC v definovaných chvílích částečně zatemní obrazovku a zobrazí dialogové okno, v němž čeká na potvrzení od administrátora. Až po schválení akce pokračuje a provede požadovanou operaci.

Pod Windows 7 lze volit mezi čtyřmi různými stupni *Řízení uživatelských účtů*. Při nejbezpečnějším nastavení bude systém informovat o všech změnách systémových nastavení, které zásadně vyžadují oprávnění správce. K jakémukoliv nastavení UAC bude zapotřebí další uživatelský souhlas.

Nejnižší úroveň neposkytuje žádné informace a pracuje plně automaticky. Je-li uživatel přihlášen jako správce, mohou hackeři nebo viry bez problémů a nepozorovaně provádět systémové změny. Pokud používá uživatelský účet bez oprávnění správce, Windows bez zpětného dotazu odeprou všechny změny systému.

Shrnutí kapitoly



Windows rozlišují práva a oprávnění. Právo (right) dovoluje provést některou systémovou akci – přidat nového uživatele, změnit nastavení plochy, určit systémové datum apod.

Oprávnění (anglicky permission) je možnost přistupovat k některému objektu vybraným způsobem. Každé oprávnění je vlastně souhrnem „Primitivních oprávnění“.

Oprávnění určuje vlastník prostředku, přiděluje oprávnění jednotlivým uživatelům nebo skupině.

Nejvyšším oprávněním v rámci NTFS je Full Control, úplné řízení. Další oprávnění kromě úplného řízení mají u souborů a složek intuitivní pojmenování, jedná se o oprávnění měnit, číst a spouštět, zapisovat, nebo pouze číst.

Přístupová oprávnění NTFS by mohla v určitých případech kolidovat, a tak se řídí některými důležitými pravidly:

- Oprávnění jsou kumulativní,
- Oprávnění k souboru mají vyšší váhu než oprávnění k dané složce.

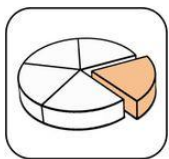
Při vytváření standardně složka nebo soubor zdědí oprávnění složky, ve které se nachází. Dědění je možné zrušit.

Nástroj Řízení uživatelských účtů je funkce systému Windows, která pomáhá zabránit neoprávněným změnám v počítači. Dříve než se provedou akce, které by mohly ovlivnit chod počítače nebo změnit nastavení ovlivňující ostatní uživatele systém požádá o povolení nebo heslo správce.

Kontrolní otázky a úkoly



- 1) Co jsou to práva a co oprávnění?
- 2) Kdo přiděluje oprávnění?
- 3) Jaká jsou v NTFS nejvyšší oprávnění?
- 4) Uveďte některá oprávnění.
- 5) Co jsou to primitivní oprávnění?
- 6) Vysvětlete pojem dědění oprávnění.
- 7) Co je to UAC a jaký je jeho význam?

Použitá literatura a jiné zdroje:

- [1] Novinky Windows 7: Řízení uživatelských účtů (UAC). In: Extra Windows [online]. 24.9.2009 [cit. 2012-05-12]. Dostupné z: <http://extrawindows.cnews.cz/novinky-windows-7-rizeni-uzivatelskych-uctu-uac>
- [2] BITTO, Ondřej. Jak fungují práva a oprávnění Windows?. Jak na počítač [online]. 12.4.2010 [cit. 2012-05-12]. Dostupné z: <http://jnp.zive.cz/jak-funguji-prava-a-opravneni-windows>
- [3] ČERVENKA, Petr. VŠB OSTRAVA. Počítačové kurzy: Windows server 2008. [2012]. [cit. 2012-05-12].

24 MS Windows: profily uživatelů

Obsah hodiny



Obsahem této hodiny je seznámení s profily v OS MS Windows.

Cíl hodiny



Po prostudování budete schopni:

- charakterizovat profily, jejich funkci,
- popsat vytvoření profilů a způsob aktualizace,
- charakterizovat cestovní profily a mandatory profily.

Klíčová slova



Profily lokální, Profily cestovní, Mandatory profily

24.1 Uživatelské profily, funkce, rozdělení

Uživatelské profily popisují pracovní prostředí jednotlivých uživatelů. Vytváří se automaticky, při prvním přihlášení uživatele na počítač.

V profilu jsou uloženy informace o nastavení pracovní plochy uživatele, např.:

- rozlišení obrazovky,
- vzhled oken, barvy,
- položky z nabídky Programy, atd.

Ukládají se v něm Temporary Internet Profiles (profilový podadresář Local Settings), což je obsah internetových stránek, které uživatel v poslední době navštívil. Pozor, zvětšuje velikost profilu. Je proto vhodné prostor pro ně omezit nebo mazat. V profilu je také nastaveno, která síťová připojení se uživateli nabídnou.

Uživatelské profily umožňují, aby různí uživatelé, kteří používají jeden počítač, mohli používat různě nastavené pracovní prostředí. Nebo opačně, aby uživatel, který pracuje v síti na různých počítačích, měl k dispozici své pracovní prostředí, tak jak je na něj zvyklý. Z toho pohledu rozdělujeme profily na:

- lokální (místní),
- cestovní (roaming).

Do adresáře s lokálním profilem má přístup pouze vlastník konta nebo skupina Administrátor a uživatel System, práva se z nadřazeného nedědí.

V adresáři je skrytý soubor NTUSER.DAT. V něm je uložena většina nastavení. Při přihlášení uživatele se tato nastavení zkopírují do registru HKEY_CURRENT_USER. V podadresáři Desktop (Plocha) je definován vzhled pracovní plochy včetně ikon na ní, kopíruje se do HKEY_CURRENT_USER\Environment. To, které položky bude mít uživatel v nabídce Programs, určuje struktura podadresáře Start Menu\Programs.

Pro sdílení dat mezi uživateli na lokálním počítači je ve Windows 2008 určen serverový adresář Public v User (nahradil Documents and Settings).

Lokální profily mají lokální – místní působnost, jsou umístěny na počítači, na kterém uživatelé pracují, ke kterému se pravidelně přihlašují. Jsou v adresáři Users\uživatelské jméno (ve Windows 2000/2003 Documents and Settings\ uživatelské jméno).

Cestovní profily mají platnost v rámci domény, jsou umístěny na serveru. Jsou určeny pro uživatele, kteří se hlásí na své konto v doméně a používají různé počítače. Do adresáře s cestovním profilem na serveru má přístup pouze vlastník konta a uživatel System. Administrátor se bez převzetí vlastnictví do adresáře nedostane.

Cestovní profil zajišťuje, že mají na každém počítači svůj vlastní profil. Při konfiguraci uživatelského účtu je nutno nastavit cestu k profilu na serveru (*Profile path*, karta *Profile* ve vlastnostech konta), pokud tato položka není nastavena, použije se po přihlášení profil lokální.

24.2 Vytvoření a aktualizace cestovního profilu

Uživateli se po přihlášení vytváří na lokálním počítači kopie cestovního profilu (je pak rychleji dosažitelný, méně zatěžuje síť). Po odhlášení se aktualizuje profil jak na lokálním počítači (lokální profil), tak cestovní profil na serveru.

Cestovní profil se vytváří při prvním přihlášení po vytvoření konta. Na doménovém řadiči se vznikne automaticky adresář se jménem a cestou tak, jak je to nastaveno v *Profile path*. Na počítači, ze kterého se doménový

uživatel přihlásil, se v adresáři Users (ve Windows 2000/2003 Documents and Settings) vytvoří automaticky adresář lokálního profilu se jménem konta, zkopíruje se do něj struktura Default z lokálního počítače (pouze při prvním přihlášení!).

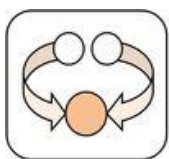
Při každém odhlášení se lokální adresář aktualizuje a zkopíruje se do cestovního profilu na serveru – tím je zajištěn pokaždé aktuální stav cestovního profilu. Při přihlášení uživatele se cestovní profil opět zkopíruje na daný počítač, při prvním celý, při dalším pouze změny.

Kopírování profilů (při aktualizaci) způsobuje zdlouhavé přihlašování a odhlašování doménového uživatele. Pokud je spojení s doménovým řadičem pomalé a doménový uživatel se pravidelně hlásí z jednoho počítače, lze v *System/User Profiles* změnit cestovní profil na místní (a opačně) na tomto počítači (pak nedochází k jeho aktualizaci na serveru).

24.3 Povinný cestovní profil – Mandatory Profil

Je to cestovní profil, který je chráněný proti zápisu, nedá se měnit. Je určený pro konta, která jsou určena více uživatelům, aby si nemohli vzájemně profil měnit. Ochrana se neřeší přes změnu oprávnění, ale přejmenováním NTUSER.DAT na NTUSER.MAN.

Shrnutí kapitoly



Uživatelské profily popisují pracovní prostředí jednotlivých uživatelů. V profilu jsou uloženy informace o nastavení pracovní plochy uživatele: rozlišení obrazovky, vzhled oken, barvy, položky z nabídky Programy, atd.

Uživatelské profily umožňují, aby různí uživatelé, kteří používají jeden počítač, mohli používat různě nastavené pracovní prostředí. Nebo opačně, aby uživatel, který pracuje v síti na různých počítačích, měl k dispozici své pracovní prostředí, tak jak je na něj zvyklý. Z toho pohledu rozdělujeme profily na:

- lokální (místní),
- cestovní (roaming).

Zvláštním typem cestovního profilu je Mandatory Profil, který je chráněný proti zápisu, nedá se měnit. Je určený pro konta, která jsou určena více uživatelům, aby si nemohli vzájemně profil měnit.

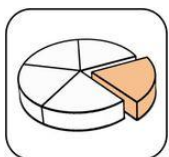
Uživatelský profil se uživateli vytvoří automaticky, při jeho prvním přihlášení na počítač.

Kontrolní otázky a úkoly



- 1) Co je to profil uživatele a jaká je jeho funkce?
- 2) Jak se vytváří a aktualizují profily?
- 3) Jaké jsou typy profilů?
- 4) Jaký je rozdíl mezi cestovním a lokálním profilem?
- 5) Co je to Mandatory Profil?

Použitá literatura a jiné zdroje:



- [1] ČERVENKA, Petr. VŠB OSTRAVA. Počítačové kurzy: Windows server 2008. [2012]. [cit. 2012-05-12].

25 Správa souborových systémů

Obsah hodiny



Obsahem této hodiny je popis základních pojmů týkajících se souborových systémů z pohledů správy.

Cíl hodiny



Po prostudování budete schopni:

- vysvětlit pojem logickou strukturu disku
- charakterizovat souborový systém,
- specifikovat úkoly správy souborových systémů.

Klíčová slova



Logická struktura disku, FS, RAID

25.1 Logická struktura disku

Pro ukládání souborů na disk potřebuje OS vytvořit na disku strukturu logickou. Za tím účelem je třeba disk rozdělit na oblasti a podoblasti (primární, extended, logické disky). Pevný disk může být rozdělen na 4 primární oblasti nebo na 3 primární oblasti a jednu rozšířenou oblast.

Rozšířenou oblast (extended) lze dále rozdělit na další podoblasti – logické disky. Každá disková oblast, podoblast se pak chová jako samostatný disk.

K rozdělení disku na oblasti se používá příkaz fdisk nebo speciální nástroje, které umožňují rozdělit disk bez zničení dat.

Na začátku každé diskové oblasti, podoblasti disku je zaváděcí sektor (VBR). Zaváděcí sektory jsou velké 512 bytů, a slouží k uložení kódu pro spuštění operačního systému uloženého na tomto oddílu.

Hlavní zaváděcí sektor - MBR je umístěn na nulté stopě, nultém sektoru. V MBR je uložena tabulka rozdělení disku a zaváděcí záznam se zaváděčem OS.

Dalším formátováním vytváří OS na diskové oblasti, podoblasti svůj souborový systém, tj. svoji vlastní strukturu pro ukládání dat. Sektory rozděluje do větších „shluků“. Ty jsou pak základní alokační jednotkou. V MS Windows se označují jako clustery, v Unixových systémech bloky.

Stejně jako u paměti RAM i na disku dochází při ukládání dat k nežádoucí fragmentaci.

Proč je vhodné rozdělit disk na oddíly:

- Správně rozdělený disk na oddíly je více přehledný.
- Šetření místem při výběru správného souborového systému (např. pro malé soubory). Velký oddíl u FAT32 zvětšuje clustery.
- Lepší administrace a údržba disku (defragmentace, správa místa, formátování).
- Bezpečnost dat, ochrana a izolace uživatelských dat při havárii operačního systému a oddílů.
- Možnost koexistence více operačních systémů.
- Možnost využívat výhody jednotlivých souborových systémů.

25.2 LVM (Logical Volume Management)

Pomocí LVM lze spojovat více fyzických zařízení - disků, diskových oddílů, RAID nebo jiných úložných zařízení do logických celků, které pak lze dále využívat stejně jako klasické diskové oddíly.

- Physical volume (fyzický svazek) - oddíl na fyzickém disku, popřípadě celý fyzický disk.
- Volume group (skupina svazků, storage) - sdružuje jednotlivé fyzické svazky do jednoho celku, nad kterým se definují logické svazky.
- Logical volume (logický svazek) - je definován uvnitř skupiny svazků a ve výsledku se operačnímu systému jeví jako fyzický disk.

Nevýhodou běžných pevných disků je obtížné přerozdělování volného místa po jejich prvotním rozdělení na diskové oddíly. LVM tento problém řeší přidáním logické vrstvy (skupina svazků, storage) mezi fyzická média a OS. Do vytvořené logické jednotky lze snadno a kdykoli (pokud použité zařízení podporují hotswap) přidávat nebo odebírat fyzická zařízení a tím měnit její velikost případně nahrazovat starší disky za nové, atp., aniž by bylo nutné stroj restartovat.

V rámci této logické jednotky lze pak vytvářet logické diskové oddíly a pokud to podporuje souborový systém (např. ReiserFS, nebo XFS), i měnit za chodu jejich velikost.

LVM také umožňuje dělat za chodu snapshoty - tj. zakonzervovat stav diskového oddílu v určitý moment, a pak jej za chodu někam odzálahovat.

25.3 Co je to souborový systém

Data se na disk nebo jiné záznamové médium ukládají ve formě souborů jako sekvence bajtů.

Souborový systém je datová struktura vytvořená vysokoúrovňovým formátováním pevného disku, která slouží k organizaci dat do souborů, adresářů na pevném disku tak, aby je bylo možné snadno najít a přistupovat k nim. Určuje, jak se mají soubory ukládat, jmenovat, vyhledávat, jaké mají vlastnosti a řídí kdo a jakým způsobem s nimi může nakládat.

Informace uložené v systému souborů dělíme na:

- metadata (informace o souborech (vlastník, časové značky, práva,...),
- data.

Souborové systémy používají k ukládání dat paměťová média jako pevný disk nebo optické paměti (CD, DVD, Blu-Ray), popřípadě poskytují přístup k datům uloženým na serveru (síťové souborové systémy).

Většina souborových systémů dnes používá hierarchickou stromovou strukturu adresářů a vznikla současně s vývojem nějakého operačního systému (FS Unixové, MS Windows, ...) nebo jako standard pro zápis na určité na CD (ISO 9660 a jeho rozšíření, UDF).

FS v současných OS byly přepracovány pro efektivní využívání velkokapacitních disků. Společným rysem dnešních OS je žurnálování.

25.4 Zabezpečení dat

- Zálohování (viz. OPS I)
- Vícenásobné diskové pole RAID (viz. HW možnosti zabezpečení)

RAID (Redundant Array of Inexpensive/Independent Disks) je vícenásobné diskové pole nezávislých disků. Jedná se o technologii řadičů, která koordinovaně řídí přístup ke dvěma nebo více diskům současně. Účelem je zvýšení kapacity, bezpečnosti nebo rychlostí (případně vše).

V principu jde o spojení několika disků do jednoho svazku, který se navenek tváří jako jeden pevný disk. Technické řešení diskových polí je dvojit, hardwarové a softwarové. V prvním případě se o spojení disků stará hardwarový řadič, v druhém totéž zajistí jádro operačního systému.

25.5 Kvóty (anglicky *quota*)

Diskové kvóty jsou limity nastavené správcem systému, které určitým způsobem omezují použití souborového systému. Nejčastěji se kvóty používají na omezení:

- velikosti využitého místa (usage nebo block quota),
- počtu souborů (file nebo inode quota)

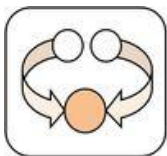
Dále může administrátor systému nastavit varování, tzv. soft quota, které uživatele informuje v případě, že se blíží ke svému limitu (který je pak nazýván hard quota). Často se také nastavuje tzv. grace interval, který v případě potřeby umožňuje krátkodobé mírné překročení kvóty.

25.6 Co je úkolem správy FS

Nástroje pro správu souborového systému musí řešit činnosti spojené s vytvořením a údržbou FS:

- rozdělení disku,
- formátování disku,
- řízení přístupu k datům na disku,
- přidělování diskového prostoru,
- mapování disků,
- zálohování dat,
- vytváření RAID,
- logování
- ...

Shrnutí kapitoly



Pro ukládání souborů na disk potřebuje OS vytvořit na disku strukturu logickou. Za tím účelem je třeba disk rozdělit na oblasti a podoblasti (primární, extended, logické disky). Pevný disk může být rozdělen na 4 primární oblasti nebo na 3 primární oblasti a jednu rozšířenou oblast.

Data se na disk nebo jiné záznamové médium ukládají ve formě souborů jako sekvence bajtů.

Souborový systém je datová struktura vytvořená vysokoúrovňovým formátováním pevného disku, která slouží k organizaci dat do souborů, adresářů na pevném disku tak, aby je bylo možné snadno najít a přistupovat k nim.

Zabezpečení dat:

- Zálohování
- Vícenásobné diskové pole RAID (viz. HW možnosti zabezpečení)

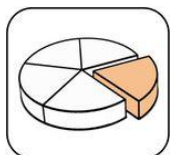
Nástroje pro správu souborového systému musí řešit činnosti spojené s vytvořením a údržbou FS.

Kontrolní otázky a úkoly



- 1) Co je to logická struktura disku?
- 2) Jak lze rozdělit disk?
- 3) Co je to souborový systém?
- 4) Jak zabezpečíme data na disku?
- 5) Co je to RAID?

Použitá literatura a jiné zdroje:



- [1] HORÁK, Jaroslav. Hardware: učebnice pro pokročilé. 3. aktualiz. vyd. Brno: CP Books, 2005, 344 s. ISBN 80-251-0647-0.
- [2] SHAH, Steve. Administrace systému Linux: jak porozumět svému počítači : podrobný průvodce začínajícího administrátora. 2. vyd. Praha: Grada, 2003, 533 s. ISBN 80-247-0641-5.

26 OS Linux: Správa FS

Obsah hodiny



Obsahem této hodiny je popis práce s diskem v Linuxu: rozdělení disku, připojování diskových oddílů.

Cíl hodiny



Po prostudování budete schopni:

- orientovat se v rozdělení disku a nástrojích pro práci s diskem,
- popsat připojování oddílů, FS,
- konfiguraci připojování.

Klíčová slova



Fdisk, Příkaz mount, Soubor `/etc/fstab`

26.1 Disk, diskové oddíly v Linuxu

V OS Linux je každý disk (diskový oddíl) reprezentován jako zařízení s vlastním názvem, tedy jako blokový soubor uložený v adresáři `/dev`. (X=písmeno, představuje jedno fyzické zařízení, Y číslo oddílu na disku):

- IDE disky: `/dev/hdaXY`,
- SCSI disky: `/dev/sdaXY`.

Rozdělení disků je úkolem správce systému zpravidla při instalaci OS. Dnes nabízí většina distribucí už při samotné instalaci jednoduché grafické rozhraní, anebo lze využít přímo program `fdisk`, který je standardním nástrojem pro rozdělování disků.

Způsob rozdělení disku vychází z požadavků na provoz. Pokud jde o OS určený pro domácí potřeby, stačí tři oddíly: `swap`, `/` (kořenový) a `home`. Pro provoz serverových služeb je výhodnější rozdělení na více oddílů (např.: `swap`, `/` (kořenový), `/boot`, `/home`, `/user`, `/var`, `/tmp`).

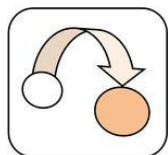
Diskové oddíly se k systému připojují pomocí přípojných bodů (prázdných adresářů). Definují místo, kde je v adresářovém stromu umístěné příslušné zařízení s FS.

Výše uvedené oddíly se připojují ke kořenovému oddílu označenému znakem lomítka: /. Jednotlivé prázdné adresáře jsou jakousi vstupní bránou k připojeným diskovým oddílům. Podobně se připojují rovněž FS umístěné na jiných zařízeních než je pevný disk (CD, flash disk). Pro jejich připojení se v adresářovém stromu vytvoří adresář a přes něj se připojí do stromu. Vzniká tak iluze jediného virtuálního FS¹⁶.

26.2 Programy pro práci s diskovými oddíly

fdisk

Základním nástrojem pro práci s diskem je v Linuxových distribucích program *fdisk*. Pro práci s ním je třeba oprávnění root. Jedná se o řádkový příkaz s řadou přepínačů a sadou příkazů.



fdisk -l vypíše tabulku rozdělení disku

```
# fdisk -l
```

```
Disk /dev/hda: 40.0 GB, 40020664320 bytes
255 heads, 63 sectors/track, 4865 cylinders
Units = cylinders of 16065 * 512 = 8225280 bytes
```

Device	Boot	Start	End	Blocks	Id	System
/dev/hda1	*	1	4864	39070048+	7	HPFS/NTFS

```
Disk /dev/hdb: 80.0 GB, 80026361856 bytes
255 heads, 63 sectors/track, 9729 cylinders
Units = cylinders of 16065 * 512 = 8225280 bytes
```

Device	Boot	Start	End	Blocks	Id	System
/dev/hdb1		1	7649	61440561	7	HPFS/NTFS
/dev/hdb2	*	7650	8954	10482412+	83	Linux
/dev/hdb3		8955	9728	6217155	f	Win95 Ext'd (LBA)
/dev/hdb5		8955	8987	265041	82	LinuxSwap

#

Přepínače:

- b velikost sektoru (512, 1024, 2048 nebo 4096)
- c vypne režim kompatibility s DOSem
- h vypíše nápovědu

¹⁶ Další informace k FS v OS Linux jsou v modulu Operační systémy I.

- u vrací velikosti v sektorech namísto v cylindrech
- v vypíše verzi
- C určuje počet cylindrů
- H určuje počet hlav
- S určuje počet sektorů na sto

Pro práci s diskem je k dispozici základní sada příkazů pro rozdělení disku, vytvoření diskových oddílů. Rozšířením této sady je režim experta a to zadáním příkazu "x".

Základní příkazy:

- a přepne příznak "startovací"
- b úprava bsd popisu disku
- c přepne příznak "DOS kompatibilní"
- d smaže diskový oddíl
- l vypíše známé typy diskových oddílů
- m vypíše tuto nabídku
- n vytvoří nový diskový oddíl
- o vytvoří prázdnou tabulku rozdělení disků typu IBM (DOS)
- p vypíše tabulku rozdělení disku
- q ukončí program bez uložení změn
- s vytvoří prázdný Sun popis disku
- t změní ID systému diskového oddílu
- u změní jednotky v nichž jsou vypisovány informace
- v ověří tabulku rozdělení disku
- w uloží tabulku rozdělení disku a ukončí program
- x rozšiřující funkce (pouze pro odborníky)

GParted (<http://gparted.sourceforge.net/>)

GParted je grafický program pro správu diskových oddílů. Ke stažení je jako ISO soubor, který se vypálí jako Live CD. Umožňuje měnit velikost, kopírovat a přesouvat diskové oddíly bez ztráty dat:

- změnit velikost oddílu,
- vytvořit místo pro nový OS,
- pokus o záchranu dat ze ztracených diskových oddílů.

Další programy pro práci s diskem:

- *Sfdisk* – linuxový editor oddílů.
- *Cfdisk* – funkčně podobný s programem fdisk, má však pohodlnější uživatelské rozhraní.
- *Disk Drake* – Mandrake/Mandriva GUI
- *Partition Magic* – Windows

26.3 Připojování a odpojování FS

Po připojení disků, diskových oddílů do jedné stromové struktury se celý virtuální FS jeví jako jeden strom s kořenem / a s podadresáři. Připojení oddílu obsahujícího jádro systému a základ adresářové struktury (/) (s několika prázdnými adresáři) se realizuje při startu systému. Postupně, jak se provádějí další skripty, se do prázdných adresářů¹⁷ připojují další oddíly (prázdné adresáře nahrazují celé podadresářové stromy se soubory). Připojování se provádí příkazem *mount*. Totéž lze provádět podle potřeby za chodu systému příkazem *mount/umount* z *příkazové řádky*.

Syntaxe příkazu *mount*:

mount [parametry] zařízení adresář(přípojný bod)

```
mount -o ro /dev/hda3 /usr
```

Parametr *-o* definuje specifické parametry pro připojování: připojení pouze pro čtení (read only).

K odpojení se používá příkaz *umount*. Pro odpojení stačí zadat jeden parametr: buďto zařízení nebo adresář:

```
umount /dev/hda3 nebo umount /usr
```

/etc/fstab

Připojování a odpojování disků je řízeno konfiguračním souborem */etc/fstab*. Má formu tabulky, je v něm seznam všech připojovaných zařízení včetně všech parametrů nutných k připojování. Soubor se přečte při startu systému a připojí všechny oddíly, které jsou zde uvedené s parametrem *defaults* pro automatické připojení. V souboru */etc/fstab* jsou následující údaje:

- soubor zařízení (např. /dev/hda1),
- přípojný bod (např. /mnt/hda1),
- typ FS (např. ext3),
- parametry a volby (oddělené čárkou),

¹⁷ Adresáře musí být prázdné, protože se jinak jejich obsah překryje soubory připojovaného zařízení a nebudou přístupné, dokud nedojde k odpojení (umout).

- číslo používané programem dump (nula tady zcela postačí),
- číslo označující pořadí při kontrole filesystemu.

```
/dev/sda1 /media vfat ro,user,noauto 0 0
```

Některé parametry pro připojení oddílů v *fstab*:

- noauto (nepřipojuje oddíl při startu automaticky),
- users (s oddílem mohou manipulovat i běžní uživatelé – obvykle cdrom),
- codepage (znaková sada názvů souborů),
- iocharset (znaková sada, do které se budou exportovat názvy souborů),
- noexec (zakázané provádění souborů na tomto oddíle),
- umask (nastavení práv souborů),
- ro (read only - pouze ke čtení),
- rw (read/write - čtení i zápis).

Některé distribuce používají k automatickému připojování démona *supermount*, který sám sleduje, co se děje a automaticky připojuje/odpojuje zařízení. I ten používá */etc/fstab* stále jako svůj konfigurační soubor. Řádek pro *supermount* může vypadat třeba takto:

```
none /mnt/cdrom supermount dev=/dev/hdc,fs=auto,ro,-  
,iocharset=iso8859-1,codepage=850 0 0
```

26.4 Utility pro práci s oddíly

Výpis oddílů, které systém registruje

```
cat /proc/partitions
```

Kontrola chyb na disku

```
badblocks /dev/hda1 > /home/kjn/vadne_bloky
```

Výpis informací o souborovém systému

```
dumpe2fs /dev/hda1
```

Vytvoření kopie disku

```
dd if=/dev/hda1 of=image_hda1.iso
```

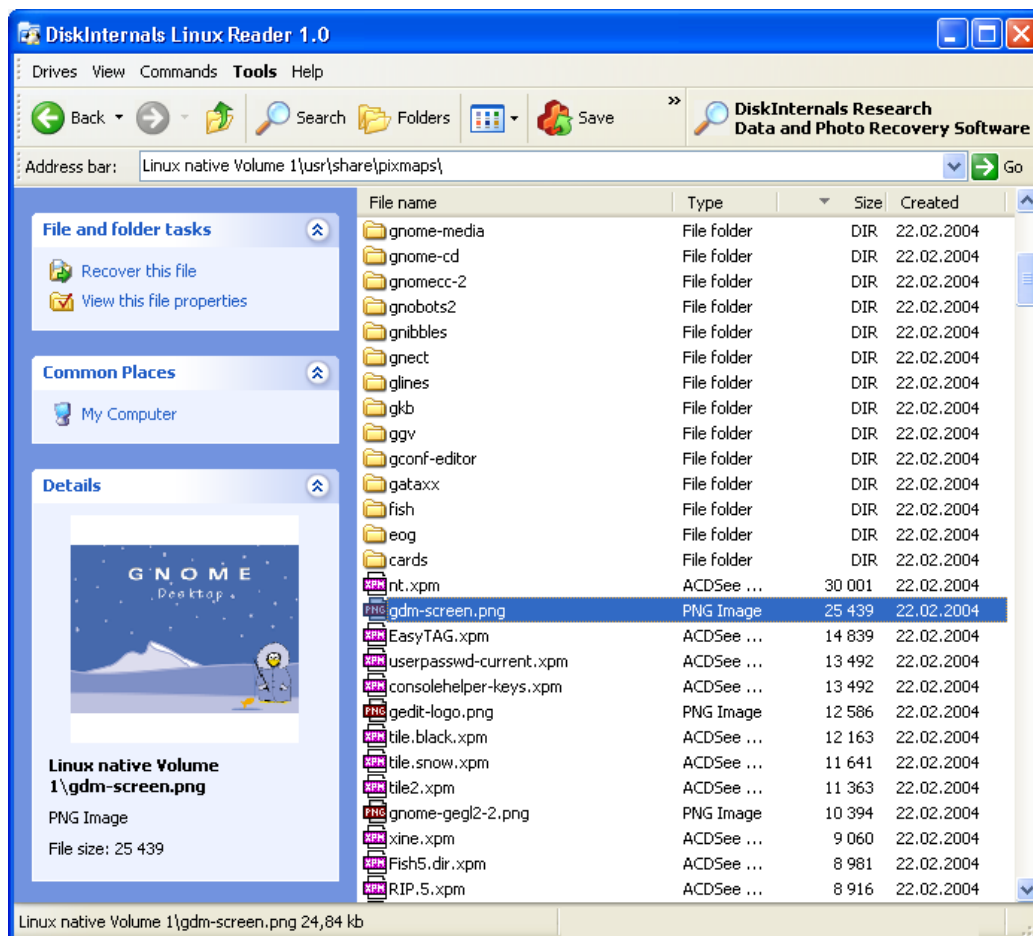
26.5 Přístup na linuxové disky z Windows

Jednorázový přístup

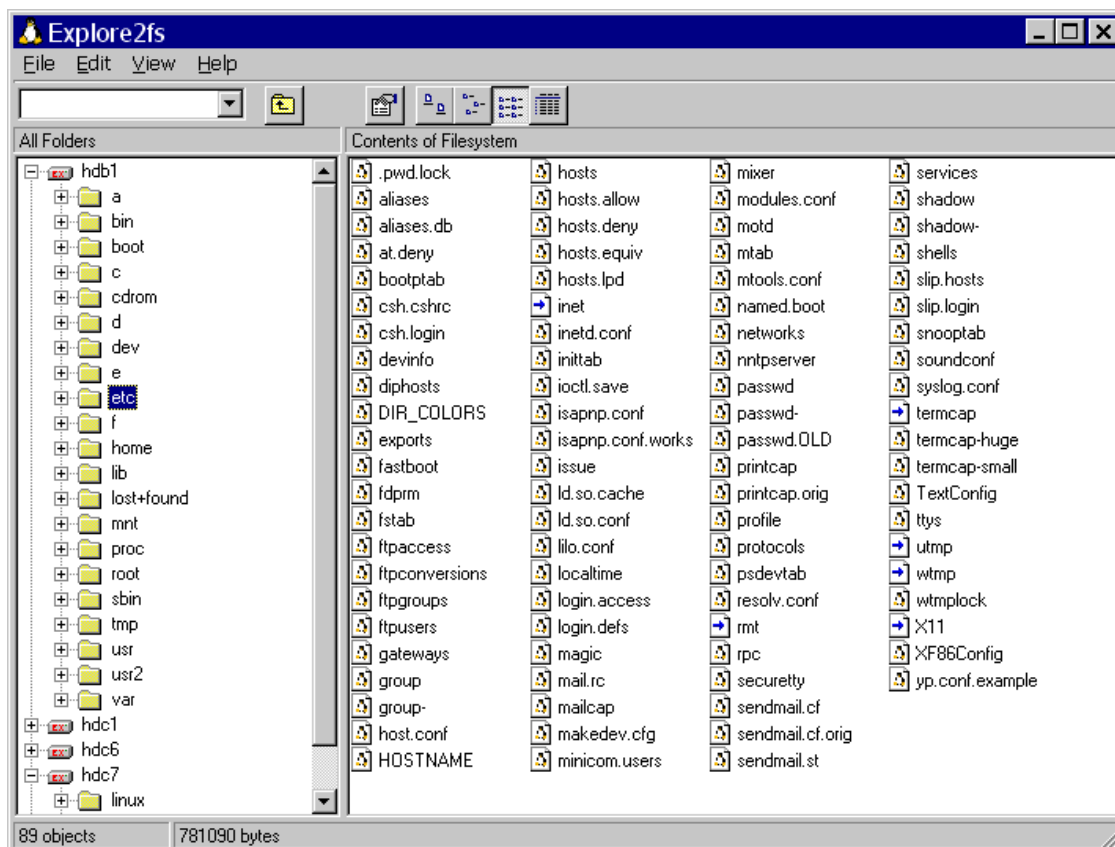
Windows nemají nativní podporu jiných než Windows souborových systémů, veškerá komunikace se tudíž odehrává přes externí nástroje. Pozor! Mohou obsahovat chyby. Záloha důležitých dat by měla být samozřejmostí.

Jednorázovým přístupem je myšleno spuštění programu, který dovolí procházet Linuxový disk a provádět operace se soubory, ale vše jen v rámci tohoto programu. Průzkumník disků neuvidí a ani jiné programy nebudou moci číst a ukládat z linuxového disku. Tento přístup se hodí, když je potřeba jednorázově nebo jednou za čas pouze z disku něco přečíst.

Disk Internals Linux Reader, Explore2fs jsou nástroje podobné Průzkumníku, které umožní procházet linuxové ext2, ext3 a ext4 disky a stahovat z nich data.



Obrázek 26-1: Disk Internals Linux Reader

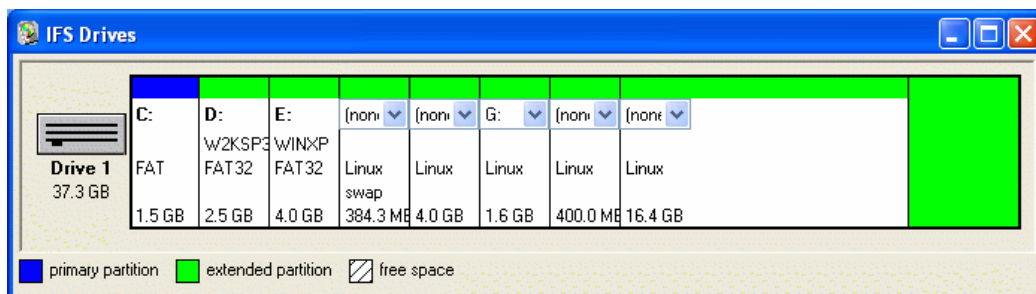


Obrázek 26-2: Explore2fs

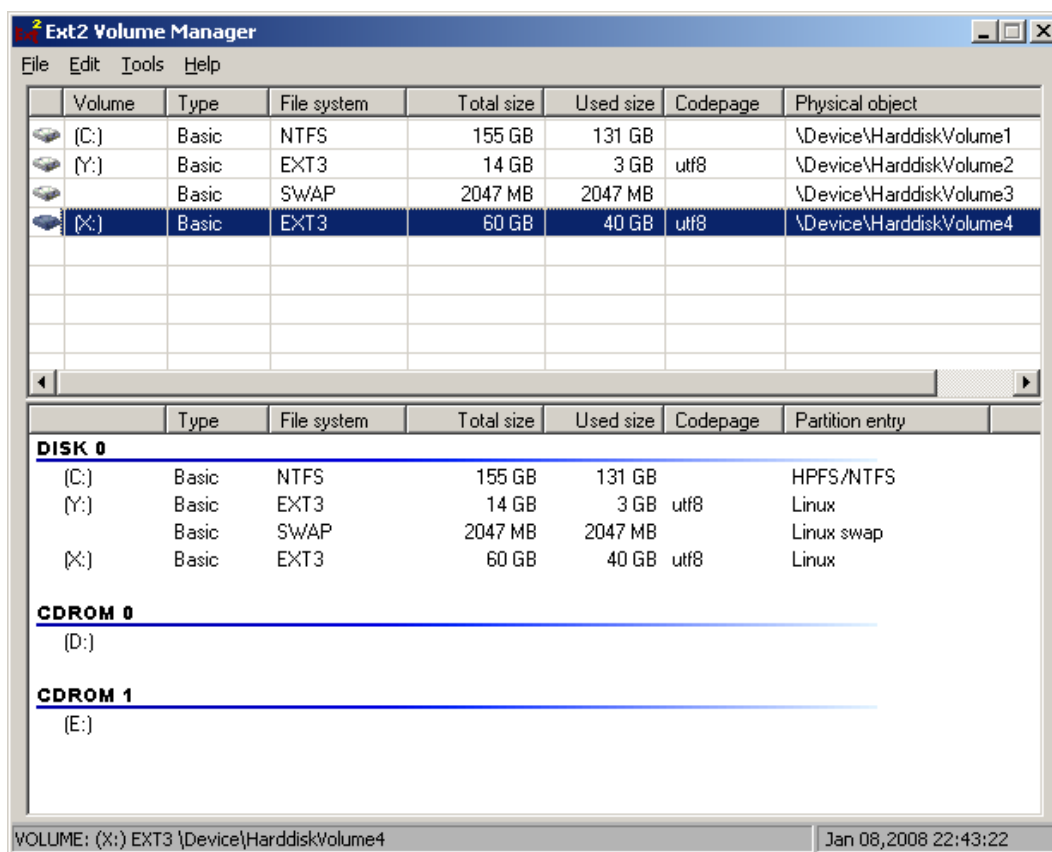
Stálý přístup

Windows se tváří, jakoby linuxové disky byly jeho vlastní. Jsou vidět v Průzkumníkovi a i všechny ostatní programy pracují s Linuxovými disky, aniž by poznaly jakýkoliv rozdíl. Jelikož podpora linuxových souborových systému je zpřístupněna pomocí nástrojů třetích stran, může připojení disků "non-stop" znamenat vyšší riziko ztráty nějakých dat.

Ext2 IFS, Ext2Fsd jsou nástroje, kterými se nainstaluje podpora pro linuxové souborové systémy ext2 a ext3 a připojí vybrané disky. Oba umí z disků číst i zapisovat. Umí připojit disky v UTF-8 kódování, takže všechny soubory a složky s českými znaky v názvu jsou správně.



Obrázek 26-3: Ext2 IFS



Obrázek 26-4:Ext2Fsd

Shrnutí kapitoly



V OS Linux je každý disk (diskový oddíl) reprezentován jako zařízení s vlastním názvem, tedy jako blokový soubor uložený v adresáři `/dev`.

Rozdělení disků se provádí zpravidla při instalaci OS. Většina distribucí při instalaci nabízí jednoduché grafické rozhraní, anebo lze využít přímo program *fdisk*.

Program *fdisk* je základním nástrojem pro práci s diskem. Jedná se o řádkový příkaz s řadou přepínačů a sadou příkazů. Pro práci s ním je třeba oprávnění *root*.

Diskové oddíly se k systému připojují pomocí přípojných bodů (prázdných adresářů) příkazem *mount*. Připojení se realizuje při startu systému nebo za jeho běhu.

K odpojení se používá příkaz *umount*.

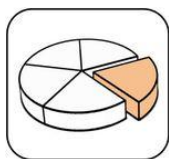
Připojování a odpojování disků je řízeno konfiguračním souborem `/etc/fstab`. Má formu tabulky, je v něm seznam všech připojovaných zařízení včetně všech parametrů nutných k připojování.

Některé distribuce používají k automatickému připojování démona *supermount*, který sám sleduje, co se děje a automaticky připojuje a odpojuje zařízení.

Kontrolní otázky a úkoly



- 1) Jak se rozděluje disk v Linuxu?
- 2) Jaké nástroje se používají pro práci s diskem v Linuxu?
- 3) Jak se připojují diskové oddíly?
- 4) Co je to přípojný bod?
- 5) Jak se používá příkaz *mount* a *umount*
- 6) Jak se konfiguruje připojování oddílů?
- 7) Jaká je funkce *supermount*?



Použitá literatura a jiné zdroje:

- [1] DYTRYCH, Karel. Diskové oddíly, rozdělování na partitions, swap. School.kjn.cz [online]. [cit. 2012-06-11]. Dostupné z: <http://school.kjn.cz/operacni-systemy/partitions.html>
- [2] SHAH, Steve. Administrace systému Linux: jak porozumět svému počítači : podrobný průvodce začínajícího administrátora. 2. vyd. Praha: Grada, 2003, 533 s. ISBN 80-247-0641-5.
- [3] KUŠNÍR, Michal. File Systems (souborový systém) v Linuxu [online]. 2011 [cit. 2012-06-15]. Dostupné z: <http://www.linux.website21.cz/navody/file-systems-souborovy-system-v-linuxu#programy-pro-praci-s-diskovymi-oddily>
- [4] GUNIŠ, Adrian. Ubuntu Česko Přístup na linuxové disky z Windows. Ubuntu.cz [online]. 2011 [cit. 2012-06-15]. Dostupné z: <http://wiki.ubuntu.cz/P%C5%99%C3%ADstup%20na%20linuxov%C3%A9%20disky%20z%20Windows>
- [5] DOČEKAL, Michal. Průvodce Linuxem: Správa GNU/Linuxu. Poznejlinux.c [online]. 2007 [cit. 2012-06-15]. Dostupné z: <http://www.poznejlinux.cz/linuxbook/xhtmll-chunks/ch06.html#id2587106>

27 MS Windows: Správa FS

Obsah hodiny



Obsahem této hodiny je správa souborového systému v OS Windows.

Cíl hodiny



Po prostudování budete schopni:

- orientovat se v nástrojích pro správu FS,
- popsat možnosti jednotlivých nástrojů.

Klíčová slova



Sdílené složky, Defragmentace disku, Správa disku, Kvóty, Blokování souborů

27.1 Správa sdílených složek: Nástroj Sdílené složky

Nástroj *Sdílené složky* umožňuje spravovat sdílené prostředky v celé síti. Pomocí nástroje *Sdílené složky* (*Správa počítače/Systémové nástroje*) je možné

- řídit uživatelská oprávnění k přístupu, aktivitu relace a vlastnosti sdílených prostředků,
- vytvořit, zobrazit a nastavit oprávnění pro sdílené prostředky,
- zobrazit souhrn připojení a použití prostředků u místních a vzdálených počítačů,
- zobrazit seznam všech uživatelů, kteří jsou k počítači připojeni pomocí sítě, a jednoho z nich nebo všechny odpojit,
- zobrazit seznam souborů, které jsou otevřeny vzdálenými uživateli, a jeden nebo všechny otevřené soubory zavřít.

27.2 Správa disků a svazků

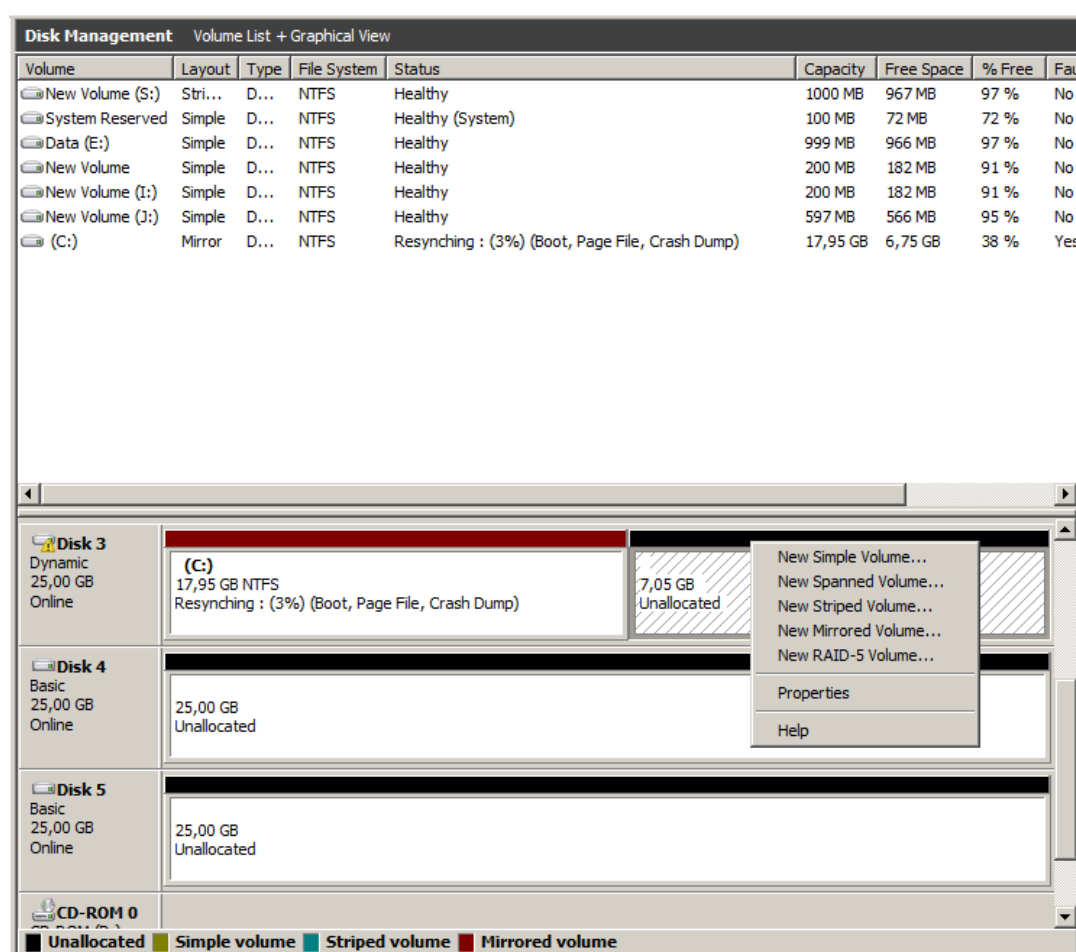
- Defragmentace disku
- Správa disků

Defragmentace disku

Nástroj *Defragmentace disku* analyzuje místní svazky a konsoliduje (defragmentuje) fragmentované soubory a složky tak, aby jednotlivě zabíraly jedno souvislé místo na svazku, což umožňuje rychlejší přístup k souborům, efektivnější ukládání souborů do vzniklého souvislého prostoru (menší pravděpodobnost fragmentace souborů).

Při defragmentaci disku mohou být defragmentovány svazky, které jsou formátovány v systému souborů FAT (file allocation table), systému souborů FAT32 a systému souborů NTFS.

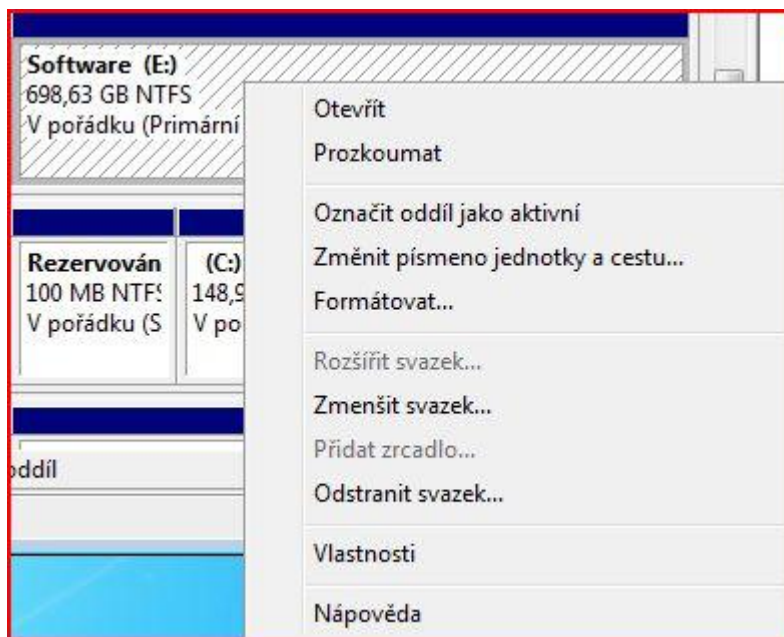
Správa disků



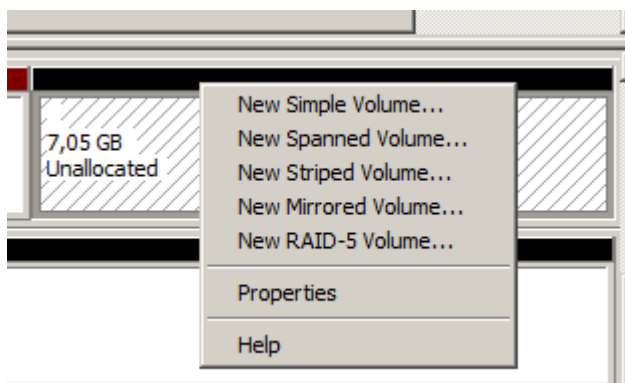
Obrázek 27-1: Disk Manager

Správa disků je systémový nástroj pro správu pevných disků a svazků nebo oddílů, které jsou na nich obsaženy. Pomocí nástroje *Správa disků* lze

- inicializovat disky,
- vytvořit svazky,
- formátovat svazky systémem souborů FAT, FAT32 nebo NTFS
- vytvořit diskové systémy odolné proti chybám (RAID).



Obrázek 27-2: Správa disků ve Windows 7



Obrázek 27-3: Správa disků Windows server

Správa disků umožňuje provádět většinu úloh souvisejících se správou disků, aniž by bylo nutné restartovat počítač nebo přerušit práci uživatelů; většina změn konfigurace vstupuje v platnost okamžitě.

27.3 Správce prostředků souborového serveru

Správa kvót umožňuje vytvořením kvót omezit místo povolené pro svazek nebo složku a generovat oznámení v případě, že jsou maximální kvóty dosaženy nebo překročeny.

Správa blokování souborů umožňuje definovat pravidla filtrování, která sledují nebo blokují pokusy uživatelů o uložení určitých typů souborů na svazek nebo do stromové struktury složek.

Správa sestav úložišť umožňuje generovat předdefinované sestavy pro sledování využití kvót, aktivity blokování souborů a vzory použití úložišť. Je také možné sledovat pokusy o uložení neoprávněných souborů u všech uživatelů nebo u vybrané skupiny uživatelů.

27.4 Zálohování serveru

Funkce *Zálohování serveru* poskytuje základní řešení pro zálohování a zotavení počítačů s operačním systémem Windows Server® 2008. *Zálohování serveru* zavádí novou technologii zálohování a obnovení a nahrazuje předchozí funkci zálohování v systému Windows (*Ntbackup.exe*), která byla dostupná v dřívějších verzích operačního systému Windows. Umožňuje zálohování celého serveru (všech svazků), vybraných svazků nebo stavu systému.

Funkci *Zálohování serveru* je možno použít k vytvoření a správě záloh místního počítače nebo vzdáleného počítače. Umožňuje také naplánovat automatické spouštění zálohování a provádět jednorázová zálohování rozšiřující plánovaná zálohování.

Shrnutí kapitoly



Nástroj *Sdílené složky* (pro desktopy i servery) umožňuje spravovat sdílené prostředky v celé síti.

Nástroj *Defragmentace disku* (pro desktopy i servery) analyzuje místní svazky a konsoliduje (defragmentuje) fragmentované soubory a složky tak, aby jednotlivě zabíraly jedno souvislé místo na svazku.

Správa disků je systémový nástroj pro správu pevných disků a svazků (pro desktopy i servery) nebo oddílů, které jsou na nich obsaženy. Pomocí nástroje *Správa disků* lze

- inicializovat disky,
- vytvořit svazky,
- formátovat svazky systémem souborů FAT, FAT32 nebo NTFS,
- vytvořit diskové systémy odolné proti chybám (RAID).

Nástroj *Správce prostředků* souborového serveru:

- Správa kvót,
- Správa blokování souborů.

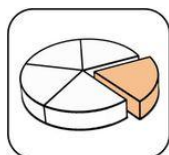
Nástroj *Zálohování serveru* poskytuje základní řešení pro zálohování a zotavení počítačů.

Kontrolní otázky a úkoly



- 1) Jaké nástroje jsou k dispozici pro správu FS ve Windows
- 2) Co umožňuje nástroj *Sdílené složky*?
- 3) Co umožňuje nástroj *Správa disků*?
- 4) Co je to defragmentace disku a jaký má význam?
- 5) Co umožňuje nástroj *Správce prostředků* souborového serveru?

Použitá literatura a jiné zdroje:



- [1] MICROSOFT. *Role Souborové služby* [online]. © 2012 [cit. 2012-06-10]. Dostupné z: [http://technet.microsoft.com/cs-cz/library/cc730983\(v=ws.10\)](http://technet.microsoft.com/cs-cz/library/cc730983(v=ws.10))

28 Instalace OS, aplikací (MS Windows, Linux)

Obsah hodiny



Obsahem této hodiny je popis procesu instalace a jeho specifika pro jednotlivé OS.

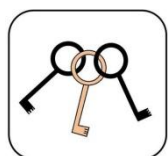
Cíl hodiny



Po prostudování budete schopni:

- popsat obecný instalační proces,
- orientovat se v typech instalací,
- orientovat se v základních licencích pro uživatele OS Windows,
- popsat způsoby instalace,
- orientovat se v požadavcích na HW.

Klíčová slova



Instalace, Instalátor, Čistá instalace, Klonování, Instalace OS Linux, Instalace OS Windows

28.1 Instalace SW

Instalace je v informatice proces, kdy je nový OS, počítačový program nebo ovladač nahrán (nakopírován) do počítače tak, aby uživatel mohl novou komponentu používat.

Programy jsou obvykle dodávány v podobě komprimovaných balíčků obsahujících sadu potřebných souborů do jediného souboru, protože se s nimi lépe manipuluje při distribuci a prodeji. Před vlastním použitím musí být balíček dekomprimován („rozbalen“), soubory umístěny na svá místa a provedeny i další potřebná nastavení.

Tvůrci software se v současnosti snaží, aby celý instalační proces, byl jednoduchý a nevyžadoval pokud možno žádné speciální znalosti. Za tímto účelem se vytváří instalátory, tj. programy, které řeší umístění instalovaných souborů, konfiguraci a další potřebné činnosti pokud možno bez nutnosti zásahů uživatele a fungují jako průvodci celou instalací včetně zprovoznění instalovaného SW.

Instalační programy na CD/DVD jsou často navrženy tak, aby se instalátor spustil automaticky po vložení média do mechaniky, což zajišťuje speciální soubor umístěný do kořenového adresáře média.

Některý je software navržen tak, aby nepotřeboval instalaci. Stačí pouze překopírování spustitelného souboru nebo adresáře se soubory na libovolné místo v počítači. Takový software se označuje jako přenositelný – *Portable*.

Také některé OS nepotřebují instalaci. Mohou být spuštěny přímo z bootovacích CD, DVD (tzv. Live CD) nebo USB flash disků. Výhodou je, že takto spuštěný operační systém nijak nezasahuje do systému nainstalovaném na počítači. Příkladem může být AmigaOS 4.0, Knoppix Linux, MorphOS, Mac OS 1-9, Windows PE a další.

Tichá instalace (silent installation): Při tiché instalaci se nezobrazují žádné informační zprávy.

Čistá instalace (clean installation): První instalace, do jejího průběhu nevstupují cizí vlivy, nemůže dojít ke kolizi z důvodu například existence souborů nebo nastavení z předešlých instalací programu. Příkladem může být instalace OS, kdy je cílový disk (resp. diskový oddíl) nejprve naformátován a instalace tak proběhne na prázdný disk.

Bezobslužná instalace (unattended installation): Bezobslužná instalace probíhá bez zásahu uživatele, popřípadě bez jeho vědomí.

Samoinstalace (self installation): Samoinstalace je instalace bez dozoru, která nepotřebuje prvotní spuštění. Jedná se například o různá zařízení, připojitelná přes USB rozhraní, přímo na kterých se nachází instalační program.

Instalace bez zobrazovací jednotky (headless installation): Instalace bez zobrazovací jednotky je prováděna bez použití monitoru nebo dokonce bez přítomnosti grafické karty, která by byla připojena do počítače, na kterém je instalace prováděna. Instalace tak může proběhnout z jiného počítače připojeného přes LAN nebo přes sériový port.

Plochá instalace (flat installation): Instalace programu není prováděna originálních instalačních médií (CD nebo DVD), ale z jejich kopie na pevný disk počítače, ne tedy přímo z původního média. Tento způsob instalace je výhodný v případě, že počítač není schopen provádět během instalace mnoho intenzivních I/O operací zároveň a je tedy výhodnější použít pro umístění instalačních souborů zařízení s rychlejším přístupem (pevný disk, CD, DVD, USB flash disk, ramdisk a podobně).

28.2 Instalace OS

Před vlastní instalací je třeba zvážit na jakém HW bude OS fungovat, jaké služby se budou na počítači provozovat včetně jejich konfigurace. Pokud systém má fungovat jako server, jsou kladeny vysoké nároky na jeho stabilitu, dostupnost a výkon.

Při čisté instalaci z DVD je nutné nejprve přepnout v BIOSu bootování z disku na DVD-ROM mechaniku. Po vložení instalačního média a restartování počítače dojde ke spuštění instalace. Průběh instalace řídí většinou instalátor.

Prvním krokem je načtení souborů potřebných pro instalaci (většinou se nabootuje jednoduchý OS určený pro instalaci). Následuje výběr jazyka, nastavení časové zóny a rozložení klávesnice. Pokud to vyžaduje instalovaný OS je potřeba přečíst a potvrdit podmínky licenční smlouvy.

Další částí instalace každého OS (pokud uvažujeme čistou instalaci) je vytvoření vhodného prostředí na disku tj. rozdělení disku na partition, naformátování disku pro daný FS (podle požadavků konkrétního OS a podle účelu jeho nasazení), nainstalování zavaděče do MBR.

Na připraveném diskovém oddílu se vytvoří adresářová struktura a nakopíruje jádro OS a všechny další části OS. Řadu služeb nebo programů, ovladačů lze instalovat z úložišť (depozitářů) na Internetu.

Pro komunikaci v síti je nutné nakonfigurovat síťové rozhraní. Zvolit firewall. Před prvním použitím je třeba vyplnit uživatelské jméno, heslo.

Pokud se nejedná o čistou instalaci, popř. se provádí reinstalace je třeba zvážit a realizovat ještě další kroky. Pak by vypadal doporučený postup následovně:

- záloha uživatelských dat ze staré instalace operačního systému,
- kontrola hardware počítače (kontrola paměti, pevného disku, ...),
- naformátování (přeformátování) pevného disku (vytvoření diskových oddílů),
- instalace systémového zavaděče (pokud se neinstaluje automaticky s instalací OS),
- instalace operačního systému,
- instalace ovladačů pro jednotlivá zařízení, záplat,
- uživatelská nastavení OS (bezpečnostní politika, firemní politika, uživatelská nastavení),
- vyčištění nově nainstalovaného operačního systému od zbytků instalačních souborů,
- záloha diskového oddílu s novou instalací OS,
- instalace dalšího SW, který není součástí OS,
- nakopírování zálohovaných uživatelských dat,

- uživatelská nastavení ostatních programů (typicky klient pro práci s elektronickou poštou),
- konečné úpravy (defragmentace pevného disku...).

Docela zásadní je jeden z prvních kroků instalace je a to rozdělení disků na partitions (oddíly). Správné rozdělení disku je základem dobré instalace. Je třeba zvážit kolik a jak velké oddíly bude ten který OS potřebovat pro systémové soubory, aplikace, data aplikací a uživatelů,, zálohování, swapování.

Pokud instalujeme na jeden disk více OS je vhodné dodržovat pořadí. U Windows od nejstaršího po nejnovější (nejdříve XP, poté Visty, poté Seveny...) a Linux se instaluje až naposled Toto pořadí je doporučeno z důvodu zachování funkčnosti zavaděče OS.



Obrázek 28-1: Příklad rozdělení pevného disku

28.3 Způsoby instalace

Pomocí instalačního média

Nejobvyklejším instalačním médiem v současnosti je CD-ROM či DVD-ROM. Pokud to podporuje základní deska (motherboard) vašeho stroje, tak lze použít jako instalační médium USB Flash disk.

Pokud se provádí instalaci bez připojení k síti, musíte být k dispozici všechna potřebná instalační média. Nestačí mít pouze nějaké minimální CD.

Po síti

Pokud síťová karta instalovaného stroje podporuje bootování po síti, je možné instalovat ze serveru s instalací. Jiná možnost je zavést systém ze např. z bootovacího CD a dále instalovat po síti.

Naklonováním již nainstalovaného systému

Celý systém (adresářovou strukturu a adresáře) lze nainstalovat (nakopírovat) na připravený disk z přichystaného "obrazu" (image) disku, jiného připojeného disku, nebo i spuštěného systému.

Výhodou je, že odpadá nezbytnost stahování softwarových balíčků. Celou operaci lze provést offline - tedy bez přístupu k internetu, nejsou potřeba žádná instalační média.

28.4 Instalace OS Linux

Při nákupu počítače, na kterém poběží Linux, je důležité se přesvědčit, že je hardware podporován jádrem operačního systému. Každý prodejce vydává seznam kompatibility hardware (HCL). Tyto informace lze dohledat na webových stránkách.

Někteří výrobci hardwaru totiž neposkytují informace potřebné k napsání ovladačů pro Linux, případně požadují podepsat smlouvu o uchování těchto informací v tajnosti před třetími osobami, což znemožňuje uveřejnění zdrojového kódu pro takový ovladač. Z důvodu nedostupnosti dokumentace pro tento hardware neexistují ovladače pro Linux. Ze stejných důvodů se doporučuje vyvarovat se zařízení „vyrobených pro Windows“.

Požadavky na hardware se liší podle distribuce, podle instalovaných služeb a použití.

Minimální hardwarové požadavky pro pracovní stanice:

- minimální doporučený procesor Pentium 4 na 1GHz,
- RAM: 128 MB, doporučeno 512 MB,
- pevný disk: 5 GB, doporučeno 16GB,
- vhodné je připojení k Internetu – instalace z veřejných depozitářů.

Rozdělení disku

- swap (odkládací oddíl),
- kořenový oddíl (/),
- další podle provozních nároků (viz část OS Linux: Správa FS).

Swapovací oddíl je nezávislá část pevného disku bez struktury FS, kterou Linux používá jako virtuální paměť, když dojde k nedostatku fyzické paměti. Velikost oddílu by měla být zpravidla 2x větší než je aktuální fyzická RAM (pro 512MB RAM, odkládací oddíl 1024MB). Tato hodnota je pouze orientační. Velikost by se měla řídit rovněž nároky aplikací, jejichž provoz se plánuje.

Kořenový souborový systém je reprezentován lomítkem (/). Nachází se v horní části adresářového stromu a obsahuje základní sadu souborů

a adresářů. Pro bezproblémové fungování Linuxu postačí s 16GB vyhrazeného místa. Je třeba počítat s instalací a provozem dalších aplikací jako kancelářské balíčky, programy pro pouštění hudby, videa, atd.

Instalace software

K instalaci (upgrade, odinstalování) programového vybavení v Linuxu se většinou používají *Správci programových balíčků distribuce*. Další možností je instalace ze zdrojových kódů zahrnující překlad, kompilaci.

28.5 Instalace OS Windows

Jako minimální pro běh systému Windows 7 se uvádí následující požadavky:

- Procesor: 1 GHz
- RAM: 512MB RAM, doporučeno 1 GB (32-bit), 2 GB (64-bit)
- Podpora DirectX 9 grafických zařízení se 128MB paměti
- Hard-Disk: 16 GB (32-bit), 20 GB (64-bit)
- grafická karta podporující alespoň DirectX 9 s WDDM

Další požadavky už se liší v závislosti na zvoleném typu instalace. Jsou jimi síťová karta, DVD-ROM mechanika a USB disk s kapacitou alespoň 4 GB.

Instalační soubory jsou na DVD v adresáři Sources:

- Boot.vim – boot manager po načtení do paměti zajistí základním instalačním prostředím Windows PE,
- Install.vim – instalace všech edicí Windows Server.

28.6 Novell SUSE LINUX Enterprise Server: HW požadavky

Minimální systémové požadavky pro instalaci

- Lokální instalace: 512 MB RAM, SSH-line síť
- Grafická instalace: 512 MB RAM, VNC-line síť
- Instalace přes FTP: 512 MB RAM

Minimální systémové požadavky pro provoz

- 512 MB RAM
- 750 MB volného místa na pevném disku pro software
- 750 MB volného místa na pevném disku pro uživatelská data

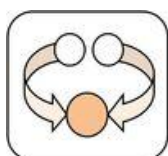
Doporučené systémové požadavky

- Minimálně 512 MB RAM pro Xen virtuálních hostitelských serverů
- Alespoň další 256 MB RAM per Xen virtuální stroj

Podporované procesor platformy

- AMD64
- IBM Power * * * (bývalé IBM iSeries a IBM pSeries systémy)
- IBM zSeries (64-bit)
- Intel EM64T
- Procesorů Itanium Muži (Itanium II nebo novější)
- X86

Shrnutí kapitoly



Instalace je v informatice proces, kdy je nový OS, počítačový program nebo ovladač nahrán (nakopírován) do počítače tak, aby uživatel mohl novou komponentu používat.

Při instalaci každého OS (pokud uvažujeme čistou instalaci) je nutné na disku vytvořit vhodné prostředí tj. rozdělit disk na partition, naformátovat disk pro daný FS (podle požadavků konkrétního OS a podle účelu jeho nasazení), nainstalovat zavaděč do MBR. Na připraveném diskovém oddílu se vytvoří adresářová struktura a nakopíruje jádro OS a všechny další části OS. Pro komunikaci v síti je nutné nakonfigurovat síťové rozhraní. Řadu služeb nebo programů lze instalovat z úložišť (depozitářů) na Internetu. Průběh instalace řídí i u OS většinou instalátor.

Typy instalace

- Tichá instalace
- Čistá instalace
- Bezobslužná instalace
- Samoinstalace
- Instalace bez zobrazovací jednotky
- Plochá instalace

Způsoby instalace

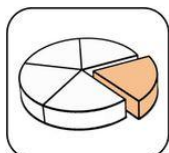
- Pomocí instalačního média
- Po síti
- Naklonováním již nainstalovaného systému

Kontrolní otázky a úkoly



- 1) Popište instalační proces
- 2) Uveďte typy instalací a jejich specifika.
- 3) Jaký je rozdíl mezi čistou instalací a reinstalací?
- 4) Jaké jsou způsoby instalace OS?

Použitá literatura a jiné zdroje:



- [1] Instalace_(software). In: Wikipedia: the free encyclopedia [online]. San Francisco (CA): Wikimedia Foundation, 2009, 2011 [cit. 2012-06-06]. Dostupné z: [http://cs.wikipedia.org/wiki/Instalace_\(software\)](http://cs.wikipedia.org/wiki/Instalace_(software))
- [2] Instalace a konfigurace OS (operačních systémů) Microsoft Windows, Linux.... In: IT Servis, Praha [online]. Copyright © 2010-2012 [cit. 2012-06-06]. Dostupné z: <http://itservispraha.cz/sluzby/instalace-os/>
- [3] Novell SUSE LINUX Enterprise Server: Systémové požadavky... [online]. [cit. 2012-06-10]. Dostupné z: <http://www.svetsoftware.cz/novell-suse-linux-enterprise-server>
- [4] SHAH, Steve. Administrace systému Linux: jak porozumět svému počítači : podrobný průvodce začínajícího administrátora. 2. vyd. Praha: Grada, 2003, 533 s. ISBN 80-247-0641-5.

29 Linux: síťové služby, konfigurace

Obsah hodiny



Obsahem této hodiny je popis konfigurace síťových služeb v Linuxu.

Cíl hodiny



Po prostudování budete schopni:

- popsat možnosti spuštění a zastavení služeb,
- orientovat se v možnostech konfigurace superserveru inetd,
- orientovat se v možnostech konfigurace superserveru xinetd,
- popsat možnosti řízení přístupu ke službám,
- charakterizovat konfigurační soubory nutné pro provoz služeb.

Klíčová slova



Superserver inetd, Superserver xinetd, Tcp_wrappers, Services, Protocols

29.1 Spuštění služeb

Služby lze v Linuxu jednoduše spouštět při startu systému pomocí rc-skriptů. Pro jednotlivé run levely se spouští přes symbolické odkazy nejčastěji z adresářů */etc/rcn.d* (přesné umístění je v */etc/inittab*). Vlastní spouštěcí skript je v adresáři *init.d* (další informace jsou v kapitole Linux: inicializace systému).

Služby lze samozřejmě spouštět, popř. zastavovat z příkazové řádky. A to zadáním názvu spouštěcího skriptu s parametrem *start*, který příslušnou a službu spustí, nebo s parametrem *stop*, ten službu zastaví. Pro zastavení popř. restart služby lze využít i příkaz *kill*, vždyť spuštěná služba je vlastně běžící proces.

29.2 Superserver inetd, xinetd

Běžící programy, které poskytují služby po síti, se označují jako *daemons* (démoni). Démon je proces, který otevře port konkrétní služby, a čeká na

příchozí spojení. Pokud k takovému spojení dojde, vytvoří proces potomka, jenž toto spojení obslouží a rodičovský proces bude stále pokračovat v odposlouchávání dalších požadavků.

Toto řešení má několik nevýhod.

- V paměti musí být trvale přítomna alespoň jedna instance každého démona pro každou provozovanou službu.
- V každém démonu se opakuje ta část kódu, která zajišťuje obsluhu a poslouchání na portu.

Řešením této neefektivity je na většině Unixových systémů speciální síťový démon označovaný jako *superserver*. Tento démon otevírá sokety pro řadu síťových služeb a na všech poslouchá. Když se na některém z portů objeví příchozí spojení, *superserver* je přijme a spustí server pro konkrétní port, kterému pak předá socket k obsluze. *Superserver* pak pokračuje v poslouchání na portech.

Nejběžnější *superserver* se jmenuje **inetd**, Internet Daemon. Je spouštěn při zavádění systému. Seznam služeb, které má spravovat, získává z konfiguračního souboru */etc/inetd.conf*.

Novou verzí této služby je *xinetd*. Má stejnou funkci, liší se výrazně jiným formátem konfiguračního souboru a disponuje dalšími možnostmi:

29.3 Konfigurace **inetd**

V tomto souboru se položka skládá z jednotlivých řádek, které jsou tvořeny následujícími poli:

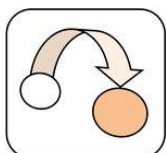
service type protocol wait user server cmdline

Význam jednotlivých polí:

- **service**: název služby,
- **type**: typ socketu: *stream* (pro protokoly využívající vlastností spojení - TCP), nebo hodnoty *dgram* (pro protokoly založené na diagramech - UDP),
- **protocol** název přenosového protokolu, který bude daná služba používat. (soubor *protocols*).
- **wait** tato volba se vztahuje pouze na typ socketu *dgram*. Nabývá hodnoty *wait* nebo *nowait*.; je-li zadána volba *wait*, spustí démon *inetd* pro daný port vždy pouze jeden server. V opačném případě bude po spuštění serveru okamžitě pokračovat v odposlouchávání portu;¹⁸

¹⁸ To je užitečné u "jednocestných" (single-threaded) serverů, které budou číst všechny přicházející datagramy tak dlouho, dokud nepřestanou přicházet a potom se ukončí. Většina serverů RPC vyhovuje tomuto typu a tudíž by u nich měla být uvedena volba *wait*.

- **user** přihlašovací uživatelské id, pod kterým bude daný proces spouštěn,
- **server** název plné cesty ke spouštěnému programu serveru, vnitřní služby jsou označeny klíčovým slovem *internal*¹⁹.
- **cmdline** příkazová řádka, která bude předána danému serveru, volba obsahuje argument 0, který odpovídá názvu příkazu, tímto názvem je obvykle vlastní název programu, u interních služeb je prázdné.



Soubor inetd.conf

```
#
# inetd služby

ftp stream tcp nowait root /usr/sbin/ftpd in.ftpd -l
telnet stream tcp nowait root /usr/sbin/telnetd
in.telnetd b/etc/issue

#finger stream tcp nowait bin /usr/sbin/fingerd
in.fingerd

#tftp dgram udp wait nobody /usr/sbin/tftpd in.tftpd
#tftp dgram udp wait nobody /usr/sbin/tftpd in.tftpd
/boot/diskless

login stream tcp nowait root /usr/sbin/rlogind
in.rlogind

shell stream tcp nowait root /usr/sbin/rshd in.rshd
exec stream tcp nowait root /usr/sbin/rexecd in.rexecd
#
# vnitřní služby inetd
#
daytime stream tcp nowait root internal
daytime dgram udp nowait root internal
time stream tcp nowait root internal
time dgram udp nowait root internal
```

Druhý typ serverů, tzv. "vícecestné servery" (multi-threaded), umožňují současně spouštět neomezený počet instancí; to je používáno jen velmi zřídka. U těchto serverů by měla být volba *nowait*. Sockety typu *stream* by měly vždy používat volbu *nowait*.

¹⁹ Služby, které provádí démon *inetd* sám. Tyto služby se nazývají vnitřní služby. Jednou z nich jsou např. služba *chargen*, která generuje řetězec znaků a služba *daytime*, která vrací systémový čas.

```
echo stream tcp nowait root internal
echo dgram udp nowait root internal
discard stream tcp nowait root internal
discard dgram udp nowait root internal
chargen stream tcp nowait root internal
chargen dgram udp nowait root internal
```

29.4 Kontrola přístupu ke službám pomocí `tcp_wrappers`

Některé služby jako např. *finger* a *fttp* je vhodné povolit pouze "důvěryhodným hostitelům", což ale nelze pomocí standardního nastavení, při kterém super-server *inetd* poskytuje tuto službu buď všem klientům, anebo žádnému klientovi.

Pro tento účel je vhodný nástroj *tcpd*, tzv. zástupce démonů. U služeb protokolu TCP, které je třeba monitorovat nebo chránit, je tento démon volán místo programu serveru. Nástroj *tcpd* zapisuje požadavky do démona *syslog*, kontroluje, zda je vzdálený hostitel oprávněn používat danou službu a pouze v tom případě spustí skutečný program serveru. Tento postup nefunguje u služeb založených na protokolu UDP.

Např.: Zastoupení démona *finger*. V souboru *inetd.conf* se změní odpovídající řádek následujícím způsobem:

```
# zastoupení démona finger
```

```
finger stream tcp nowait root /usr/sbin/tcpd in.fingerd
```

Pokud se nepřidá žádné řízení přístupu, bude se tato úprava klientovi jevit stejně, jako obvyklé nastavení služby *finger*, s tou výjimkou, že veškeré požadavky budou zapisovány s prioritou *auth* do souboru *syslog*.

Řízení přístupu je implementováno za pomoci dvou souborů, které obsahují položky, které některým hostitelům povolují, resp. zakazují přístup k určitým službám. Jmenují se */etc/hosts.allow* (přístup klientovi povoluje) a */etc/hosts.deny* (přístup klientovi povoluje). Při požadavku o službu se tyto soubory se v uvedeném pořadí prohledávají

Pokud je odpovídající položka nalezena v souboru *hosts.allow*, bude přístup povolen bez ohledu na položky v souboru *hosts.deny*. Pokud ale bude odpovídající položka nalezena v souboru *hosts.deny*, bude požadavek odmítnut a spojení se ukončí. Jestliže se ani v jednom souboru odpovídající položka nenajde, bude požadavek přijat.

Položky v souboru s přístupy vypadají následovně:

```
servicelist: hostlist [:shellcmd]
```

Pole `servicelist` obsahuje seznam názvů služeb ze souboru `/etc/services` nebo klíčové slovo `ALL`. Povolení všech služeb kromě *finger* a *tftp*:

```
ALL EXCEPT finger, tftp
```

Pole `hostlist` obsahuje seznam názvů hostitelů nebo IP-adres, případně klíčová slova `ALL`, `LOCAL` nebo `UNKNOWN`.

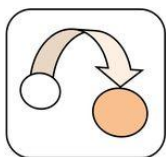
Zákaz přístupu ke službám *finger* a *tftp* všem hostitelům s výjimkou místních hostitelů:

Soubor /etc/hosts.allow ponechte prázdný

Soubor /etc/hosts.deny:

```
in.tftpd, in.fingerd: ALL EXCEPT LOCAL, .your.domain
```

Volitelné pole `shellcmd` může obsahovat příkaz rozhraní, jenž bude vykonán při splnění dané položky. To je užitečné při nastavování pastiček, které mohou odhalit potenciální útočníky:



```
in.ftpd: ALL EXCEPT LOCAL, .vbrew.com : \
echo "request from %d@%h" >> /var/log/finger.log; \
if [ %h != "vlager.vbrew.com" ]; then \
finger -l @%h >> /var/log/finger.log \
fi
```

Nástroj *tcpd* nahradí argumenty `%h` a `%d` skutečným názvem hostitele klienta, resp. skutečným názvem služby.

29.5 Konfigurace xinetd

Konfiguraci je přes *xinetd* je možné rozdělit do více souborů. Často konfigurační soubor `/etc/xinetd.conf` obsahuje jen základní nastavení a odkaz na adresář, kde se nacházejí konfigurační soubory jednotlivých služeb (např. v `/etc/xinetd.d`). Syntaxe je následující:

```
jméno_služby
{
    jméno_atributu operátor hodnota
    ...
}
```

Povinné atributy:

- **socket_type**: nejčastěji se používá `stream` (služby využívající spolehlivá spojení - protokol TCP), `dgram` (služby používající datagramy - protokol UDP),

- **user:** uživatel, pod kterým služba poběží (nezadává se v případě interní služby),
- **server:** dává cestu k serveru dané služby (v případě interní služby nebo redirekce se neudává),
- **wait:** tento atribut má v případě služby používající protokol TCP vždy hodnotu "no"; v případě služby používající protokol UDP záleží na tom, zda server uvolní socket a komunikuje s klientem přes nové spojení - v tomto případě může současně běžet více instancí serveru a zadáme "no"; v opačném případě server čte datagramy tak dlouho, dokud přicházejí a po uplynutí určité doby od přijetí posledního datagramu spojení (timeoutu) se ukončí - v tomto případě použijeme volbu "yes" (takto fungují např. talkd, démon služby talk anebo bootpd, démon služby bootps),
- **protocol:** tento atribut uvádíme pouze u služeb, které nejsou evidovány v /etc/services a u služeb RPC (Remote Procedure Call),
- **atributy rpc_version, rpc_number a port** se týkají RPC služeb.

29.6 Kontrola přístupu ke službám

Oproti staršímu *inetd* nabízí *xinetd* řadu možností jak řídit přístup ke službám:

- Omezení přístupu na základě IP adres / jmen počítačů.
- Řízení přístupu pomocí *tcp_wrappers*.
- Přístup ke službám v závislosti na čase.
- Služby vázané na vybrané síťové rozhraní.

Omezení přístupu na základě IP adres / jmen počítačů

Provádí se přímo v konfiguraci *xinetd*. První možností je použít direktivy *only_from* s výčtem IP adres, sítí či jmen počítačů pro povolení přístupu nebo *no_access* pro povolení přístupu všemi mimo vybraných strojů.

Řízení přístupu pomocí *tcp_wrappers*

Je založeno na využití *tcp_wrappers* - tedy je podmínkou aby *xinetd* byl sestaven s podporou *tcp_wrappers*. V Linuxových distribucích se *tcp_wrappers* běžně používají. Konfigurace je uložena v souborech */etc/hosts.deny* a */etc/hosts.allow*.

Přístup ke službám v závislosti na čase

Příjemnou možností *xinetd* je omezit přístup k síťovým službám na určité časové rozmezí, k tomu slouží atribut *access_times*:

```
access_times = 5:00-7:00 15:00-24:00
```

Služby vázané na vybrané síťové rozhraní

Pokud máme v systému více síťových rozhraní, můžeme specifikovat na kterém rozhraní daná služba poběží pomocí atributu *bind* (nebo *interface*, obojí znamená totéž):

```
# služba bude dostupná pouze na lokálním rozhraní
bind                                = 127.0.0.1
```

29.7 Soubory services a protocols

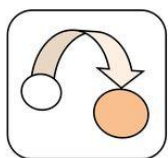
Název služby ve výše uvedených souborech musí být převeden na číslo portu pomocí vyhledání názvu služby v souboru */etc/services*. Číslo portů, na kterých jsou nabízeny „standardní“ služby, jsou definována v RFC Assigned Numbers.

Aby mohly servery nebo klienti převádět názvy služeb na tato čísla, musí být alespoň část z tohoto seznamu uložena na každém hostiteli; ukládá se v souboru */etc/services*. Položky v souboru mají následující syntaxi:

služba port/protokol [aliasy]

Pole *služba* definuje název služby, *port* definuje port, na kterém je služba nabízena, a pole *protokol* definuje typ používaného transportního protokolu. Tento údaj je obecně buď *tcp* nebo *udp*. (Stejnou službu je možné nabízet oběma protokoly, naopak lze na stejném portu různých protokolů nabízet různé služby). Pole *aliasy* umožňuje zadat alternativní názvy stejné služby.

Příklad souboru */etc/services*

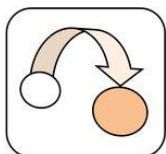


```
# Soubor služeb:
#
# známé služby
echo 7/tcp # Echo
echo 7/udp #
discard 9/tcp sink null # Discard
discard 9/udp sink null #
daytime 13/tcp # Daytime
daytime 13/udp #
chargen 19/tcp ttytst source # Character Generator
chargen 19/udp ttytst source #
ftp-data 20/tcp # File Transfer Protocol (Data)
ftp 21/tcp # File Transfer Protocol (Control)
```

```
telnet 23/tcp # Virtual Terminal Protocol
smtp 25/tcp # Simple Mail Transfer Protocol
nntp 119/tcp readnews
```

Podobně jako soubor se službami potřebuje i síťová knihovna nějaký způsob, jakým by mohla přeložit názvy protokolů - například těch protokolů, které jsou použity v souboru `services` - na čísla protokolů, kterým by rozuměly IP-vrstvy ostatních hostitelů. To se provede vyhledáním daného názvu v souboru `/etc/protocols`.

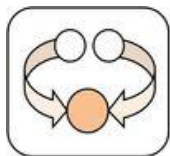
Ten obsahuje na každé řádce jednu položku. Každá položka obsahuje název protokolu a číslo sdružené s daným protokolem. Provádění změn v tomto souboru je ještě méně pravděpodobné, než zasahování do souboru `/etc/services`.



Soubor protocols:

```
#
# Internetové (IP) protokoly
#
ip 0 IP # internet protocol
icmp 1 ICMP # internet control message protocol
igmp 2 IGMP # internet group multicast protocol
tcp 6 TCP # transmission control protocol
udp 17 UDP # user datagram protocol
raw 255 RAW # RAW IP interface
```

Shrnutí kapitoly



Služby lze v Linuxu jednoduše spouštět při startu systému pomocí *rc-skriptů*. Pro zastavení popř. restart služby lze využít i příkaz *kill*.

Běžící programy, které poskytují služby po síti, se označují jako *daemons* (démoni). Démon je proces, který otevře port konkrétní služby, a čeká na příchozí spojení.

Efektivní spouštění služeb umožňuje speciální síťový démon označovaný jako *superserver*. Tento démon otevírá sokety pro řadu síťových služeb a na všech poslouchá. Když se na některém z portů objeví příchozí spojení, superserver je přijme a spustí server pro konkrétní port, kterému pak předá soket k obsluze. Superserver pak pokračuje v poslouchání na portech.

Nejběžnější superserver se jmenuje *inetd* nebo *xinetd*, liší se výrazně jiným formátem konfiguračního souboru a dalšími možnostmi, zejména v řízení přístupu ke službám.

Superserver *inetd* kontroluje přístup ke službám pouze pomocí *tcp_wrappers*, *xinetd* pomocí dalších mechanismů:

- Omezení přístupu na základě IP adres / jmen počítačů
- Přístup ke službám v závislosti na čase
- Služby vázané na vybrané síťové rozhraní

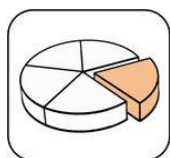
Pro spuštění služeb jsou nutné ještě další dva soubory: Soubory *services* a *protocols*.

Kontrolní otázky a úkoly



- 1) Jak se v Linuxu spouští, zastavují popř. restartují služby?
- 2) Co je to superserver a proč se používá?
- 3) Jaký dva superservery se používají v Linuxu, jaký je mezi nimi rozdíl?
- 4) Které konfigurační soubory a proč jsou pro spuštění služeb důležité?
- 5) Jaké jsou možnosti řízení přístupu ke službám?

Použitá literatura a jiné zdroje:



- [1] /KOLEKTIV AUTORŮ. Linux: Dokumentační projekt. Brno: Computer Press, a.s., 2008. ISBN 978-80-251-1525-1. Dostupné z: <http://www.root.cz/knihy/linux-dokumentacni-projekt-4-vydani/>

- [2] Linux documentation Project (CS) [online]. [cit. 2012-06-09]. Dostupné z: <http://www.nuc.elf.stuba.sk/lit/ldp/index.htm>
- [3] SHAH, Steve. Administrace systému Linux: jak porozumět svému počítači : podrobný průvodce začínajícího administrátora. 2. vyd. Praha: Grada, 2003, 533 s. ISBN 80-247-0641-5.

30 MS Windows: Správa počítače, služby

Obsah hodiny



Obsahem této hodiny je popis služeb v OS Windows a jejich správa.

Cíl hodiny



Po prostudování budete schopni:

- charakterizovat služby v OS Windows,
- popsat Role serveru,
- orientovat se v možnostech spuštění modulu snap-in Služby,
- orientovat se v možnostech konfigurace služeb.

Klíčová slova



Snap-in služby, Role serveru

30.1 Služby Windows Server

Služba je typ aplikace spuštěné na pozadí. Služba je podobná aplikaci typu démon systému Unix. Služby poskytují základní funkce operačního systému, jako je například provoz webových a souborových serverů, protokolování událostí, nápověda a odborná pomoc, tisk, kryptografie a zasílání zpráv o chybách. Služby lze spravovat prostřednictvím modulu snap-in. Služby OS dodávané se systémy řady Microsoft® Windows Server jsou navrženy tak, aby byly spuštěny pouze klíčové služby potřebné pro běžné role serverů.

Modul snap-in Služby umožňuje:

- spuštění, zastavení, pozastavení, pokračování nebo zakázání služby ve vzdáleném nebo v místním počítači,
- správu služeb v místních nebo vzdálených počítačích,
- nastavení zotavovacích postupů pro případ selhání služby, například automatické restartování služby nebo počítače,
- povolení nebo zakázání služeb v konkrétním hardwarovém profilu,
- export informací o službě do souborů formátů TXT a CSV pro účely správy systému,

- zobrazení stavu a popisu jednotlivých služeb.

Pro správu rolí serveru (serverové služby) je určený nástroj Správa serveru. Nástroj Správa se automaticky spustí při prvním přihlášení s pověřeními pro správu k počítači serveru.

Role serveru

- Role souborového serveru: souborové servery umožňují přístup k souborům a jeho správu.
- Role tiskového serveru: tiskové servery umožňují přístup k tiskárnám a jeho správu.
- Role aplikačního serveru: aplikační server představuje základní technologii, která poskytuje klíčové služby a infrastrukturu pro aplikace umístěné v systému.
- Role e-mailového serveru: služby e-mailového serveru: ukládání a spravování e-mailové účtů, přístup uživatelů k e-mailovému serveru a načítání e-mailů z místního počítače pomocí e-mailového klienta, který podporuje protokol POP3.
- Role terminálového serveru: uživatelé mohou ze vzdáleného umístění spouštět programy, ukládat soubory a používat síťové prostředky stejným způsobem, jako by tyto prostředky byly nainstalovány v jejich vlastních počítačích.
- Role serveru vzdáleného přístupu a virtuální privátní sítě: Služba Směrování a vzdálený přístup.
- Role řadiče domény: řadiče domén ukládají data adresáře a spravují komunikaci mezi uživateli a doménami, včetně procesů přihlášení uživatele, ověřování a vyhledávání v adresáři.
- Role serveru DNS: Služba DNS (Domain Name System) se používá v Internetu k překladu adres IP na doménové jméno a opačně.
- Role serveru DHCP: centrální správa IP adres a jejich dynamické přidělování klientům.
- Role serveru multimediálních datových proudů: servery multimediálních datových proudů poskytují organizaci službu Windows Media. Umožňuje např. vysílat datovými proudy podnikovou komunikaci v intranetu - schůzky, projevy a školení, vysílat externí podnikovou komunikaci zákazníkům, dodavatelům a obchodním partnerům přes Internet.
- Role serveru WINS (Windows Internet Name Service) mapují adresy IP na názvy počítačů pro rozhraní NetBIOS a naopak.

30.2 Služby systému Windows 7

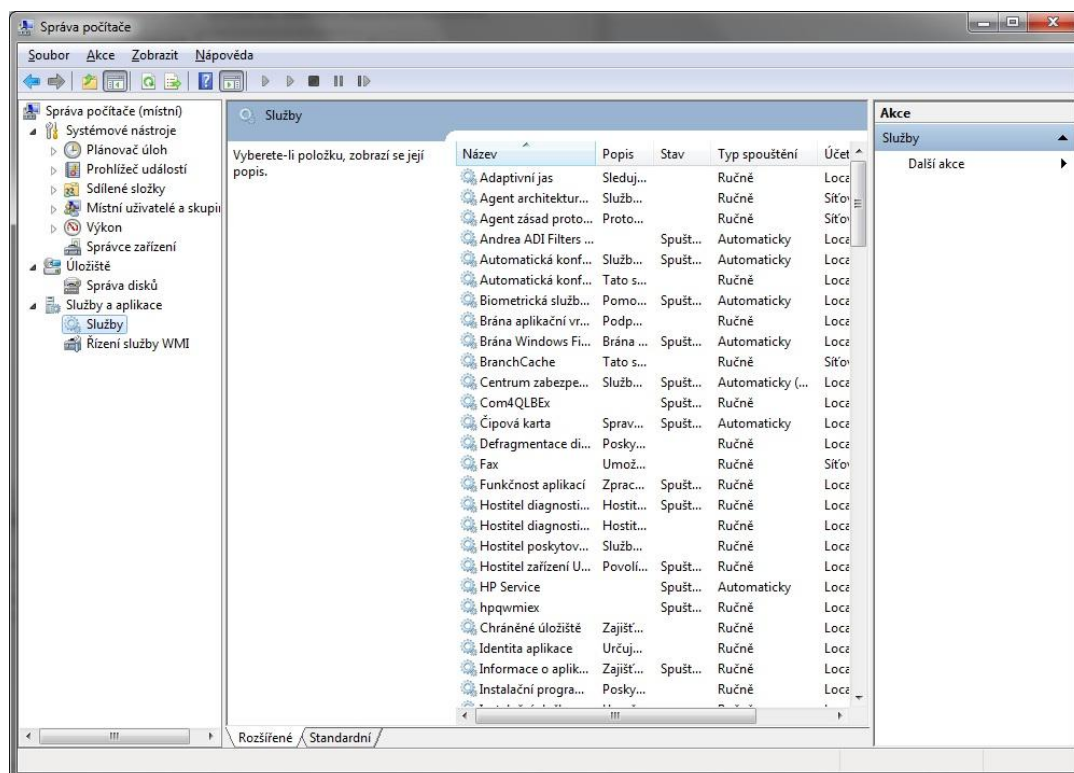
OS se skládá z mnoha jednotlivých částí. Jednou z nich jsou i služby, které zajišťují běh aplikací a procesů. Služby systému Windows 7 představují jednotlivé komponenty, které zajišťují a jsou nutné pro jeho bezproblémové fungování. Většina služeb je spouštěna automaticky ihned po startu systému nebo přihlášení uživatele. Některé jsou nezbytné jiné lze naopak vypnout. Tím se OS zrychlí. Důvodem, proč se všechny spouští automaticky je snaha o univerzální nastavení systému pro široké spektrum uživatelů.

Správa služeb (snap-in *Služby*) je umístěna ve *Správě počítače*. Okno pro správu počítače je ve Windows 7 umístěno v nabídce *Start* v kontextovém menu *Počítač/Spravovat*. Pro tuto operaci je nutné mít oprávnění administrátora. Následuje otevření okna *Správa počítače* se stromem kategorií.

V kategorii *Systémové nástroje* jsou zde k dispozici:

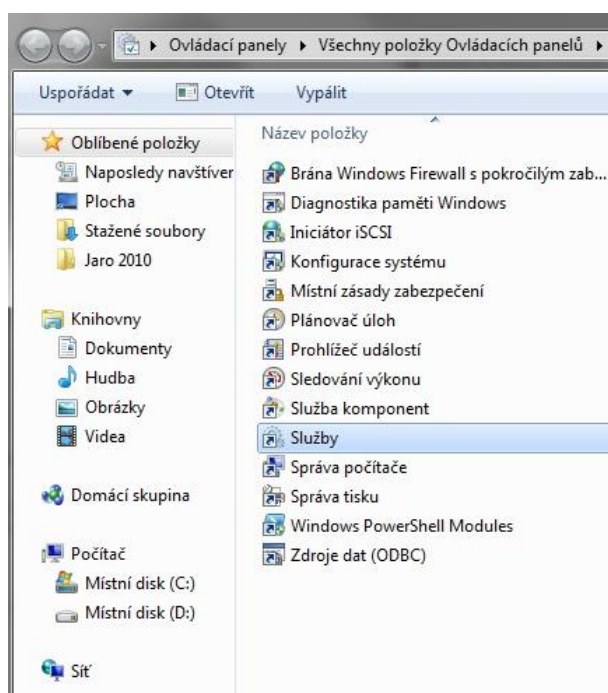
- Plánovač úloh,
- Prohlížeč událostí,
- Sdílené složky,
- Místní uživatelé skupiny,
- Výkon,
- Správce zařízení.

V kategorii *Úložiště* je *Správa disků* a v kategorii *Služby a Aplikace* je seznam nainstalovaných služeb a aplikací, jejich vlastností. Pravým tlačítkem je možno měnit vlastnosti vybraných služeb, nastavovat typ spouštění, služby povolovat a zakazovat apod.



Obrázek 30-1: Správa počítače - služby

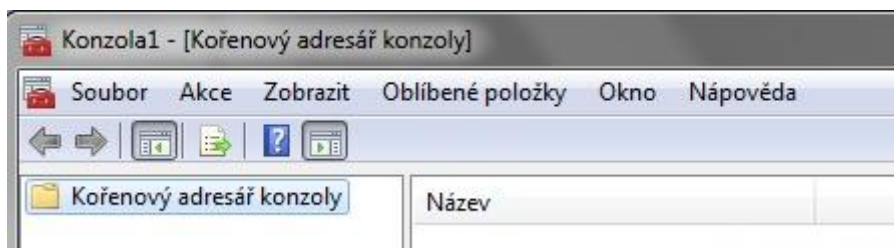
Další možností spuštění snap-in *Služby* je přes *Ovládací panely /Nástroje pro správu/Služby*. Odtud lze snap-in *Služby* spustit bez oprávnění správce, ale pouze pro čtení. Pro změnu jakéhokoliv nastavení je nutné klepnout na položku *Služby* pravým tlačítkem myši a zvolit možnost *Spustit jako správce*.



Obrázek 30-2: Otevření snap-slужby přes Ovládací panely

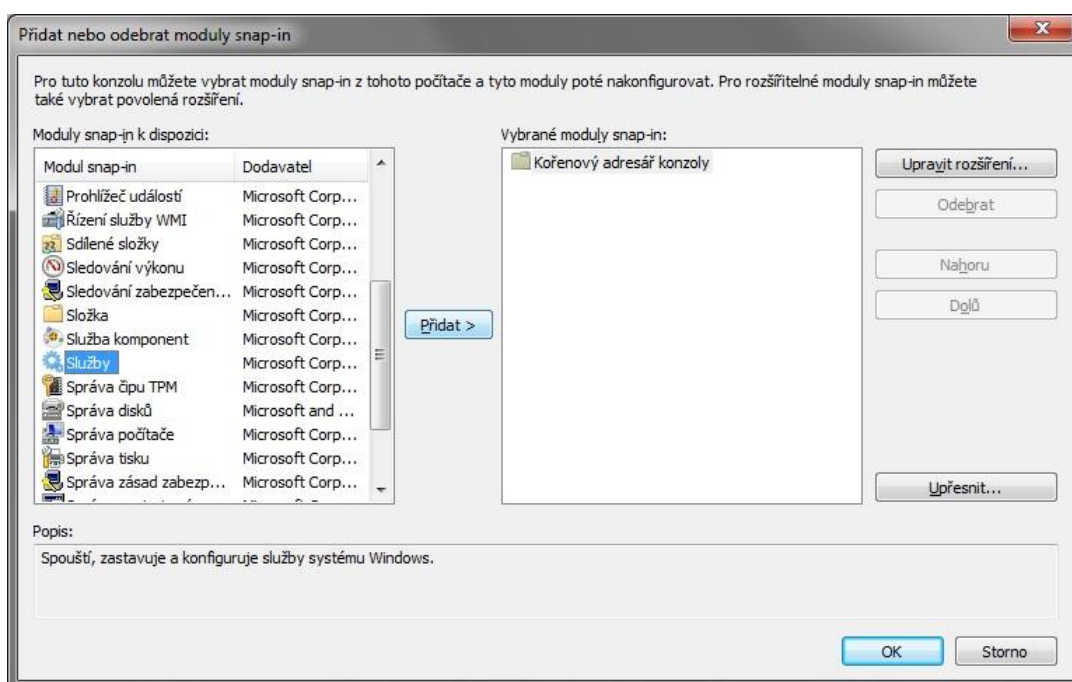
Nejrychleji lze spustit Modul snap-in služby přes Start/ pole “Prohledat programy a soubory”/ services.msc/enter.

Jiná možnost je vytvoření vlastní *Management Console*. Start/Prohledat programy a soubory, napsat mmc, potvrdit.



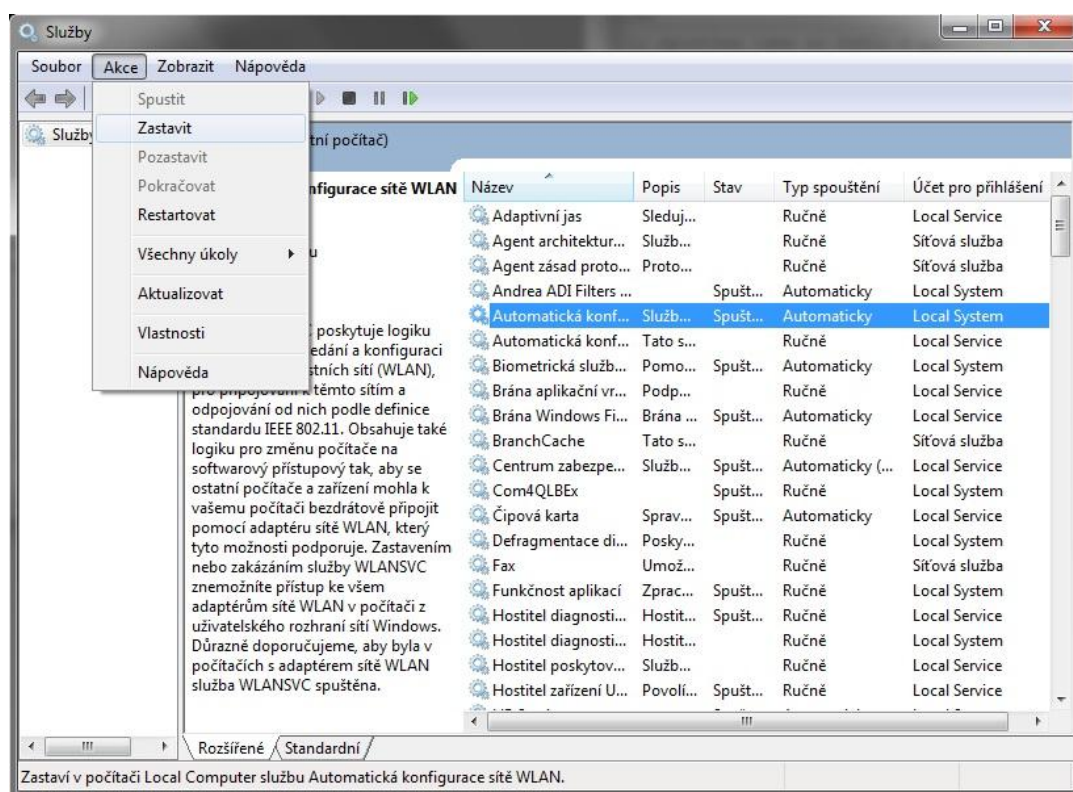
Obrázek 30-3: Okno Management Console

Otevře se okno *Microsoft Management Console*. V menu nahoře je třeba vybrat *Soubor/Přidat* nebo *Odebrat modul snap-in*, otevře se okno, které umožňuje přidat nebo odebrat všechny konzole pro správu, včetně snap-in modulu *Služby*. Vlevo jsou všechny konzole/snap-in moduly pro správu systému, vpravo seznam přidanych.



Obrázek 30-4: Vytvoření vlastní konzoly pro správu

30.3 Spuštění a zastavení služby



Obrázek 30-5: Snap-in Služby: Akce

Služby, které nemají uveden žádný stav je možno spustit. Služby, které mají stav "*Spuštěno*" lze zastavit případně pouze pozastavit, pozastavenou službu opětovně spustit (volbou pokračovat). Poslední volbou je možnost restartovat. Ta se využívá v případech, kdy dojde ke změně konfigurace systému, případně se služba nechová dle očekávání, a je potřeba ji zastavit a znovu spustit. Po restartu se služba nejprve zastaví a pak restartuje.

Ve vlastnostech služby se nastavují *Typy spouštění služby*:

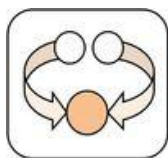
- Automaticky - služba se spustí během procesu spuštění a přihlášení,
- Automaticky (zpožděné spuštění) - umožňuje mírně zpoždit spuštění služby a urychlit tak start systému a přihlášení uživatele,
- Ručně - službu si operační systém spustí až v momentě, kdy ji bude opravdu potřebovat - nezabírá tedy žádnou paměť,
- Zakázáno - služba se nespustí za žádných okolností.

30.4 Služby v OS Windows a příkazový řádek

Pro správu služeb v příkazovém řádku je k dispozici příkaz `sc`, který podporuje celou řadu doplňujících parametrů a voleb, umožňujících ke službám opravdu detailní přístup. Nejjednodušší použití tohoto příkazu je společně s parametrem *query*: výpis právě běžících služeb společně s přidruženými podrobnostmi:

- název služby,
- zobrazovaný název,
- typ,
- stav,
- ukončovací kód WIN32,
- ukončovací kód služby,
- kontrolní bod,
- nápověda při čekání.

Shrnutí kapitoly



Služba je typ aplikace spuštěné na pozadí. Služba je podobná aplikaci typu démon systému Unix. Služby poskytují základní funkce operačního systému, jako je například provoz webových a souborových serverů, protokolování událostí, nápověda a odborná pomoc, tisk, kryptografie a zasílání zpráv o chybách. Jaké serverové služby se spustí určují role serveru.

Služby lze spravovat prostřednictvím modulu snap-in. Pro správu rolí serveru (serverové služby) je určený nástroj Správa serveru. Nástroj Správa se automaticky spustí při prvním přihlášení s pověřeními pro správu k počítači serveru.

Služby OS dodávané se systémy řady Microsoft® Windows Server jsou navrženy tak, aby byly spuštěny pouze klíčové služby potřebné pro běžné role serverů.

Služby systému Windows 7 představují jednotlivé komponenty, které zajišťují a jsou nutné pro jeho bezproblémové fungování. Většina služeb je spouštěna automaticky ihned po startu systému nebo přihlášení uživatele.

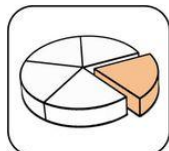
Správa služeb (snap-in Služby) je ve Windows 7 umístěna ve Správě počítače. Ze ji spustit různými způsoby nejrychleji příkazem `services.msc`. Pro správu služeb v příkazovém řádku je k dispozici příkaz `sc`.

Kontrolní otázky a úkoly



- 1) Jaké role má OS Microsoft Server?
- 2) Jaký je rozdíl mezi službami v OS Windows 7 a OS Microsoft Server?
- 3) Jaké jsou možnosti spuštění modulu snap-in Služby?
- 4) Jak lze konfigurovat služby?

Použitá literatura a jiné zdroje:



- [1] MASARYKOVA UNIVERZITA - ÚSTAV VÝPOČETNÍ TECHNIKY. Windows 7 Tutoriál [online]. 2010 [cit. 2012-06-09]. Dostupné z: <http://kurzy.ucn.muni.cz/Win7/>
- [2] Modul snap-in Služby [online]. © 2012 [cit. 2012-06-09]. Dostupné z: [http://technet.microsoft.com/cs-cz/library/cc757797\(v=ws.10\)](http://technet.microsoft.com/cs-cz/library/cc757797(v=ws.10))
- [3] Role serveru [online]. © 2012 [cit. 2012-06-09]. Dostupné z: [http://technet.microsoft.com/cs-cz/library/cc756962\(v=ws.10\)](http://technet.microsoft.com/cs-cz/library/cc756962(v=ws.10))
- [4] BITTO, Ondřej. Jak na počítač profi: Služby Windows podrobně. [online]. 2011 [cit. 2012-06-09]. Dostupné z: <http://jnp.zive.cz/jak-na-pocitac-profi-sluzby-windows-podrobne>

31 Adresářové služby, LDAP

Obsah hodiny



Obsahem této hodiny je popis adresářových služeb LDAP.

Cíl hodiny



Po prostudování budete schopni:

- charakterizovat adresářové služby a protokol LDAP,
- popsat službu LDAP pomocí jejích čtyř modulů.

Klíčová slova



LDAP, Adresářová služba, Informační model, Jmenný model, Funkční model, Bezpečnostní model

31.1 Adresářová služba

V síťovém prostředí je velmi důležité uchovávat důležité informace na dostupném místě a v uspořádané podobě. To lze zajistit službou, která, poskytuje informace ve strukturované a přehledné formě s možností snadného vyhledávání.

Adresářové služby jsou aplikace, které ukládají, organizují a centrálně spravují informace o uživatelích a zdrojích v počítačové síti a zpřístupňují je administrátorům, uživatelům, aplikacím apod. Jednotlivé aplikace si tedy nemusí udržovat vlastní databázi, ale stačí jedna centrální pro všechny.

Adresářové služby fungují také jako centrální autentizační autorita. Umožňují bezpečnou autentizaci zdrojů (uživatelů, služeb, počítačů) a to, že lze k různým aplikacím přistupovat pod stejnými uživatelskými údaji.

Příkladem implementace adresářových služeb jsou :

- *e-Directory* – služba v OS Novell NetWare (dříve NDS),
- *Active Directory* – služba ve Windows, od verze Windows 2000 Server.

Data se ukládají do adresáře, což je specializovaná databáze s hierarchickou strukturou, optimalizovaná pro rychlé, efektivní čtení a vyhledávání. Adresáře obsahují položky – objekty. Každý objekt je popsán řadou vlastností – atributů. Například objekt uživatel má vlastnosti jako jméno, příjmení, přihlašovací jméno, heslo, e-mailovou adresu, telefonní číslo apod.

Proč je databáze optimalizovaná pro čtení a vyhledávání? Je to proto, že data, o které se adresářová služba stará, se příliš často neměnní, ale musí být velmi rychle dohledatelná. Operace čtení jsou tedy častější než operace zápisu (na 1000 čtení připadá jeden zápis). Adresářové služby dovolují uživatelům a aplikacím hledat objekty (lidi, zdroje) dle specifikovaných podmínek a poskytovat informace o těchto objektech.

Porovnání adresářové a relační databáze:

- Adresáře poskytují rychlou odezvu při čtení informací, relační databáze jsou výkonnější při častých aktualizacích.
- Adresáře nepodporují komplikované transakce ani náročné dotazy jako je spojování tabulek, jako je obvyklé u relačních databází.
- Adresáře mají lepší podporu vyhledávání podřetězců.
- Adresáře umožňují replikovat informace na více strojů pro zvládnutí větší zátěže, zvýšení spolehlivosti a zkrácení doby odezvy.
- Adresáře většinou používají předdefinovaná schémata a není tedy nutné schéma definovat, jako v případě relačních databází.

Z hlediska rozsahu platnosti informací mohou být adresářové služby lokální nebo globální. Globální služby jsou obvykle distribuované, což znamená, že data, která obsahují, jsou rozložena na mnoha strojích, které spolupracují při poskytování adresářové služby.

31.2 LDAP: Protokol pro adresářové služby

LDAP, Lightweight Directory Access Protocol, je protokol, určený ke správě a uchovávání informací v adresářové struktuře. Je to aplikační protokol pro dotazování a modifikaci adresářových služeb nad TCP/IP. Vznikl jako zjednodušení standardu X.500.

V 80tých letech vznikla skupina standardů X.500 pro adresářové služby. Tyto standardy specifikují adresářové datové struktury a operace nad nimi. Jsou postaveny na principu klient - server (komunikace klienta s adresářovým serverem - *Directory Access Protocol DAP*). LDAP byl navržen jako zjednodušená forma DAP (*Directory Access Protocol*) přizpůsobená protokolům TCP/IP a časem se osamostatnil.

Dnes je LDAP samostatným řešením pracujícím bez podpory X.500 a nabízí víc, než X500 zejména v oblasti bezpečnosti. Protokol LDAP má vlastní standardní API a standardní datové formáty.

Protokoly:

- DAP: *Directory Access Protocol* - komunikace mezi klientem a serverem,
- DSP: *Directory System Protocol* – komunikace mezi servery, pro zprostředkované vyhledávání informace,
- DISP: *Directory Information Shadowing Protocol* – pro replikaci, databáze mezi servery z důvodu rozložení zátěže mezi více serverů.

LDAP je popsán pomocí čtyř modelů

- *informační model* – *schéma databáze* - popisuje strukturu informací (atributy) v adresáři,
- *jmenný model* - popisuje, jak jsou informace organizovány a odkazovány,
- *funkční model* – popisuje operace nad informacemi,
- *bezpečnostní model* - jak jsou informace chráněny, řízení přístupu.

31.3 Informační model

- Datové entity: položka, atribut.
- Položka - záznam
 - má typ položky (třída objektu),
 - obsahuje atributy,
 - má jméno, DN (rozlišovací jméno) globální v rámci DIT,
 - uspořádání do Directory Information Tree (DIT).
- Atribut
 - má typ,
 - má hodnotu, resp. hodnoty,
 - má jméno - identifikaci v rámci položky.
- Schéma

Informační model tvoří záznamy, položky obsahující souhrn atributů, s informacemi o nějakém objektu (něčem konkrétním), jako je např. uživatel nebo počítač. Každý záznam je instancí objektové třídy, musí obsahovat všechny atributy definované pro objektovou třídu (povinné a nepovinné).

Implementace informačního modelu se označuje jako **schéma**. Schéma definuje všechny možné třídy objektů a jejich atributy. Výchozí schémata pro určitý adresář je možno rozšiřovat. Ve schématu jsou dva typy objektů, schema classes (určuje možné objekty, je souhrnem atributů) a schema

attributes (jednotlivé atributy pro objekt). Dohromady se tyto objekty nazývají metadata.

Objekt lze definovat jako pojmenovanou skupinu atributů, které reprezentují síťový prostředek (resource). Některé objekty mohou obsahovat jiné objekty, to jsou kontejnery (container).

Třídy objektů (object classes) jsou kategorie objektů, které mohou být vytvořeny v adresáři. V LDAP se používá označení **objectClass** a může se jednat například o *User*, *Computer*, *OrganizationalUnit*.

Atributy objektů (object attributes) jsou charakteristiky (vlastnosti) objektů. Atribut může obsahovat jednu nebo více hodnot, například jméno, příjmení, e-mail. Určité atributy patří k určité třídě objektů a schéma také definuje, které hodnoty musí být vyplněny a které jsou volitelné. Schéma také určuje, jaké typy hodnot může atribut nabývat, například textový řetězec, celé číslo.

Informace v adresáři jsou uloženy ve stromové struktuře, která se označuje jako **Directory Information Tree** (DIT). Kořenem adresářového stromu je **rootDSE**, obsahuje globální informace o adresáři a nemá žádné jméno ani třídu. Strom je tvořen uzly a listy. Uzly jsou položky/záznamy a informace uspořádané hierarchicky do skupin. Označují se jako **kontejner** (container object) a tvoří větve stromu. Kontejner v sobě může obsahovat jeden či více objektů (položek). Listy (leaf object) jsou vlastně koncové objekty – jednotlivé položky/ záznamy, které se dále nečlení (nemají žádné potomky).

31.4 Jmenný model

Úkolem jmenného modelu LDAP je definovat, jakým způsobem budou data v adresáři organizována a jak je možné se na ně odkazovat.

K záznamům v adresáři se přistupuje pomocí cesty – úplné DN a relativní RDN. Každý záznam v rámci stromu je jednoznačně identifikovatelný pomocí *Distinguished Name* (DN) – rozlišovacího jména.

Distinguished Name (DN, **rozlišovací jméno** je jednoznačný identifikátor objektu a obsahuje úplnou cestu k záznamu (pozici ve stromu, kontext). DN se skládá ze jména objektu a jmen jednotlivých kontejnerů, které obsahují objekt.

Relative Distinguished Name (RDN), **relativní rozlišovací jméno**, je jméno, které jednoznačně identifikuje objekt v dané větvi, kontejneru, ale ne v celém stromu. To znamená, že v jiné větvi (kontejneru) může být objekt se stejným RDN.

Typ atributu, který se používá k popisu RDN, se označuje jako **jmenný atribut**. Každá třída (*ObjectClass*) má přiřazen jmenný atribut, například *User* (uživatel, koncový objekt) má CN.

Alias	Jméno	Význam
CN	Common Name	"common name" koncový objekt
OU	Organization Unit	jméno organizační jednotky
O	Organization	jméno organizace
C	Country	jméno (zkratka) státu

Tabulka 4: Jmenné atributy

31.5 Funkční model

Funkční model LDAP definuje, co se může provádět s informacemi v adresáři. Jedná se o devět operací, které jsou zařazeny do tří kategorií:

- Dotazování a prohledávání - slouží pro získávání informací z adresářového stromu, operace *search* a *compare*.
- Změny dat – operace *add*, *delete*, *modify* (*modifyRDN*).
- Autentizace - navázání spojení a prokázání identity uživatele.
 - *bind* - navázání spojení mezi LDAP serverem a klientem. Při navázání spojení probíhá autentizace,
 - *unbind* - zrušení spojení mezi LDAP serverem a klientem,
 - *abandon* - klient požaduje zrušení nedokončené (předchozí) operace.

31.6 Bezpečnostní model

Poslední model LDAPu určuje, jak se přistupuje k datům z bezpečnostního hlediska. Zahrnuje

- *autentizaci uživatele*, tj. metodě prokázání identity (a tím vazbě uživatele na položku, která ho reprezentuje v adresářovém stromu),
- *bezpečnost obecně* - zabezpečení proti odposlechu a napadení komunikace,
- *autorizace*- řízení přístupových práv k jednotlivým objektům a operacím nad nimi.

Shrnutí kapitoly



Adresářové služby jsou aplikace, které ukládají, organizují a centrálně spravují informace o uživatelích a zdrojích v počítačové síti a zpřístupňují je administrátorům, uživatelům, aplikacím apod.

Adresářové služby fungují také jako centrální autentizační autorita. Umožňují bezpečnou autentizaci zdrojů (uživatelů, služeb, počítačů) a to, že lze k různým aplikacím přistupovat pod stejnými uživatelskými údaji.

Příkladem takových to adresářových služeb jsou :

- e-Directory – služba v OS Novell NetWare (dříve NDS),
- Active Directory – služba ve Windows, od verze Windows 2000 Server.

LDAP služby mohou být lokální nebo globální. Globální služby jsou obvykle distribuované.

LDAP, Lightweight Directory Access Protocol, je protokol, určený ke správě a uchovávání informací v adresářové struktuře. Je to aplikační protokol pro dotazování a modifikaci adresářových služeb nad TCP/IP. Vznikl jako zjednodušení standardu X.500.

LDAP je popsán pomocí čtyř modelů

- informační model – schéma databáze - popisuje strukturu informací v adresáři: datové entity: položky, atributy, strom, schéma,
- jmenný model - popisuje, jak jsou informace organizovány a odkazovány (jmenné atributy, DN, RND),
- funkční model – popisuje tři kategorie operací nad informacemi: vyhledávání dat, Změny dat, Autentizace,
- bezpečnostní model - jak jsou informace chráněny, řízení přístupu: *autentizaci uživatele, autorizace, bezpečnost obecně.*

Kontrolní otázky a úkoly

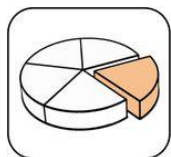


- 1) Charakterizujte to protokol LDAP.
- 2) Co je úkolem adresářové služby LDAP?
- 3) Jaké moduly popisují LDAP?
- 4) Co definuje informační model?
- 5) Co popisuje jmenný model?
- 6) Co popisuje funkční model?
- 7) Jaké operace lze provádět nad informacemi v LDAP?
- 8) Co řeší bezpečnostní model?

Otázky k zamyšlení



- 1) Jsou adresářové služby implementovány v Internetových aplikacích?



Použitá literatura a jiné zdroje:

- [1] SITERA, Jiří. Adresářové služby - úvod do problematiky: Technická zpráva TEN-155 CZ číslo 4/2000. Cesnet [online]. 1. vyd. 7. září 2000 [cit. 2012-03-03]. Dostupné z: <http://www.cesnet.cz/doc/techzpravy/2000-4/>
- [2] BOUŠKA, Petr. Adresářové služby a LDAP. Www.Samuraj-cz [online]. 14.09.2007 [cit. 2012-03-03]. Dostupné z: <http://www.samuraj-cz.com/clanek/adresarove-sluzby-a-ldap/>

32 MS Windows: Active Directory

Obsah hodiny



Obsahem této hodiny je popis adresářové služby Active Directory v OS Windows.

Cíl hodiny



Po prostudování budete schopni:

- orientovat se ve struktuře Active Directory,
- popsat funkci jednotlivých objektů.

Klíčová slova



Active Directory, Forest, Tree, Domain, Organizational Unit

32.1 Active Directory

Active Directory (dále AD) je implementace adresářových služeb LDAP firmou Microsoft pro použití v prostředí systému Microsoft Windows.

AD v sobě zahrnuje řadu služeb. Jeho primární role je poskytování centrálních služeb pro autentizaci a autorizaci, tedy správa uživatelů (přesněji správa účtů, protože to může být i počítač).

Různé části AD poskytují další funkce. Například Group Policy umožňuje spravovat politiky jednotlivých počítačů (co je na nich povoleno) a instalovat hromadně (a vzdáleně) aplikace.

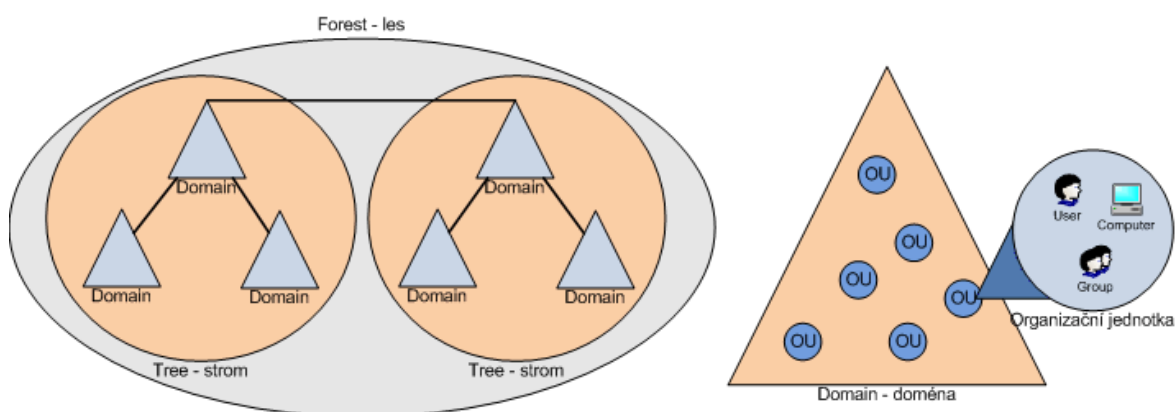
AD je silně provázáno s DNS, používá stejnou hierarchickou strukturu. Bez DNS nefunguje.

AD tvoří komponenty, které vytvářejí strukturu adresáře tak, aby odpovídala organizační struktuře organizace a splňovala její potřeby. Některé komponenty reprezentují logickou a jiné fyzickou strukturu.

32.2 Logická struktura

Logické seskupování zdrojů, logická struktura AD, umožňuje přistupovat k objektům nezávisle na jejich fyzickém umístění. Logickou strukturu AD tvoří objekty

- Forest – les,
- Tree – strom,
- Domain – doména,
- Organizational Unit – organizační jednotka



Obrázek 32-1: Logická struktura AD

Na vrcholu struktury je les - Forest. Ten může obsahovat jeden nebo více stromů - Trees. Strom je tvořen jednou či více doménami - domains. Uvnitř domén jsou jednotlivé organizační jednotky - OU (Organizational Unit). Uvnitř OU se nachází jednotlivé objekty (počítače, uživatelé, tiskárny, apod.).

Doména

Doména (domain) je základním prvkem logické struktury AD. Má jednoznačné označení, vlastní zásady zabezpečení. Vytváří vztahy důvěry s ostatními doménami.

V doméně jsou přímo uloženy OU a koncové objekty. AD je tvořena alespoň jednou nebo více doménami. Doména není spojena s fyzickým umístěním jednotlivých objektů, může obsahovat objekty např. z různých poboček. Doména je jakousi bezpečnostní hranicí, přístup k doménovým objektům je řízen pomocí ACL. Bezpečnostní nastavení a oprávnění nemohou přecházet mezi doménami.

Většinou se vytváří logická struktura s jednou doménou. Na úrovni domény se řeší, například politika na hesla (aplikuje se na celou doménu).

Při vytvoření domény se určuje úroveň funkčnost. Úroveň funkčnosti doménové struktury lze pouze zvýšit, nelze ji snížit. (např. při upgrade serveru, pozor zvýšení platí pro všechny domény).

Organizační jednotka (OU)

OU (Organizational Unit) je uzlový objekt, kontejner, který se uvnitř domény používá k seskupování objektů do logických administračních skupin. Nejčastěji obsahuje:

- uživatelské účty,
- sdílené prostředky,
- další OU.

Většinou odpovídá organizační struktuře ve firmě (divizí a oddělení). OU je jednotka, na kterou lze delegovat administrační oprávnění. OU může obsahovat (dělit se) další OU a vytvářet libovolnou hierarchickou strukturu. Hierarchie OU je lokální uvnitř domény a neovlivňuje jiné domény.

Na úrovni OU se řeší správu uživatelů a počítačů, skupinová politika.

OU umožňují přiřadit zásady skupiny pro malý počet objektů domény, aniž by ovlivňovaly zbytek domény. To umožňuje spravovat odděleně jednotlivé části organizace podle její hierarchie.

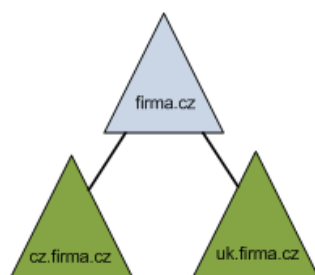
OU vytvářejí menší pohledy na adresářové objekty domény a je tak možné s nimi lépe pracovat. To umožňuje efektivní správu prostředků.

OU umožňují delegovat řízení a jednoduše řídit přístup ke správě doménových prostředků. Lze tak stanovit rozsah práv jednotlivých správců v doméně. Pro jednotlivou OU lze stanovit samostatného správce. Na druhou stranu lze jednomu správci delegovat oprávnění na správu všech OU v doméně.

OU dovoluje seskupovat různé typy objektů, na něž pak mohou být aplikována pravidla nastavená pro OU.

Strom

Strom je seskupení nebo hierarchická organizace jedné nebo více domén. Jedná se o hierarchické spojení domén vytvořené vztahem rodič-potomek.



Obrázek 32-2: Tree - strom

Strom tvoří rodičovská doména (parent domain), k ní jsou připojeny podřízené domény (child domain). Doména na vrcholu stromu se nazývá kořenová doména (Root Domain).

Domény ve stromě sdílí souvislý jmenný prostor (namespace), schéma a hierarchické spojení doménových jmen. Používá se DNS standard, takže doménové jméno potomka (child domain) vznikne použitím jeho relativního jména doplněné za tečkou jménem jeho rodičovské domény.

Existence více stromů není běžná. Více stromů je zapotřebí pouze pro provozování různých, oddělených jmenných prostorů (namespace). To může nastat například při akvizici nějaké jiné firmy: lze sdílet oprávnění a zároveň zachovat vlastní názvy.

Les - Forest

Les je volné seskupení jednoho nebo více nezávislých stromů. Všechny domény v lese sdílí stejné schéma, globální katalog a jsou propojeny implicitním dvoucestným vztahem důvěry (trust). Stromy v lese mají vlastní pojmenování - DNS jméno (oddělený jmenný prostor podle domén). Domény v lese pracují nezávisle, ale díky lesu je umožněna vzájemná komunikace přes celou organizaci (autorizace).

Více lesů (forest) je potřeba jen výjimečně, ve speciálních případech. Je to tehdy, když potřebujeme absolutní oddělení z pohledu oprávnění a autonomie (izolace). Například máme provozní prostředí a testovací, které spolu nesmí mít žádný vztah.

32.3 Fyzická struktura

Fyzickou strukturu Active Directory tvoří

- Site (podsítě),
- Domains Controllers (DC) - Doménové řadiče (servery).

Site

Site je kombinace jednoho nebo více IP subnetů (podsítí, je určena rozsahem adres), které jsou spojeny spolehlivými a rychlými linkami. Site obsahuje doménové řadiče. Pokud je ve firmě více lokálních sítí (lokalit, poboček) spojených pomocí WAN, tak se většinou vytváří site pro každou LAN. Když se podíváme na logickou strukturu AD, tak se zde site nikde nezobrazují.

Doménový řadič

Doménový řadič - Domain Controller – DC je vlastně server v site s OS Windows Server 2008 (nebo 2003), na kterém se nachází část nebo celá

AD (přesněji replika, lokální doménová databáze). V jedné doméně může být více doménových řadičů a každý obsahuje úplnou repliku adresáře pro danou doménu. Na jednom řadiči může být pouze jedna doména. Doménový řadič slouží k autentizaci uživatelů.

Pokud instalujeme první DC, tak ten se automaticky stává Root Domain.

Řadič domény plní zároveň roli globálního katalogu. Uchovává úplnou repliku všech objektů adresářové služby z vlastní domény a částečnou repliku všech ostatních domén lesa.

Globálním katalogem je standardně 1. nainstalovaný řadič domény.

32.4 Globální katalog GC

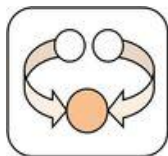
Globální katalog je centrální repository, obsahuje informace o objektech z celého stromu či lesa. Umožňuje nalézt informace z adresáře bez ohledu na to, v které doméně v lese se nachází. Jeho druhou funkcí je, že poskytuje informace o členství v univerzálních skupinách (universal group membership), které jsou potřeba při přihlašovacím procesu.

DC, který obsahuje kopii globálního katalogu, se nazývá Global Catalog Server. Globálních katalogů můžeme mít více a mezi nimi se provádí multimaster replikace. GC se často umísťují do různých site.

Pokud není k dispozici globální katalog při přihlašování, tak se uživatel může přihlásit pouze lokálně na počítač. Možností, jak tento problém obejít bez provozování GC, je zapnutí funkce universal group membership caching (UGMC) na danou site. V tomto případě si DC ukládá informace lokálně. Při prvním přihlášení uživatele se dotáže globálního katalogu a uloží vrácené hodnoty do keše, kde je uchovává a obnovuje. Při dalším přihlášení se použijí informace z této keše.

Obecně je dobré mít v každé pobočce GC, protože to urychluje přihlašování a nepřenáší se data pokaždé po WAN. Také v případě výpadku WAN linky zajistí GC, aby se uživatelé mohli přihlásit. Na druhou stranu se při replikaci přenáší větší objem dat a řada jich je (pro pobočku) zbytečná. Proto pro malé pobočky s pomalým připojením je vhodnější použít universal group membership caching.

Shrnutí kapitoly



Adresářová služba Active Directory je rozšiřitelná a škálovatelná adresářová služba. Umožňuje efektivně uspořádat, konfigurovat a spravovat síťové prostředky.

- je založena na standardních internetových protokolech,
- vyžaduje instalaci a správnou konfiguraci služby DNS,
- jednoznačně definuje logickou i fyzickou strukturu sítě,
- řešení pro správu počítačové sítě s počítači OS Windows.

AD má dvě úrovně – logickou a fyzickou.

Logická struktura AD, umožňuje sdružovat objekty přístupovat k nim nezávisle na jejich fyzickém umístění. Logickou strukturu AD tvoří objekty

- Forest – les,
- Tree – strom,
- Domain – doména,
- Organizational Unit – organizační jednotka

Fyzickou strukturu Active Directory tvoří

- Site (podsítě),
- Domains Controllers (DC) - Doménové řadiče (servery).

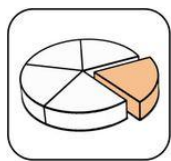
Na DC je umístěna AD nebo část AD. Při změně v AD se provádí automatická replikace, tak aby byl všude stejný stav AD.

Globální katalog je centrální repository, obsahuje informace o objektech z celého stromu či lesa. Umožňuje nalézt informace z adresáře bez ohledu na to, v které doméně v lese se nachází. GK a jeho kopie jsou umístovány na vybrané DC. Urychlují přístup uživatele, ale probíhá mezi nimi komunikačně náročná replikace (z důvodu změn v GK).

Kontrolní otázky a úkoly



- 1) Popište službu Active Directory.
- 2) Jaká je logická struktura Active Directory?
- 3) Jaká je fyzická struktura Active Directory?
- 4) Charakterizujete doménu a OU?
- 5) Jaká je funkce doménového řadiče?
- 6) Co je to Globální katalog?

Použitá literatura a jiné zdroje:

- [1] BOUŠKA, Petr. Active Directory komponenty - domain, tree, forest, site. Samuraj-cz [online]. 08.02.2008 [cit. 2012-06-16]. Dostupné z: <http://www.samuraj-cz.com/clanek/active-directory-komponenty-domain-tree-forest-site/>
- [2] Active Directory. In: Wikipedia: the free encyclopedia [online]. San Francisco (CA): Wikimedia Foundation, 12. 1. 2008, 27. 4. 2012 [cit. 2012-06-16]. Dostupné z: http://cs.wikipedia.org/wiki/Active_Directory

33 MS Windows: Politiky, zásady zabezpečení

Obsah hodiny



Obsahem této hodiny je Bezpečnostní politika OS MS Windows, vysvětlení Politiky hesel – Password Policy.

Cíl hodiny



Po prostudování budete schopni:

- vysvětlit pojem „Zásady zabezpečení“,
- charakterizovat Group Policy a orientovat se v jejích aplikaci,
- popsat Password Policy,
- definovat „Komplexnost hesla“.

Klíčová slova



Zásady zabezpečení, Group Policy, Password Policy

33.1 Zásady zabezpečení (politiky/ policy)

Zásady zabezpečení představují konfigurovatelnou sadu pravidel, která dodržuje operační systém, když zjišťuje, jaká oprávnění udělit v reakci na žádost o přístup k prostředkům.

Zásady zabezpečení nastavují bezpečnostní politiku systému, představují kombinaci nastavení zabezpečení, která ovlivňuje zabezpečení počítače. Označují se jako bezpečnostní politiky. Jedná se o nastavení platná pro všechny účty, o taktiku jak pracovat s účty. Právo politiky vidět a nastavovat má pouze skupina Administrators.

Nastavením zásad zabezpečení lze například řídit, kdo má přístup k počítači, jaké prostředky jsou uživatelé oprávněni používat v počítači a zda jsou akce uživatele nebo skupiny zaznamenávány do protokolu událostí.

Nastavení zásad zabezpečení je definováno na základě objektů zásad skupiny (Group policy), které lze nastavit na úrovni místního počítače nebo

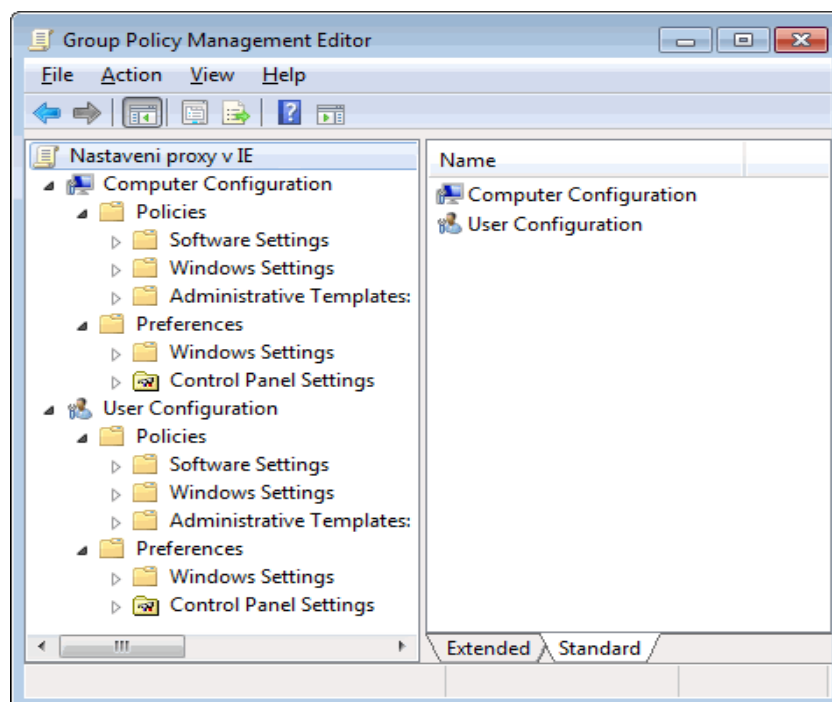
domény. Některá nastavení, jako nastavení zásad hesel, fungují pouze na úrovni domény. V rámci politik se definují:

- Zásady účtů:
 - Zásady hesla,
 - Zásady zamčení účtu,
- Zásady auditu,
- Přiřazení uživatelských práv,
- Možnosti zabezpečení (více než 70 možností zabezpečení).

33.2 Doménové politiky, Group Policy

Základem centrální správy počítačů v doméně jsou skupinové politiky (Group Policy). Řídí nastavení, bezpečnost a chování pracovních stanic a serverů, účtů. Standardně se při instalaci prvního DC vytvoří dvě GPO:

- Default Domain Policy GPO - připojena na kořen domény, hlavní nastavení pro doménu včetně politiky hesel,
- Default Domain Controller Policy GPO - připojena k OU Domain Controllers, úvodní bezpečnostní nastavení pro DC.



Obrázek 33-1: Editor Group Policy

Group Policy nejčastěji fungují na principu úprav registrů na klientské stanici či serveru. Skládají se ze dvou hlavních částí:

- konfigurace počítače (Computer Configuration),
- konfigurace uživatele (User Configuration).

Obě části mají rozdílné jednotlivé položky (možnosti nastavení), ale mají společné kategorie

- Software Settings,
- Windows Settings,
- Administrative Templates.

Část **Computer Configuration** se týká nastavení pro počítač, tato nastavení se mohou aplikovat na počítačové objekty v Active Directory (uplatňuje se na vybraný počítač a nezáleží na přihlášeném uživateli). Upravují větev registrů HKEY_LOCAL_MACHINE (HKLM).

Část **User Configuration** se týká nastavení pro uživatele, politiku s tímto nastavením lze aplikovat na uživatelské účty v Active Directory (na vybraného uživatele a nezáleží na jakém počítači). Když vytvoříme politiku hesel a připojíme ji na kontejner s počítači, tak se toto nastavení neuplatní pro doménové účty, ale pro lokální účty na daných počítačích. Upravuje větev registrů HKEY_CURRENT_USER (HKCU).

Group Policy se aplikují tak, že je spojíme s nějakým kontejnerem (link to). Při aplikaci politik se uplatňuje dědění (inheriting), dané hierarchickou strukturou AD, a souhrnný účinek (cumulative). To znamená, že se politika, aplikovaná na OU, projeví na všech počítačích a uživateli, kteří se nachází v této a ve vnořených OU. Když je více politik, tak se jejich účinek spojuje dohromady.

Politiky se zpracovávají postupně, později zpracovaná politika může přepsat nastavení předchozí. Postupuje se v pořadí lokální GPO, site, doména, OU, poslední je OU nejbližší k objektu.

Politiky aplikované na počítač se standardně uplatňují při startu počítače, politiky aplikované na uživatele probíhají při přihlášení uživatele. Obě se pak aplikují při periodické obnově Group Policy (to je standardně každých 90 minut + náhodný posun o až 30 minut). Aplikaci politik je možno vynutit ručně pomocí příkazu *gpupdate*.







33.3 Politika hesel (Password Policy)

V běžných nastaveních uživatelských účtů není možnost nastavit pravidla pro hesla jednotlivých uživatelů. Tato možnost se nachází až v pokročilých nástrojích pro správu, kterými jsou Místní zásady (politiky) zabezpečení.

Politika hesel (Password policy) určuje, jak mají být hesla silná a co se děje při zadání špatných hesel. Hesla lze definovat pro lokální účty a v doménovém prostředí také pro doménové účty.

Doménová politika hesel je standardně součástí Default Domain Policy. Definování a vynucení parametrů hesel se realizuje přes Group Policy:

- **Vynutit použití historie hesel** – nedovolí uživateli nastavit heslo, které již bylo použito.
- **Minimální, maximální doba platnosti hesla.**
- **Minimální délka hesla** – pomocí této možnosti lze nastavit délku nejkratšího dovoleného hesla, odstraní se tak problém příliš krátkých hesel, ty nejsou příliš bezpečná.
- **Komplexní heslo** - heslo musí splňovat požadavky na složitost, vynucuje použití silných hesel, nebudou tedy povolena příliš jednoduchá hesla (viz. dále).
- **Ukládat hesla pomocí šifrování** – bezpečnější skladování hesel, které útočníkovi nedovoluje získat jejich původní otevřenou podobu.

Policy	Security Setting
 Enforce password history	0 passwords remembered
 Maximum password age	0
 Minimum password age	0 days
 Minimum password length	10 characters
 Password must meet complexity requirements	Enabled
 Store passwords using reversible encryption	Disabled

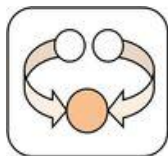
Obrázek 33-2: Password policy

Komplexní heslo znamená, že heslo nesmí obsahovat část uživatelského jména a musí obsahovat znaky minimálně ze tří skupin (ze čtyř možných), což jsou:

- velké písmeno (A-Z),
- malé písmeno (a-z),
- číslice (0-9),
- speciální (ne-alfanumerický) znak (třeba *#,.@%).

Politika zamykání účtů (Account Lockout Policy) určuje jestli, a po kolika chybně zadaných heslech, se účet zamkne, jestli se po zadané době automaticky odemkne a po jaké době se resetuje počítadlo chybných hesel.

Shrnutí kapitoly



Zásady zabezpečení představují kombinaci nastavení zabezpečení, která ovlivňuje zabezpečení počítače. Označují se jako bezpečnostní politiky. Jedná se o nastavení platná pro všechny účty, o taktiku jak pracovat s účty. Právo politiky vidět a nastavovat má pouze skupina Administrators.

Nastavením zásad zabezpečení lze například řídit, kdo má přístup k počítači, jaké prostředky jsou uživatelé oprávněni používat v počítači a zda jsou akce uživatele nebo skupiny zaznamenávány do protokolu událostí.

Nastavení zásad zabezpečení je definováno na základě objektů zásad skupiny (Group policy), které lze nastavit na úrovni místního počítače nebo domény. Některá nastavení, jako nastavení zásad hesel, fungují pouze na úrovni domény.

Politika hesel (Password policy) určuje, jak mají být hesla silná a co se děje při zadání špatných hesel.

Komplexní heslo je bezpečné heslo. Znamená, že heslo nesmí obsahovat část uživatelského jména a musí obsahovat znaky minimálně ze tří skupin ze čtyř možných.

Kontrolní otázky a úkoly

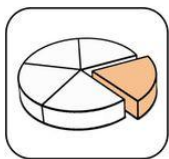


- 1) Co jsou to bezpečnostní politiky?
- 2) Jaké zásady se v rámci politik definují?
- 3) Charakterizujte Password Policy.
- 4) Co je to komplexnost hesla?

Otázky k zamyšlení



- 1) Lze najít v Linuxu ekvivalent pro bezpečnostní politiky OS MS Windows?

Použitá literatura a jiné zdroje:

- [1] Group Policy - Politiky hesel a zamykání účtů. In: Www.samuraj-cz.com [online]. 21.02.2011 [cit. 2012-05-12]. Dostupné z: <http://www.samuraj-cz.com/clanek/group-policy-politiky-hesel-a-zamykani-uctu/>
- [2] Group Policy - Politiky hesel a zamykání účtů. In: Www.samuraj-cz.com [online]. 21.02.2011 [cit. 2012-05-12]. Dostupné z: <http://www.samuraj-cz.com/clanek/group-policy-politiky-hesel-a-zamykani-uctu/>

34 OS Novell NetWare/NOES: eDirectory

Obsah hodiny



Obsahem této hodiny je popis LDAP služby eDirectory.

Cíl hodiny



Po prostudování budete schopni:

- charakterizovat vlastnosti eDirectory a možnosti nasazení,
- orientovat se ve správě a nástrojích správy eDirectory,
- popsat objekty tvořící eDirectory.

Klíčová slova



eDirectory, NOES, iManager

34.1 Od NDS k eDirectory

K nezbytným základním součástem síťových OS patří adresářové služby a správa identity. Zajišťují totiž v počítačových sítích správu uživatelů a síťových prostředků. Mezi produkty společnosti Novell zastává tuto roli Novell eDirectory. Jedná se adresářovou službu, která je mimo jiné multiplatformní, tzn. použitelná v různých OS.

Adresářová služba eDirectory i její předchůdce NDS (Novell Directory Services) jsou založeny na celosvětovém standardu X.500. Služba NDS se objevila poprvé v systému NetWare 4 (rok 1993), eDirectory v NetWare 5.1 (rok 2000) jako alternativa k NDS, přičemž v následujících systémech NetWare 6 a NOES (Novell Open Enterprise Server) již představuje jejich standardní systémový adresář.

34.2 Základní vlastnosti eDirectory

Služba eDirectory je databáze, která udržuje informace o součástech počítačové sítě (tzn. o uživatelích, serverech, tiskárnách, licencích, aplikacích, politikách apod.). Ty jsou pak přístupné OS na různých platformách, administračním nástrojům i kompatibilním aplikacím (např. GroupWise, ZENworks). Služba eDirectory významně zjednodušuje správu

sítě. Díky ní lze všechny prostředky sítě spravovat z jednoho místa a jednotnými nástroji. V současnosti je eDirectory k dispozici ve verzi 8.8.

Základní vlastnosti eDirectory:

- Objektovost, informace o součástech sítě jsou udržovány ve formě objektů a jejich vlastností.
- Otevřenost, schéma eDirectory (množina typů těchto objektů a jim příslušných vlastností) lze rozšiřovat a upravovat dle potřeby.
- Hierarchičnost, jednotlivé definované objekty jsou umísťovány do hierarchické struktury nazývané strom eDirectory, vhodné umístění usnadňuje uživatelům přístup k síťovým prostředkům.
- Globálnost, má také globální platnost, takže objekty, jež jsou v ní definovány, platí v prostředí celé sítě a nikoli jen na hostitelském serveru.
- Distribuovatelnost, lze ji distribuovat: Jednak je možné ji udržovat ve formě několika vzájemně synchronizovaných kopií na různých serverech a zvýšit tak její zabezpečení před haváriemi, jednak ji lze rozdělit na několik menších vzájemně souvisejících částí a snížit tím zatížení sítě od režijní komunikace (důležité především v sítích WAN).
- Multiplatformnost, je možné ji implementovat a používat i na jiných operačních platformách (SUSE Linux, Red Hat Linux, Solaris, AIX, HP-UX a Windows).

Multiplatformnost umožňuje realizovat jednotnou centrální správu i heterogenních sítí. Konkrétním příkladem je heterogenní síťová platforma Novell Open Enterprise Server (NOES), jejíž základnu tvoří systémy Novell NetWare 6.5 a SUSE LINUX Enterprise Server.

34.3 Instalace

Adresářovou službu eDirectory je možné získat jednak jako standardní součást systémů NetWare a NOES, jednak jako samostatný produkt, který lze instalovat i do prostředí Linux/Unix a Windows. Koncepce eDirectory, podstata její správy i poskytované služby jsou na všech platformách stejné, způsob instalace se však poněkud liší.

V případě systémů NetWare a NOES se eDirectory instaluje automaticky v průběhu jejich standardního generování. V rámci instalace se uvádějí základní parametry potřebné při vytváření eDirectory, např. zda se jedná se o generování prvního serveru v síti nebo již síť a její eDirectory existuje, dále se zadává jméno stromu eDirectory, umístění objektu reprezentujícího server ve stromu, jméno a heslo správce sítě, parametry pro synchronizaci času v síti apod.

V případě platformy Windows se v roli adresářových služeb používá standardně ActiveDirectory. Služba eDirectory se na servery Windows instaluje dodatečně z instalačního CD „Novell eDirectory“ nebo si lze pro účely testování stáhnout příslušný balíček z www.novell.com. Po spuštění instalace autorunem nebo přes setup.bat se zadávají obvyklé parametry.

Na platformě Linux se k instalaci používá utilita nds-install, kterou lze nalézt v adresáři Setup instalačního CD nebo testovací sady stažené z Internetu. Prostřednictvím zmíněné utility se instalují balíčky, jež náleží požadovaným součástem. Takto lze instalovat např. součásti eDirectory server, eDirectory administration utilities apod. V SUSE Linux lze pro účely zmiňované instalace použít v současnosti už i nástroj YaST.

Co se týče nároků na hardware serverů se na všech třech zmíněných operačních platformách se za typickou konfiguraci považuje v případě eDirectory spravující 100 000 objektů server s procesorem Pentium III 450 až 700 MHz, RAM 348 MB a volným prostorem na disku 144 MB. Pro 10 milionů objektů je to pak dvou až čtyřprocesorový server, který má Pentium III 450–700 MHz, RAM alespoň 2 GB a prostor na disku 15 GB.

34.4 Správa eDirectory

Činností, které lze v rámci správy eDirectory provádět, je celá řada, lze je rozdělit do následujících skupin:

- správa objektů eDirectory,
- správa oblastí a kopií eDirectory,
- údržba eDirectory a řešení problémů.

Do první zmíněné skupiny, tzn. správy objektů eDirectory patří činnosti, jako je vytváření a rušení objektů (např. uživatelů, kontejnerů), určování jejich umístění ve stromu, zadávání jejich vlastností, stanovení přístupových práv apod. Jedná se o běžné každodenní operace, jež se týkají informací uložených v eDirectory.

Skupinu správa oblastí a kopií eDirectory tvoří již závažnější činnosti, které se provádí jen občas a ovlivňují především strukturu eDirectory. Provádějí se zde operace s oblastmi eDirectory (tzn. jejich vytváření, přemísťování či rušení) i operace s kopiemi (vytváření, změna typu, rušení). Lze sem řadit také operace se servery (např. zařazení serveru do sítě), úpravy schéma apod.

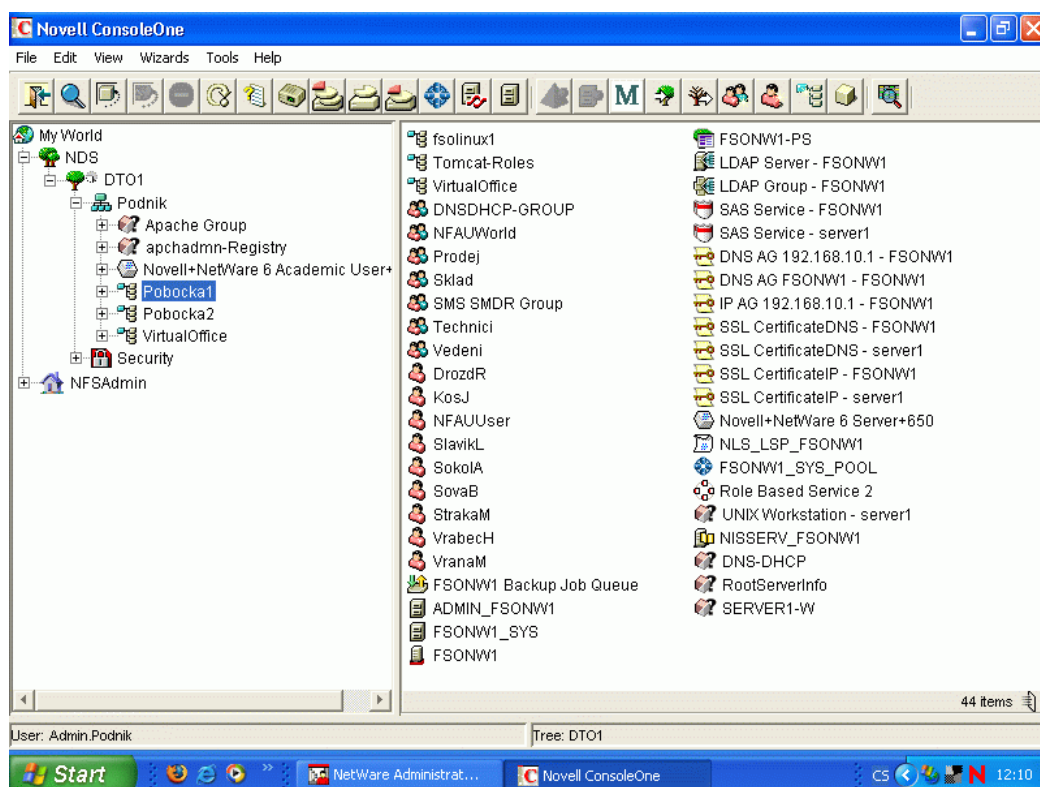
V poslední skupině, tzn. údržbě eDirectory a řešení problémů, pak jsou činnosti zaměřené na předcházení problémovým stavům eDirectory a jejich řešení v případech, na optimalizaci výkonnosti eDirectory, její udržování v korektním stavu, monitorování a zálohování. Při řešení problémů se pak

užívají operace, jako je oprava lokální databáze eDirectory, oprava či násilné zrušení kopií, násilné zrušení serveru v síti apod.

34.5 Nástroje pro správu

Pro realizaci činností souvisejících se správou eDirectory je k dispozici řada nástrojů. Nejvýznamnější místo mezi nimi zaujímá webová utilita iManager (Novell Identity Manager). Jejím prostřednictvím lze spravovat eDirectory umístěnou na libovolné operační platformě (NetWare, Linux/Unix, Windows), a to i na dálku (tzn. přes Internet), odkudkoli pomocí webového prohlížeče a komplexně (umožňuje provádět většinu operací týkajících se správy).

Mezi nástroje pro správu eDirectory na platformě NetWare patří např. klasická Windows utilita *NetWare Administrator* sloužící ke správě objektů. (na logickém disku SYS ve složce *PUBLIC/WIN32/NWADMN32*). Komplexnějším nástrojem je pak javová utilita *ConsoleOne*, která umí navíc i správu oblastí a kopií eDirectory. Pro účely zálohování se používá *Enhanced SBackup*, diagnostiku umožňuje *nlm-modul DSDiag*, k řešení problémových stavů slouží *DSRepair* atd. Nástroje obsažené v systému NetWare jsou k dispozici i v prostředí heterogenní síťové platformy NOES.



Obrázek 34-1: Strom objektů eDirectory zobrazený v ConsoleOne

V současnosti je eDirectory k dispozici již ve verzi 8.8. Ta obsahuje řadu novinek a zdokonalení. Např. v oblasti instalace a upgrade umožňuje instalaci eDirectory do zadaného adresáře, na platformě Linux/Unix nabízí

různé formáty instalačních balíčků apod. Dále přináší možnost realizovat více instancí eDirectory na jednom serveru, autentizaci do eDirectory i prostřednictvím SASL-GSSAPI (tzn. přes LDAP a Kerberos), univerzální hesla s rozlišováním velikosti písmen, prioritní synchronizaci eDirectory (např. pro okamžitou synchronizaci hesel), šifrování dat uložených a přenášovaných mezi eDirectory servery, zálohování přes LDAP (což poskytuje standardní rozhraní pro zálohovací aplikace třetích výrobců) atd.

34.6 Objekty v eDirectory

Základem eDirectory je kořenový objekt **[Root]**. Ten musí mít každá eDirectory. Dále pod kořenem je možno použít nepovinný objekt **Country**. V menších sítích LAN není obvykle používán

Důležitý je povinný objekt **Organization**. V každém eDirectory stromu musí být minimálně jeden. Dále se Organization člení na objekty Organizational Unit.

Organizational Unit (OU) představuje hlavní prostředek pro větvení databáze. Umožňuje převedení struktury organizace do eDirectory. Zpravidla odpovídá samostatným skupinám v podniku, odloučeným pracovištím či pobočkám.

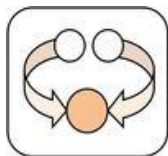
Všechny dosud uvedené objekty jsou uzlové, umožňují větvení databáze, V terminologii Novellu se označují se jako kontejner, kontejnerový objekt. Umožňují dědění práv a vlastností pro celou větev OU.

Při správě sítě se nejčastěji pracuje s koncovými objekty. Jde o prvky, které popisují skutečně existující součásti sítě. Dále se nedělí a obsahují řadu vlastností, kterými je daný síťový prvek popsán a nakonfigurován.

Koncových objektů je velmi mnoho, běžně se používají např. objekty typu:

- **User** zastupuje uživatele, kterému je dovoleno pracovat v síti. Mezi jeho typické vlastnosti patří jméno a heslo, kterým se do sítě hlásí, práva popisující povolené (či nepovolené) činnosti ve složkách, souborech nebo vztazích k jiným objektům. Zvláštním uživatelem, který je umístěný na úrovni OU je uživatel Admin.
- **Group** – přes Group se vytváří skupiny uživatelů v rámci jedné větve OU, podobný význam má objekt **Profile**, ten ale sdružuje uživatele z různých větví OU. Klíčovou vlastností je seznam členů – tedy uživatelů ve skupině, u objektu *Profile* navíc *login script*.
- **Server** se instaluje automaticky, Obsahuje především popisné informace (umístění serveru, jeho síťovou adresu apod.).
- **Volume** - logické disky.
- **Printer** – tiskárny a řada dalších.

Shrnutí kapitoly



Služba eDirectory je databáze, která udržuje informace o součástech počítačové sítě (tzn. o uživateli, serverech, tiskárnách, licencích, aplikacích, politikách apod.). Významně zjednodušuje správu sítě. Díky ní lze všechny prostředky sítě spravovat z jednoho místa a jednotnými nástroji. V současnosti je eDirectory k dispozici ve verzi 8.8.

Základní vlastnosti eDirectory:

- objektovost
- otevřenost
- hierarchičnost
- globálnost
- distribuovatelnost
- multiplatformnost

Správu eDirectory lze je rozdělit na:

- správu objektů eDirectory
- správu oblastí a kopií eDirectory
- údržbu eDirectory a řešení problémů

Pro realizaci činností souvisejících se správou eDirectory je k dispozici řada nástrojů:

- webová utilita iManager (Novell Identity Manager)
- Windows utilita NetWare Administrator
- Javová utilita *ConsoleOne*

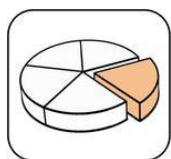
Základem eDirectory je kořenový objekt [Root]. Dále pod kořenem je nepovinný objekt Country, následuje povinný objekt Organization. V každém eDirectory stromu musí být minimálně jeden. Dále se Organization člení na objekty Organizational Unit.

Na nejnižší úrovni jsou objekty koncové, představující konkrétní síťové prvky jako např. objekty typu User, Group, Server, Printer, apod.

Kontrolní otázky a úkoly



- 1) Charakterizujte eDirectory a její vlastnosti.
- 2) Jak vypadá strom objektů v eDirectory?
- 3) Co jsou to uzlové a koncové objekty?
- 4) Jaké nástroje se používají pro správu eDirectory?
- 5) Co řeší správa eDirectory?

Použitá literatura a jiné zdroje:

- [1] PŘICHYSTAL, Oldřich. Adresářová služba Novell eDirectory. Novell.cz [online]. 2006 [cit. 2012-06-09]. Dostupné z: <http://www.novell.cz/cs/aktuality/technicke-clanky/novell-open-enterprise-server-specificke-instalace.html>

35 Licenční politiky v OS

Obsah hodiny



Obsahem této hodiny seznámení s pojmem licence, licenční politikou v OS.

Cíl hodiny



Po prostudování budete schopni:

- definovat pojem licence v informatice,
- charakterizovat jednotlivé typy licencí,
- orientovat se v licenční politice OS.

Klíčová slova



Licence, Licenční politika, FFF, OEM, Multilicenční programy, Software Assurance

35.1 Co je to licence?

Softwarová licence je v informatice právní nástroj, který umožňuje používat nebo redistribuovat software, který je chráněn zákonem. V České republice se jedná o Autorský zákon.

Nákupem softwarového produktu uživatel získává licenci, tedy právo používat software dle podmínek, které stanovuje autor. Je třeba mít na paměti, že zakoupení software neznamena vlastní výhradní užívací práva a nelze s produktem zacházet dle vlastního uvážení.

Podmínky, které autor uživateli uděluje, jsou definované v nejrůznějších licenčních ustanoveních a jsou v nejčastějších případech k dispozici před instalací produktu, nebo v různých dokumentech či smlouvách. Vždy platí, že autor má vyhrazená práva, což znamená, že není možné software používat jinak, než jak je to v licenčních podmínkách dovoleno. Zjednodušeně - co není v podmínkách povoleno, je zakázáno.

Povinnost dodržovat licenční podmínky je zakotvena v autorském zákoně. Ten mimo jiné definuje i přísné sankce a tresty, které mohou hrozit v případě nesouladu s licenčními podmínkami.

POZOR – používáním softwaru uživatel souhlasí s licenčními podmínkami.

Proprietární software je takový software, kde jeho autor upravuje licenci či jiným způsobem možnosti jeho používání. K takovému software nejsou zpravidla k dispozici volně zdrojové kódy či v nich nelze svobodně dělat úpravy a výsledné dílo distribuovat. Takový software obvykle spadá do kategorie komerčního software, který jeho autor prodává.

Otevřený software (open-source software nebo open software, zkratka OSS) je počítačový software s otevřeným zdrojovým kódem. Otevřenost zde znamená jak technickou dostupnost kódu, tak legální dostupnost - licenci software, která umožňuje, při dodržení jistých podmínek, uživatelům zdrojový kód využívat, například prohlížet a upravovat (na rozdíl od proprietárního software).

Svobodný software (free software) je software, ke kterému je k dispozici také zdrojový kód, spolu s právem tento software používat, modifikovat a distribuovat. Svobodný software je možno využívat i ke komerčním účelům.

EULA (End-User-License-Agreement) uzavření smlouvy s koncovým uživatelem. Určuje, co uživatel smí a nesmí dělat. Je možné, aby byl zdrojový kód open source, ale výsledný produkt už spadá pod EULA, kde se hovoří o zákazu editace a šíření tohoto programu.

35.2 Některé licence pro „svobodný“ software

BSD Licence (BSD Unixové systémy)

Zkratka BSD označuje „Berkeley Software Distribution“ – obchodní organizaci při University of California, Berkeley, která tuto licenci vyvinula a používala pro práce nad operačním systémem BSD.

BSD licence je licence pro svobodný software, mezi kterými je jednou z nejsvobodnějších. Umožňuje volné šíření licencovaného obsahu, vyžaduje pouze uvedení autora a informace o licenci, spolu s upozorněním na zřeknutí se odpovědnosti za dílo.

GNU General Public License (OS GNU/Linux, OS Hurd)

GNU GPL (česky „všeobecná veřejná licence GNU“) je licence pro svobodný software, původně napsaná Richardem Stallmanem pro projekt GNU. Zajišťuje základní svobody svobodného software, copyleft licenci.

Copyleft licence říká, že redistribuce originální nebo pozměněné verze se musí provádět pod stejnou licenci jako původní program. Znamená, že nelze přidávat žádná omezení.

35.3 Licenční politika Microsoft

Licenční politika společnosti Microsoft je oblast velmi složitá, zejména v oblasti pro organizace, nabízí řadu licenčních programů. Podrobné informace k této problematice najdete na stránkách:

- <http://www.microsoft.com/cze/legalnisoftware/>
- <http://www.microsoft.com/cs-cz/licensing/Default.aspx>

V zásadě je licencování postaveno licencích Retail (krabicový software *Full Package Product*), OEM licencích a multilicenčních programech.

Licenci lze nejen zakoupit, ale rovněž pronajmout.

35.4 Krabicový produkt FPP (*Full Package Product*)

Krabicové verze jsou určeny koncovým uživatelům, kteří potřebují jednu či dvě licence. Součástí balení je licenční smlouva (EULA - *End User Licence Agreement*), registrační karta, obvykle i tištěný manuál a instalační média. Uživatel si kupuje právo užívat software a rovněž službu technické podpory (podpora se vztahuje pouze na registrované zákazníky). Obdobně lze zakoupit produkt přes internet (stáhnout a posléze aktivovat přes koupený licenční klíč).

Majitel může krabicovou verzi dále prodat či převést na jiný subjekt. Nový majitel při prokazování legálnosti takto získaného software musí mít veškeré součásti původního "balení" a dále převodní smlouvu, ve které původní majitel, potvrzuje, že software řádně odinstaloval a nadále jej nepoužívá. Nový majitel se pak zavazuje splnit podmínky licenčního ujednání.

Jedná se o nejdražší variantu.

35.5 OEM licence

Další nejčastější možností při pořizování nového počítače je tzv. OEM (neboli *Original Equipment Manufacture*) software, což je výhodná možnost jak produkt získat výrazně levněji než krabicovou verzi. V praxi se jedná o nejlevnější cestu k Windows pro většinu lidí nejen pro malé firmy. Funkčně je shodná s plnou verzí, omezení je pouze licenční!!

Tyto produkty se od svých krabicových kolegů liší pouze ve formě distribuce, v ceně a dalších podmínkách používání. Technickou podporu v tomto případě neposkytuje Microsoft, ale daný dodavatel hardware. Kvalita takové služby je pak přímo závislá na úrovni daného prodejce.

OEM licence je možné prodat pouze s úplným počítačovým systémem. Neplatí možnost prodeje s komponentou nebo částí PC, musí jít o nákup

nového PC. OEM licence není možné přesunout na jiný hardware, z čehož vyplývá, že při zániku hardware zaniká i s ním svázaná OEM licence.

Zákazník nezíská žádná práva na předchozí verze produktů (downgrade).

OEM licence jsou nabízeny pro produkty

- Microsoft Windows® Windows 7 ve verzích Home Premium, Professional a Ultimate.
- Microsoft Office 2010 Home and Business, Microsoft Office 2010 Pro
- Microsoft Windows Server 2008R2 a Windows Small Business Server 2011.

35.6 Multilicenční programy

Při získání softwarových licencí prostřednictvím multilicenčních programů společnosti Microsoft se platí pouze za licenci na software, nikoli za disk CD-ROM nebo DVD, uživatelskou příručku a další položky, které jsou součástí krabicového produktu.

Multilicenční programy se snaží zohlednit potřeby jednotlivých odvětví, v závislosti na primární funkci organizace (například pro potřeby organizací veřejného sektoru, jako jsou školy a univerzity).

V případě některých multilicenčních programů společnosti Microsoft je možné koupit také program Software Assurance (u OEM softwaru nebo Krabicového produktu do 90 dnů po zakoupení). Ten představuje řadu výhod a benefitů, které je možné přikoupit k produktům Microsoft.

Operační systém Windows zakoupený v multilicenčním programu není plnohodnotnou licencí, ale pouze upgrade. Licenci je možné instalovat pouze na počítače s odpovídající podkladovou licencí.

Software Assurance je dostupná v různých multilicenčních programech (Open License, Open Value, Select Plus, Enterprise Agreement).

Některé výhody Software Assurance (SA)

Právo na nové verze a právo používat nejvyšší edici OS Enterprise, která obsahuje veškerou funkcionalitu.

Licence pro virtualizaci Windows na PC a serveru: lze instalovat systém Windows (libovolné verze a edice) v rámci až 4 virtuálních prostředích na licencovaném zařízení a přistupovat k nim ze zalicencovaného zařízení.

Není možné, aby k virtualizovanému Windows na serveru přistupoval současně jak primární uživatel z nezalicencovaného (nefiremního!) zařízení, tak jiný uživatel ze zalicencovaného zařízení.

Poukazy na školení - podrobné technické školení v učebnách pro IT specialisty a vývojáře. Možnosti E-Learningu.

35.7 Licenční politika pro produkty Novell

Společnost Novell nabízí tři základní licenční programy pro různé typy zákazníků.

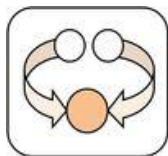
Hlavní licenční smlouva (Master License Agreement - MLA) poskytuje speciální licenční možnosti pro významné zákazníky společnosti Novell, vycházející z hromadných nákupů produktů a jistotě dlouhodobého vztahu.

Objemová licenční smlouva (Volume Licence Agreement - VLA) je základní úrovní programu nákupu u společnosti Novell. Licence, zakoupené v režimu VLA, podléhají termínům a podmínkám Dohody o licenci koncového uživatele (EULA), specifickým pro každý produkt.

Licence mohou být zakoupeny buď samostatně, nebo v kombinaci se standardní nebo přednostní údržbou. Údržba je kombinace aktualizace produktů, technické podpory a školení.

Smlouva o školské licenci (School License Agreement - SLA) je licenční nástroj pro organizace, které poskytují základní vzdělání. Poskytuje za roční poplatek některé výhody – např. přístup k nejnovějším aktualizacím bez dalších nákladů, právo a slevy na nákup trvalých licencí produktů.

Shrnutí kapitoly



Softwarová licence je v informatice právní nástroj, který umožňuje používat nebo redistribuovat software, který je chráněn zákonem. V České republice se jedná o Autorský zákon.

Nákupem softwarového produktu uživatel získává licenci, tedy právo používat software dle podmínek, které stanovuje autor.

Některé licence pro „svobodný“ software:

- BSD Licence (BSD Unixové systémy)
- GNU General Public License (OS GNU/Linux, OS Hurd)

Licenční politika společnosti Microsoft je oblast velmi složitá, zejména v oblasti multilicencí. Základem licenční politiky jsou

- Retail - krabicový software FPP (*Full Package Product*)
- OEM licence
- Multilicenční programy

V případě některých multilicenčních programů společnosti Microsoft je možné koupit také program Software Assurance, který obsahuje řadu výhod a benefitů, které je možné přikoupit k produktům Microsoft.

Licenční politika pro produkty Novell

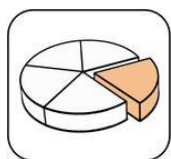
- Hlavní licenční smlouva
- Objemová licenční smlouva
- Smlouva o školské licenci

Kontrolní otázky a úkoly



- 1) Co je to licence?
- 2) Co je to proprietární, otevřený a svobodný SW?
- 3) Jaké licence používají OS GNU/Linux a BSD Unix?
- 4) Jaké jsou možnosti licencování ve Windows?
- 5) Jaké jsou možnosti licencování v Novellu?

Použitá literatura a jiné zdroje:



- [1] BSD licence. In: Wikipedia: the free encyclopedia [online]. San Francisco (CA): Wikimedia Foundation, 2004, 2012 [cit. 2012-06-10]. Dostupné z: http://cs.wikipedia.org/wiki/BSD_licence
- [2] Vyznáte se v licenční politice Microsoftu? OEM nebo FPP?. In: Zive.cz [online]. 23. 6. 2005 [cit. 2012-06-06]. Dostupné z: <http://www.zive.cz/clanky/vyznate-se-v-licencni-politice-microsoftu-oem-nebo-fpp/sc-3-a-125434/default.aspx>
- [3] MICROSOFT CORPORATION. Microsoft Partner Network: Licencování [online]. ©2012 [cit. 2012-06-10]. Dostupné z: <https://partner.microsoft.com/cze/licensing>
- [4] Microsoft Licencování. MICROSOFT. Licensing [online]. © 2012 [cit. 2012-06-10]. Dostupné z: <http://www.microsoft.com/cs-cz/licensing/default.aspx>
- [5] NOVELL, Inc. Licenční programy [online]. 2011 [cit. 2012-06-10]. Dostupné z: <http://www.novell.cz/cs/zpusob-nakupu/licencni-programy>