

Obsah

Předmluva	11
Poděkování	15
1 Úvod	17
Správa sítě	18
Proč nástroje s otevřeným kódem?	18
Cena je důležitá	19
Vežce v košíku	19
Možná získáte to, co potřebujete	20
Otázka kvality	20
Je to bezpečné?	21
Podpora	21
Nástroje v této knize	21
Prostředí	22
Pozadí	22
Terminologie a konvence	23
2 SNMP	25
Seznámení s SNMP	26
SNMP	26
Proměnné a MIB	27
Identifikátory objektu a hierarchie proměnných	28
Instance jednoduché proměnné	29
Úvod do tabulek	30
Lexikografické řazení a požadavek typu Get-Next-Request	31
Trapy	32
Jak vám může SNMP pomoci	32
Skupina system	32
Skupina interfaces	34
Tabulka ip.ipNetToMediaTable	35
MIB bridge	36
Instalace nástrojů SNMP	37
Překlad ze zdrojového kódu	38
Překlad a instalace	38
Práce s nástroji SNMP	39
Program snmpget	39
Program snmpset	41
Program snmpwalk	42
Program snmptrapd	43

Další nástroje	44
Manipulace s MIB	45
Skripty a nástroje SNMP	45
Údržba nástrojů SNMP	46
Odkazy a další informace	46
3 MRTG	47
Seznámení s programem MRTG	48
Jak vám může MRTG pomoci	48
Instalace MRTG	49
Překlad knihovny PNG	49
Překlad knihovny GD	50
Překlad programu MRTG	50
Konfigurace programu MRTG	51
Generování konfiguračního souboru	51
Další konfigurační volby	53
Generování počátečních dat	53
Generování indexových stránek	54
Nastavení pravidelného sběru dat	55
Použití MRTG	56
Chybná data	56
Chybějící data	56
Údržba programu MRTG	57
Odkazy a další informace	57
4 NEO	59
Seznámení s programem Neo	60
Jak vám může Neo pomoci	60
Instalace programu Neo	63
Použití programu Neo	64
Příkazový řádek	64
Syntaxe zadání cíle	65
Proměnné	68
Příkaz arpfind	69
Příkaz locate	70
Příkaz port	71
Příkaz device summary	72
Příkaz device info	74
Příkaz stats	75
Nápověda	77
Řádkové parametry	77
Další příkazy	78
Použití programu Neo ve zhoršených podmínkách	78
Příklady použití	79

Údržba programu Neo	81
Odkazy a další informace	82
5 NETFLOW	83
Seznámení s funkcí NetFlow a nástroji Flow-Tools	84
Jak vám může NetFlow pomoci	84
Jak NetFlow funguje	85
Toky	85
NetFlow a přepínací cesty	86
Export dat z NetFlow	86
Verze programu NetFlow	86
Instalace nástrojů Flow-Tools	87
Nastavení mechanismu NetFlow na směrovači	88
Použití nástrojů Flow-Tools	88
Příjem dat	89
Zobrazení dat	94
Manipulace s daty	100
Odkazy a další informace	102
6 OAK	103
Seznámení s programem Oak	104
Jak vám může Oak pomoci	104
Instalace programu Oak	106
Použití programu Oak	106
Nastavení syslogu na unixových stanicích	106
Nastavení syslogu na síťových zařízeních	109
Úvod do regulárních výrazů	109
Konfigurace programu Oak	112
Údržba programu Oak	117
Odkazy a další informace	117
7 Dohled služeb	119
Seznámení s dohledem služeb	120
Jak vám může dohled služeb pomoci	121
Instalace programu Sysmon	122
Kam umístit dohledový server	122
Instalace programu Sysmon	122
Použití programu Sysmon	123
Konfigurace Sysmonu	126
Kořenový uzel	126
Objekty a závislosti	126
Globální volby	130
Údržba programu Sysmon	133

Nagios	134
Odkazy a další informace	135

8 TCPDUMP **137**

Seznámení s programem tcpdump	138
Jak vám může tcpdump pomoci	138
Omezení programu tcpdump	140
Instalace programu tcpdump	140
Možná máte vyhráno	140
Kterou verzi přeložit	140
Knihovna pcap	141
Tepdump	141
Použití programu tcpdump	142
Spouštění jako superuživatel	142
Řádkové volby	142
Filtry	145
Příklady použití	146
Popis výstupního formátu	146
Zobrazení dat v paketech	147
Jak vidět všechno	148
Příklady diagnostiky programem tcpdump	150
Zahlcení provozem	150
Složitější příklad	151
Údržba programu tcpdump	152
Jiné analyzátoři paketu	152
Odkazy a další informace	152

9 Základní nástroje **153**

ping	154
Jak ping funguje	154
Telnet	158
Netcat	159
Instalace programu Netcat	160
Použití programu Netcat	160
Traceroute	163
Jak traceroute funguje	163
Instalace programu traceroute	164
Použití programu traceroute	165
MTR	166
Instalace MTR	166
Použití programu MTR	167
Netstat	169

10 Vlastní nástroje	171
Skriptovací jazyky	172
Spuštění skriptu	173
Konvence názvů	174
Lokální proměnné a proměnné prostředí	174
Bourne shell	174
Základy Bourne shellu	174
Použití proměnných	175
Lokální proměnné a proměnné prostředí	176
Návratový kód	177
Podmínky	178
Parametry	179
Smyčky	180
Použití výstupu příkazu	180
Práce se vstupem a výstupem	181
Funkce	181
Další různé možnosti	182
Perl	184
Základy Perlu	184
Použití proměnných	184
Lokální proměnné a proměnné prostředí	184
Podmínky	185
Manipulace s textem	186
Seznamy	187
Hashe	188
Čtení ze souboru	188
Zápis do souboru	189
Parametry	190
Smyčky	190
Použití výstupu příkazu	191
Podprogramy	191
Ukončení	191
Perl a skripty pro sledování sítě	192
Programování dohledových systémů	192
Časování smyček	192
Stavový automat	193
Zajištění trvalého běhu	194
Pěknější mail pomocí sendmailu	194
Spouštění programu z cronu	195
Odkazy a další informace	196
11 Ethereal	197
K čemu Ethereal slouží?	198
Packet driver, promiskuitní mód	199
WinPCapp	200
Začínáme s Etherealem	200

Filtry	203
Colorig rules	205
Follow TCP stream	206
Statistiky	207
Tisk a export	208
Příkazový řádek	208
Sniffer	209
Závěr	209

Rejstřík	211
-----------------	------------
