

# Obsah

---

<b>Poděkování autora</b>	<b>13</b>
<b>Úvod</b>	<b>15</b>
Komu je kniha určena	15
Co v knize najdete a nenajdete	15
<b>Výběr témat</b>	<b>16</b>
<b>Obsah doprovodného CD</b>	<b>17</b>
Několik slov o operačním systému Microsoft Windows Server 2008	18
KAPITOLA 1	
<b>Nástroje pro správu operačního systému</b>	<b>21</b>
Základy správy pomocí Správce serveru	21
<b>Přidání a odebrání role serveru</b>	<b>23</b>
<b>Odstranění role serveru</b>	<b>24</b>
<b>Přidání funkcí serveru</b>	<b>24</b>
<b>Odebrání funkce serveru</b>	<b>25</b>
<b>Rychlý přístup k základním nastavením serveru</b>	<b>26</b>
Administrativní rozhraní MMC	27
<b>Osazení rozhraní MMC moduly snap-in</b>	<b>27</b>
<b>Vytvoření vlastního rozhraní MMC</b>	<b>29</b>
Ovládání operačního systému z příkazového řádku	32
<b>Nastavení vlastností okna Příkazového řádku</b>	<b>32</b>
<b>Ovládání příkazového řádku klávesovými příkazy</b>	<b>33</b>
Správa operačního systému pomocí skriptovacího jazyka PowerShell	34
<b>Instalace PowerShellu v Správci serveru</b>	<b>34</b>
<b>Úprava profilu PowerShellu</b>	<b>35</b>
<b>Konfigurace spouštění skriptů</b>	<b>36</b>
<b>Získání nápovědy</b>	<b>36</b>
Skriptovací prostředí Windows Script Host (WSH)	37
<b>Instalace prostředí WSH</b>	<b>38</b>
<b>Spuštění skriptu WSH</b>	<b>38</b>
<b>Nastavení výchozího interpreteru pro skripty WSH</b>	<b>38</b>
<b>Použití VBScriptu ve stránce HTA</b>	<b>39</b>

Technologie Windows Management Instrumentation (WMI)	40
<b>Dotaz na objekt operačního systému z příkazového řádku</b>	<b>40</b>
<b>Dotaz na objekt operačního systému v PowerShellu</b>	<b>40</b>
<b>Generování dotazů WMI</b>	<b>40</b>
Možnosti vzdálené správy	41
<b>Použití Vzdálené plochy pro správu</b>	<b>41</b>
<b>Vzdálená správa pomocí rozhraní MMC</b>	<b>42</b>
<b>Vzdálená správa serveru v režimu jádra (Server Core)</b>	<b>43</b>

## KAPITOLA 2

**Instalace a konfigurace operačního systému** **45**

Možnosti instalace operačního systému	45
<b>Instalace z DVD</b>	<b>45</b>
<b>Vytvoření odpovědního souboru pro bezobslužnou instalaci</b>	<b>51</b>
<b>Bezobslužná instalace z média DVD</b>	<b>56</b>
<b>Instalace jádra serveru (Server Core)</b>	<b>57</b>
Instalace operačního systému pomocí Služby pro nasazení systému Windows (WDS)	58
<b>Úvodní konfigurace serveru Služby pro nasazení systému Windows (WDS) a instalace této služby</b>	<b>59</b>
<b>Úvodní konfigurace serveru Služby pro nasazení systému Windows</b>	<b>60</b>
<b>Přidání výchozí spouštěcí bitové kopie na server služby WDS</b>	<b>62</b>
<b>Přidání výchozí instalační bitové kopie na server služby WDS</b>	<b>64</b>
<b>Přidání spustitelné bitové kopie pro zachycení obrazu počítače</b>	<b>65</b>
<b>Vytvoření bitové kopie z referenčního počítače</b>	<b>67</b>
<b>Instalace počítače z bitové kopie</b>	<b>71</b>
Konfigurace disků a datového úložiště	72
<b>Vytvoření nového jednoduchého svazku</b>	<b>73</b>
<b>Konfigurace zrcadlení existujícího svazku</b>	<b>76</b>
<b>Vytvoření nového zrcadleného svazku</b>	<b>77</b>
<b>Vytvoření svazku RAID-5</b>	<b>79</b>
<b>Oprava zrcadleného svazku při selhání jednoho z disků</b>	<b>80</b>
<b>Konverze souborového systému z FAT32 na NTFS</b>	<b>81</b>
<b>Zvětšení nebo zmenšení svazku</b>	<b>82</b>
Připojení serveru k síti	83
<b>Nastavení vlastností TCP/IP pomocí Správce serveru</b>	<b>83</b>
<b>Nastavení vlastností TCP/IP z příkazového řádku</b>	<b>85</b>
<b>Ověření konektivity serveru</b>	<b>85</b>
<b>Připojení serveru do domény Active Directory</b>	<b>87</b>

Zálohování a obnova serveru	88
<b>Instalace nástroje Zálohování serveru</b>	<b>89</b>
<b>Naplánování zálohovacích úloh</b>	<b>90</b>
<b>Jednorázové zálohování</b>	<b>92</b>
<b>Zálohování z příkazového řádku pomocí nástroje Wbadmin</b>	<b>94</b>
<b>Výpis seznamu disků</b>	<b>94</b>
<b>Vytvoření naplánované úlohy zálohování</b>	<b>94</b>
<b>Zastavení naplánovaných denních úloh zálohování</b>	<b>95</b>
<b>Jednorázová záloha kolekce dat Stav systému</b>	<b>95</b>
<b>Obnova dat v grafickém rozhraní</b>	<b>95</b>
<b>Obnova dat z příkazového řádku pomocí nástroje Wbadmin</b>	<b>97</b>
<b>Obnova složky včetně podsložek a souborů</b>	<b>97</b>
<b>Obnova souborů ze vzdáleného počítače</b>	<b>98</b>
<b>Obnova operačního systému ze zálohy</b>	<b>98</b>

## KAPITOLA 3

**Správa síťové infrastruktury 103**

Dynamická konfigurace síťových klientů pomocí DHCP	103
<b>Instalace role serveru DHCP</b>	<b>103</b>
<b>Instalace role serveru DHCP na jádru serveru</b>	<b>105</b>
<b>Autorizace serveru DHCP v doméně Active Directory</b>	<b>105</b>
<b>Vytvoření oboru DHCP a jeho vlastností</b>	<b>106</b>
<b>Nastavení možností DHCP</b>	<b>108</b>
<b>Vytvoření rezervace klienta DHCP</b>	<b>109</b>
<b>Kontrola konzistence</b>	<b>111</b>
<b>Konfigurace DHCP pomocí příkazu netsh</b>	<b>111</b>
<b>Záloha serveru DHCP</b>	<b>112</b>
<b>Obnova serveru DHCP</b>	<b>113</b>
<b>Statistiky serveru DHCP</b>	<b>113</b>
Zavedení překladu názvů pomocí služby DNS	114
<b>Instalace služby DNS pomocí Správce serveru</b>	<b>114</b>
<b>Instalace služby DNS z příkazového řádku (Server Core)</b>	<b>115</b>
<b>Vytvoření nové zóny dopředného vyhledávání integrované v Active Directory</b>	<b>115</b>
<b>Vytvoření standardní primární zóny DNS</b>	<b>116</b>
<b>Vytvoření sekundární zóny DNS</b>	<b>117</b>
<b>Vytvoření nové zóny zpětného vyhledávání</b>	<b>118</b>
<b>Vynucená registrace záznamu počítače v zóně DNS</b>	<b>120</b>
<b>Vytvoření nového záznamu v zóně DNS</b>	<b>120</b>
<b>Přidání serveru DNS do seznamu názvových serverů</b>	<b>121</b>
<b>Konfigurace přenosu zóny</b>	<b>122</b>
<b>Použití zóny GlobalNames</b>	<b>123</b>

<b>Delegování domény DNS</b>	<b>124</b>
<b>Konfigurace předávání dotazů DNS jiným serverům</b>	<b>125</b>
<b>Záloha a obnova standardní zóny DNS</b>	<b>126</b>
<b>Vyprázdnění paměti cache pomocí konzoly DNS</b>	<b>126</b>
<b>Vyprázdnění paměti cache pomocí příkazového řádku</b>	<b>126</b>
<b>Výpis informací o serveru DNS</b>	<b>126</b>
<b>Nastavení stárnutí a úklidu záznamů</b>	<b>127</b>
<b>Spuštění operace úklidu zastaralých záznamů pomocí nástroje DNSCMD</b>	<b>128</b>
<b>Diagnostika překladu názvů DNS pomocí nástroje DNSLINT</b>	<b>129</b>
Integrace služby DNS a Active Directory	133
<b>Konverze standardní zóny DNS do zóny integrované v AD DS</b>	<b>133</b>
<b>Konfigurace dynamických aktualizací</b>	<b>134</b>
<b>Vytvoření vlastního aplikačního oddílu Active Directory</b>	<b>134</b>
<b>Změna oboru replikace zóny uložené v Active Directory</b>	<b>135</b>
Směrování protokolu IP	136
<b>Instalace služeb Směrování a vzdáleného přístupu</b>	<b>136</b>
<b>Konfigurace protokolu RIP</b>	<b>138</b>
<b>Nastavení statického směrování</b>	<b>139</b>
<b>Směrování pomocí příkazu Route</b>	<b>140</b>
Překlad síťových adres pomocí Network Address Translation (NAT)	140
<b>Nastavení Sdílení připojení k Internetu</b>	<b>141</b>
<b>Konfigurace překladu síťových adres pomocí služby Směrování a vzdáleného přístupu</b>	<b>142</b>
<b>Povolení předávání žádostí DNS</b>	<b>145</b>
Umožnění vzdáleného přístupu klientům z jiných sítí	146
<b>Povolení a konfigurace vzdáleného přístupu pomocí připojení VPN</b>	<b>146</b>
<b>Připojení klienta k síti VPN</b>	<b>148</b>
<b>Nastavení paketových filtrů serveru VPN</b>	<b>149</b>

## KAPITOLA 4

**Nasazení a správa adresářové služby Active Directory** **151**

Instalace a správa infrastruktury Active Directory	151
<b>Instalace řadiče domény do nové doménové struktury</b>	<b>152</b>
<b>Kontrola úspěšné instalace řadiče domény</b>	<b>155</b>
<b>Instalace řadiče domény pomocí replikace ze zálohy</b>	<b>155</b>
<b>Bezobslužná instalace řadiče domény</b>	<b>158</b>
<b>Bezobslužná odinstalace doménového řadiče</b>	<b>159</b>
<b>Bezobslužná instalace řadiče domény bez odpovědního souboru</b>	<b>160</b>
<b>Instalace řadiče domény pouze pro čtení (RODC)</b>	<b>160</b>
<b>Delegovaná instalace doménového řadiče pouze pro čtení – fáze vytvoření účtu řadiče</b>	<b>164</b>
<b>Delegovaná instalace doménového řadiče pouze pro čtení – fáze povýšení řadiče</b>	<b>166</b>
<b>Odinstalování Active Directory z řadiče domény</b>	<b>168</b>

<b>Odstanění záznamů o doménovém řadiči, který již neexistuje</b>	<b>170</b>
<b>Přesun databáze a logů AD DS do jiného umístění</b>	<b>172</b>
<b>Defragmentace a údržba databáze Active Directory</b>	<b>174</b>
<b>Migrace replikace složky SYSVOL z FRS na DFS-R</b>	<b>177</b>
<b>Zvýšení funkční úrovně domény a doménové struktury</b>	<b>177</b>
Active Directory Lightweight Directory Services	178
<b>Požadavky na instalaci AD LDS</b>	<b>179</b>
<b>Instalace AD LDS</b>	<b>179</b>
<b>Instalace AD LDS na jádro serveru (Server Core)</b>	<b>180</b>
<b>Vytvoření instance AD LDS</b>	<b>180</b>
Hlavní operační servery	182
<b>Správné umístění hlavních operačních serverů</b>	<b>183</b>
<b>Zjištění držitele rolí Emulátor primárního řadiče domény (PDC Emulátor),         hlavní server infrastruktury (Infrastructure Master)         a hlavní operační server RID (RID Master)</b>	<b>183</b>
<b>Zjištění hlavního operační serveru schématu</b>	<b>184</b>
<b>Zjištění hlavního operačního serveru pro pojmenování domén</b>	<b>185</b>
<b>Zjištění rolí hlavních operačních serverů na konkrétním řadiči domény</b>	<b>185</b>
<b>Přenos rolí hlavních operačních serverů</b>	<b>185</b>
<b>Převzetí role hlavního operačního serveru v případě jeho nedostupnosti</b>	<b>187</b>
Správa uživatelských účtů	188
<b>Vytvoření uživatelského účtu pomocí konzoly Uživatelé         a počítače služby Active Directory (Active Directory Users and Computers)</b>	<b>189</b>
<b>Vytvoření uživatelského účtu pomocí příkazu DSADD.EXE</b>	<b>191</b>
<b>Vytváření uživatelských účtů pomocí nástroje CSVDE.EXE</b>	<b>191</b>
<b>Vytváření uživatelských účtů pomocí nástroje LDIFDE.EXE</b>	<b>193</b>
<b>Vytvoření uživatelského účtu pomocí VBScriptu</b>	<b>194</b>
<b>Vytvoření uživatelského účtu pomocí PowerShellu</b>	<b>194</b>
<b>Zobrazení skrytých atributů uživatelského účtu</b>	<b>195</b>
<b>Přidání vlastní záložky Additional Account Info do vlastností uživatelského účtu</b>	<b>196</b>
Správa skupin	197
<b>Vytvoření doménové skupiny pomocí konzoly Uživatelé         a počítače služby Active Directory</b>	<b>197</b>
<b>Vytvoření skupiny pomocí příkazu DSADD.EXE</b>	<b>198</b>
<b>Vytvoření skupin pomocí nástroje CSVDE.EXE</b>	<b>198</b>
<b>Vytváření skupin pomocí nástroje LDIFDE.EXE</b>	<b>199</b>
<b>Vytváření skupin pomocí VBScriptu</b>	<b>200</b>
<b>Vytváření skupin pomocí PowerShellu</b>	<b>202</b>
<b>Změna typu a rozsahu skupiny</b>	<b>203</b>
<b>Přidání skupiny do jiné skupiny</b>	<b>205</b>
<b>Přejmenování skupiny</b>	<b>206</b>
<b>Výpis přímých členů skupiny</b>	<b>206</b>

<b>Výpis přímých i nepřímých členů skupiny</b>	<b>207</b>
<b>Výpis skupin, jichž je skupina členem</b>	<b>208</b>
<b>Výpis přímého členství ve skupinách</b>	<b>208</b>
<b>Výpis přímého i nepřímého členství</b>	<b>208</b>
<b>Hromadné přidání členů skupiny do jiné skupiny</b>	<b>209</b>
Správa organizačních jednotek	209
<b>Vytvoření organizační jednotky v konzole Uživatelé a počítače Active Directory</b>	<b>210</b>
<b>Odstranění organizační jednotky</b>	<b>211</b>
<b>Přesun objektů mezi organizačními jednotkami</b>	<b>212</b>
<b>Výpis objektů podle kritérií</b>	<b>213</b>
Delegovaná správa Active Directory	213
<b>Delegace řízení uživateli nebo skupině</b>	<b>213</b>
<b>Zjištění seznamu oprávnění přiřazených na objektu adresářové služby</b>	<b>215</b>
<b>Zjištění seznamu oprávnění přiřazených na objektu AD DS v příkazovém řádku</b>	<b>217</b>
Zásady skupiny	218
<b>Vytvoření nového objektu zásad skupiny</b>	<b>219</b>
<b>Úprava existujícího objektu zásad skupiny</b>	<b>220</b>
<b>Propojení objektu zásad skupiny</b>	<b>220</b>
<b>Zákaz a odstranění propojení</b>	<b>220</b>
<b>Změna priority vazby</b>	<b>221</b>
<b>Povolení a zakázání uzlu objektu zásad skupiny</b>	<b>222</b>
<b>Cílení na úrovni položky</b>	<b>223</b>
<b>Režim zpracování duplicitních zásad skupiny uživatele (Loopback Processing)</b>	<b>225</b>
<b>Zablokování dědičnosti</b>	<b>227</b>
<b>Vynucené propojení objektu zásad skupiny</b>	<b>227</b>
<b>Filtrování zabezpečení</b>	<b>227</b>
<b>Vyhledávání nastavení v šablonách pro správu pomocí filtrů</b>	<b>229</b>
<b>Generování výsledné sady zásad</b>	<b>230</b>
<b>Modelování zásad skupiny</b>	<b>232</b>
<b>Změna intervalu pro aktualizaci zásad skupiny</b>	<b>234</b>
<b>Vyžádání aktualizace zásad skupiny na klientském počítači</b>	<b>236</b>
Ověřování v Active Directory Domain Services	237
<b>Nastavení zásad hesla</b>	<b>237</b>
<b>Nastavení podrobných zásad hesla pro různé skupiny uživatelů</b>	<b>238</b>
<b>Která zásada hesla je platná pro daného uživatele?</b>	<b>240</b>
<b>Definice uživatelů, kteří mohou být ověřeni řadičem domény pouze pro čtení (RODC)</b>	<b>240</b>
<b>Předběžné vyplnění hesel uživatelů na řadiči domény RODC</b>	<b>241</b>
Lokality a replikace	243
<b>Vytvoření nové lokality</b>	<b>243</b>
<b>Konfigurace serveru globálního katalogu</b>	<b>244</b>
<b>Povolení ukládání členství v univerzální skupině do mezipaměti</b>	<b>245</b>

<b>Použití nástroje repadmin.exe pro řešení problémů s replikací</b>	<b>246</b>
<b>Zobrazení stavu replikace</b>	<b>246</b>
<b>Kontrola replikační topologie pomocí KCC</b>	<b>247</b>
<b>Vynucená replikace oddílů z jednoho řadiče domény na druhý</b>	<b>248</b>
<b>Vytvoření objektu propojení lokalit</b>	<b>248</b>
<b>Změna replikačního plánu</b>	<b>248</b>
<b>Záloha a obnova Active Directory</b>	<b>250</b>
<b>Záloha adresářových služeb</b>	<b>250</b>
<b>Běžná a autoritativní obnova objektu Active Directory</b>	<b>251</b>
<b>Běžná obnova</b>	<b>252</b>
<b>Autoritativní obnova</b>	<b>253</b>

## KAPITOLA 5

**Instalace, konfigurace a správa souborových a tiskových služeb 255**

<b>Souborové služby</b>	<b>255</b>
<b>Instalace role Souborová služba (File Server)</b>	<b>255</b>
<b>Instalace nástroje Správce prostředků souborového serveru (File Server Resource Manager)</b>	<b>257</b>
<b>Nasazení kvót pomocí Správce prostředků souborového serveru (File Server Resource Manager)</b>	<b>258</b>
<b>Blokování ukládání určitých typů souborů</b>	<b>259</b>
<b>Vytváření přehledů o úložišti dat</b>	<b>260</b>
<b>Nasazení služby DFS</b>	<b>261</b>
<b>Vytvoření oboru názvů DFS</b>	<b>262</b>
<b>Přidání složky do oboru názvů DFS</b>	<b>263</b>
<b>Replikace složek v systému DFS</b>	<b>264</b>
<b>Sdílení dat v síti</b>	<b>265</b>
<b>Vytvoření sdílené složky</b>	<b>265</b>
<b>Publikování sdílené složky v Active Directory</b>	<b>266</b>
<b>Zajištění sdílené složky</b>	<b>268</b>
<b>Zabezpečení pomocí oprávnění SMB</b>	<b>270</b>
<b>Výčet založený na úrovni přístupu</b>	<b>270</b>
<b>Výpis sdílených složek pomocí grafického rozhraní</b>	<b>271</b>
<b>Výpis sdílených složek pomocí příkazového řádku</b>	<b>271</b>
<b>Mapování síťového disku pomocí grafického rozhraní</b>	<b>272</b>
<b>Mapování síťového disku pomocí příkazu nebo skriptu</b>	<b>272</b>
<b>Zabezpečení přístupu k datům pomocí oprávnění NTFS</b>	<b>272</b>
<b>Zabezpečení pomocí oprávnění NTFS obecně</b>	<b>273</b>
<b>Principy oprávnění NTFS</b>	<b>273</b>
<b>Změna oprávnění NTFS a vypnutí dědičnosti</b>	<b>274</b>
<b>Udělení přístupu prostřednictvím oprávnění NTFS</b>	<b>276</b>

<b>Zjištění skutečných oprávnění NTFS</b>	<b>277</b>
<b>Zjištění a nastavení oprávnění pomocí příkazového řádku</b>	<b>278</b>
<b>Převzetí vlastnictví souboru nebo složky</b>	<b>279</b>
Tiskové služby	280
<b>Instalace role Tiskové služby</b>	<b>280</b>
<b>Instalace tiskárny na tiskový server</b>	<b>281</b>
<b>Vytvoření fondu tiskáren</b>	<b>282</b>
<b>Instalace tiskárny na klientský počítač pomocí skriptu</b>	<b>284</b>
<b>Instalace tiskárny na klientský počítač pomocí zásad skupiny</b>	<b>284</b>
<b>Instalace tiskárny na klientský počítač pomocí předvoleb zásad skupiny</b>	<b>288</b>
<b>Přesunutí tiskové úlohy z jedné tiskárny na druhou</b>	<b>291</b>
<b>Nastavení exkluzivity pro používání tiskárny specifickou skupinou uživatelů</b>	<b>291</b>
<b>Upřednostnění tiskových úloh zaslaných specifickou skupinou uživatelů</b>	<b>293</b>
<b>Změna složky pro zařazování tiskových úloh</b>	<b>294</b>
<b>Nastavení a vytvoření vlastní oddělovací stránky</b>	<b>295</b>
<b>Přesunutí tiskáren i tiskových front na jiný tiskový server</b>	<b>296</b>
KAPITOLA 6	
<b>Sledování systému</b>	<b>299</b>
<hr/>	
Správa protokolů událostí	299
<b>Práce s protokoly událostí a Prohlížečem událostí</b>	<b>299</b>
<b>Prohlížení událostí a jejich interpretace</b>	<b>300</b>
<b>Připojení úlohy k události</b>	<b>304</b>
<b>Odstranění úlohy připojené k události</b>	<b>306</b>
<b>Vytvoření vlastního pohledu na události</b>	<b>306</b>
<b>Nastavení vlastností souboru protokolů</b>	<b>308</b>
<b>Export záznamů</b>	<b>309</b>
<b>Vytvoření odběru událostí ze vzdálených počítačů</b>	<b>309</b>
Sledování spolehlivosti a výkonu	312
<b>Sledování výkonu a procesů pomocí Správce úloh</b>	<b>313</b>
<b>Podrobné sledování výkonu v reálném čase</b>	<b>314</b>
<b>Protokolované sledování výkonu systému</b>	<b>316</b>
<b>Vytvoření vlastní sady kolekcí dat</b>	<b>318</b>
<b>Naplánování sledování výkonu</b>	<b>321</b>
Správa přiřazování prostředků serveru	322
<b>Instalace Správce systémových prostředků</b>	<b>322</b>
<b>Nastavení přidělení zdrojů pro konkrétní aplikaci</b>	
– vytvoření kritéria přiřazování procesů	<b>323</b>
<b>Vytvoření zásady přidělení prostředků</b>	<b>324</b>
<b>Nastavení přidělení zdrojů pomocí kalendáře</b>	<b>326</b>



## KAPITOLA 7

**Internetové a intranetové služby 329**

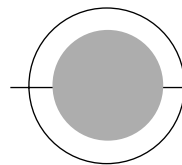
Instalace a konfigurace služeb terminálového serveru	329
<b>Instalace role Terminálového serveru</b>	<b>330</b>
<b>Zveřejnění aplikací RemoteApp</b>	<b>331</b>
<b>Spuštění aplikace RemoteApp prostřednictvím webového rozhraní TS Web Access</b>	<b>333</b>
<b>Spuštění aplikace RemoteApp pomocí souboru RDP</b>	<b>334</b>
<b>Vytvoření instalačního balíčku MSI</b>	<b>335</b>
<b>Implementace jednotného přihlášení (Single Sign-On)     pro použití s terminálovými službami</b>	<b>336</b>
<b>Nasazení služby role Brána TS (TS Gateway)</b>	<b>338</b>
<b>Konfigurace Brány TS</b>	<b>338</b>
<b>Nasazení certifikátu SSL pro bránu TS</b>	<b>339</b>
<b>Vytvoření zásady autorizace připojení a zásady autorizace prostředků</b>	<b>341</b>
<b>Konfigurace klienta pro připojení pomocí Brány TS</b>	<b>344</b>
Instalace a konfigurace webového serveru IIS	344
<b>Instalace role Webového serveru</b>	<b>344</b>
<b>Přidání nové vazby k existujícímu webu</b>	<b>345</b>
<b>Vytvoření nového webu</b>	<b>347</b>
<b>Vytvoření webové aplikace</b>	<b>348</b>
<b>Vytvoření virtuálního adresáře</b>	<b>349</b>
<b>Nasazení zabezpečené komunikace SSL – získání certifikátu</b>	<b>351</b>
<b>Nasazení zabezpečené komunikace SSL – nasazení certifikátu</b>	<b>353</b>
Instalace a konfigurace služby FTP	354
<b>Instalace služby role Služba publikování FTP (FTP 6)</b>	<b>355</b>
<b>Vytvoření a konfigurace nového serveru FTP</b>	<b>355</b>
<b>Instalace Microsoft FTP Publishing Service 7.5 for IIS 7.0</b>	<b>357</b>
<b>Vytvoření a konfigurace serveru FTP 7</b>	<b>357</b>
Instalace a konfigurace služby SMTP	359
<b>Instalace serveru SMTP</b>	<b>359</b>
<b>Vytvoření nového virtuálního serveru SMTP</b>	<b>359</b>

## KAPITOLA 8

**Zabezpečení operačního systému a sítě 361**

Konfigurace Brány firewall systému Windows	361
<b>Vytvoření příchozího pravidla</b>	<b>364</b>
<b>Vytvoření odchozího pravidla</b>	<b>368</b>
<b>Protokolování síťového provozu</b>	<b>369</b>
Auditování událostí	371
<b>Povolení auditování</b>	<b>371</b>

<b>Audit přístupu ke sdílené složce</b>	<b>373</b>
<b>Audit přístupu k adresářové službě</b>	<b>375</b>
<b>Využití nových možností auditu přístupu k adresářové službě a práce s příkazem Auditpol</b>	<b>377</b>
Nasazení infrastruktury veřejných klíčů (PKI) a certifikačních služeb Active Directory	378
<b>Instalace role Active Directory Certificate Services</b>	<b>379</b>
<b>Vygenerování uživatelského certifikátu prostřednictvím webového rozhraní</b>	<b>381</b>
<b>Povolení automatického přidělování certifikátů</b>	<b>382</b>
<b>Získání certifikátu počítače</b>	<b>383</b>
Zabezpečení síťového provozu pomocí protokolu IPSec	384
<b>Nasazení zabezpečené komunikace prostřednictvím zásad skupiny</b>	<b>385</b>
<b>Nasazení zabezpečené komunikace pomocí Pravidel zabezpečení připojení</b>	<b>388</b>
<b>Vytvoření nové zásady protokolu IPSec</b>	<b>390</b>
Nasazení systému Network Access Protection	394
<b>Instalace role serveru NPS</b>	<b>394</b>
<b>Konfigurace serveru NAP pomocí průvodce</b>	<b>395</b>
<b>Povolení architektury NAP na oboru DHCP</b>	<b>397</b>
<b>Nastavení tříd DHCP pro použití s architekturou NAP</b>	<b>398</b>
<b>Vytvoření validátoru stavu systému</b>	<b>399</b>
<b>Konfigurace klienta systému NAP prostřednictvím zásad skupiny</b>	<b>400</b>
KAPITOLA 9	
<b>Seznámení s operačním systémem Windows Server 2008 R2</b>	<b>403</b>
Nové vlastnosti	403
Instalace a základní konfigurace operačního systému	405
Správa Active Directory	406
<b>Obnova smazaných objektů</b>	<b>408</b>
<b>Použití Best Practices Analyzeru</b>	<b>410</b>
<b>Omezení spouštění aplikací pomocí zásad AppLockeru</b>	<b>412</b>
Novinky v souborových službách	415
<b>Vytvoření nové úlohy správy souborů</b>	<b>415</b>
<b>Rejstřík</b>	<b>419</b>



# Poděkování autora

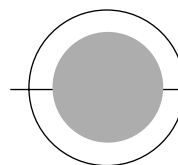
Bývá takovým zvykem, že jistou nefinanční formou odměny autorovi za napsání knihy je, že se mu dostane prostoru čítajícího jedné strany, kde může vyjádřit svůj vděk tomu, komu uzná za vhodné. I já bych zde tak rád učinil, i když jsem si vědom toho, že tato kniha není završením celoživotní práce a není tudíž zcela namísto děkovat tisícovce lidí, kteří nemají s touto knihou nic společného. Někteří z nich však ke zdárnému dokončení díla přispěli přímo či nepřímo, jiní mi zase museli v průběhu psaní ledacos odpustit a tolerovat.

Rád bych tedy na tomto místě poděkoval následujícím osobám:

- Svě matce Libuši za její obětavou, a vzhledem k nulové návratnosti investic, patrně i nezištnou podporu a péči. Ono to tak navenek asi moc nevypadá, ale všeho, co pro mne udělala, si moc vážím a mám ji za to rád.
- Přítelkyni Tereze, která ač nevím proč, snáší se mnou mé IT i jiné patálie již přes dva roky a podporuje mne v každé blbosti, kterou zrovna vymyslím. Nebo zkouším vymyslet. Zvláště v posledních týdnech dokončování knihy si užila své, tzn. nerudného nervózního chlapa, který nevychází z pracovny a když už ano, tak jen unaveně mumlá nesmysly, občas podnikne útok na ledničku a celkově je s ním ohromná zábava. Také děkuji jejím rodičům za pomoc v mnoha situacích.
- Panu redaktoru Liboru Páclovi, který mi dal šanci tuto knihu napsat a který toho asi v následujících měsících hořce litoval. Patří mu můj obdiv a vděk za to, že mne jako autora po psychologické stránce zvládnul, uměl motivovat a usměrňovat. Být na jeho místě, tak se zastřelím (myslím mne, ne jeho).
- Mgr. Romanu Fryšovi za odbornou pomoc a asistenci při dokončování knihy.
- PhDr. Romanu Hytychovi za to, že mi ukázal nové možnosti, a přesvědčivě mi vysvětlil, že na to, aby byl člověk obstojný „ajťák“, nemusí být úplný magor, který ignoruje okolní svět a realitu.
- Martinu Trtílkovi za „beta testing knihy“ a podnětné nápady i kritiku. Držte se toho co děláte, děláte to výborně!
- Aleně Kolovrátníkové za pomoc při finálních kontrolách textu a úpravě a kontrole doprovodného CD, kdy na to na rozdíl ode mne ještě viděla.
- Martinu Benešovi za to, že vytvořil krásné rozhraní k doprovodnému CD (ještě o tom v okamžiku psaní tohoto poděkování neví) a i za další poskytnutou pomoc, kterou zvládnul vždy s drtivou rychlostí, kvalitou a profesionalitou.
- Paní Stanislavě Kratochvílové, která se mi stará o účetnictví a při mé skleróze a roztržitosti také o spoustu dalších věcí nad rámec povinností.

- Petru Bohumelovi ze školicího střediska Prioris, že mne několik týdnů před dokončením knihy, kdy mi v poněkud nevhodný okamžik zlobila výpočetní technika, nenechal ve štychu a za cenu značných obětí mne vybavil luxusním hardwarem, na kterém byla radost pracovat a který mi konečně umožnil pracovat svižněji.
- Radku Havelkovi, Liboru Šromovi, Petru Slavíkovi a dalším lidem ze školicího střediska PCDIR za pomoc při řešení mnoha standardních i nestandardních problémů.
- Paní Marii Janouchové ze školicího střediska Digi-Trade a jejím kolegům za podnětnou spolupráci a vstřícnost.
- Aleně Hosové, jejímu manželovi Pepíkovi a jejich rodinné kamarádce Zdeňce Liškové za pomoc vždy v pravou chvíli a trpělivost vždy, když jí bylo zapotřebí (což bylo pokaždé).

*Martin Babarík*



# Úvod

---

## Komu je kniha určena

Jestliže čtete tento úvod, nacházíte se zřejmě v jedné z následujících situací:

- Stojíte v knihkupectví a přemýšlíte, zda vám tato kniha může v něčem pomoci nebo jestli v ní najdete nějaké užitečné informace. V tomto případě si prosím pozorně přečtěte úvod, kde je popsáno, co v této knize najdete a co nikoliv.
- Chystáte se implementovat operační systém Windows Server 2008, máte o něm jen kusé informace a chcete vědět, co všechno vás může při nasazení a správě tohoto operačního systému potkat. Pokud je tomu tak, tato kniha by ve vaší knihovničce administrátora, technika nebo IT manažera neměla chybět. Bude vám vždy k dispozici jako pohotová příručka, kde bez zbytečných okolků a zdlouhavého čtení najdete řešení, které hledáte.
- Operační systém Windows Server 2008 již používáte, získali jste už určité znalosti a zkušenosti, ale přesto jste občas zaskočeni tím, jak se nový operační systém chová nebo si nejste jisti tím, jak provést nějaký konkrétní postup, kam zmizelo vaše oblíbené tlačítko nebo průvodce, apod.

## Co v knize najdete a nenajdete

Jak už název publikace napovídá, kniha obsahuje sbírku hotových řešení, která se týkají nasazení a správy operačního systému Windows Server 2008. Najdete zde tedy velké množství popisných (a je-li to zapotřebí, tak i ilustrovaných) návodů pro různé administrativní úkony. Kniha *Microsoft Windows Server 2008 Hotová řešení* je další publikací z úspěšné řady „Hotová řešení“ a její rozsah i obsah je tak do jisté míry dán tradicí této knižní řady.

Kniha není vyloženě určena k tomu, aby si s ní čtenář sedl do křesla, nechal se unášet dějem (on tady mimochodem žádný není) a přečetl ji od první po poslední stranu. Kniha je určena především IT odborníkům, administrátorům a konzultantům, kteří ke své práci nebo zábavě (ano, i správa serveru je někdy zábava) chtějí mít po ruce pohotovou referenční příručku, kde najdou konkrétní postup popsaný od začátku do konce bez toho, aniž by museli číst všechny související informace napříč kapitolami.

Cílem této publikace není poskytnout úplné a komplexní informace o operačním systému Microsoft Windows Server 2008, ani zasvětit čtenáře do tajů administrace a poskytnout vyčerpávající teoretický výklad. Naopak – do jisté míry se předpokládá, že čtenář této knihy má alespoň základní znalosti administrace operačních systémů Microsoft Windows Server 2000

nebo 2003, má přinejmenším povrchní znalost popisovaných technologií a služeb a spíše než otázky „co“, případně „proč“ si klade otázku „jak“.

Na druhou stranu nepředpokládám, že čtenář knihy je expertem v oboru a nesnažím se učinit knihu nečitelnou a nepoužitelnou širší veřejnosti. Hotová řešení jsou poskytnuta co nejsrozumitelnější formou a tam, kde je to nutné, je poskytnuto i vysvětlení dané akce nebo objasnění různých souvislostí.

Pokud jste v oboru úplným začátečníkem, není to ničemu na překážku. Jste-li k nějakému vzdělávání motivováni, můžete tuto knihu do značné míry využít jako učebnici operačního systému Windows Server 2008, projít si uvedené postupy třeba ve virtuálním prostředí a získat tak větší přehled a hlavně jistotu v daných oblastech.

## Výběr témat

---

Tato kniha začala pomalu vznikat krátce poté, co se operační systém Windows Server 2008 vyvinul do své závěrečné podoby. Určitě tedy nemohu říci, že bych začal psát po pětileté rutinní práci s tímto operačním systémem. Měl jsem však v té době již nezanedbatelnou praxi s administrací serverových operačních systémů jako takových a také s vedením školení v této oblasti.

Seznam témat jsem tedy sestavil na základě zkušeností, které jsou řekněme „platform-independent“. Znalosti operačního systému se téměř vždy dají shrnout do několika mála okruhů a je vcelku jedno, zda se jedná o žhavou novinku nebo 15 let starý systém. Tyto okruhy jsem tedy použil jako základ osnovy, ve které dominuje následujících osm oblastí:

- Obecné seznámení s nástroji pro správu a možnostmi správy
- Instalace operačního systému a základní konfigurace
- Správa síťové infrastruktury a všeho, co s ní z pohledu operačního systému souvisí
- Nasazení a správa Active Directory
- Nasazení a správa souborových a tiskových služeb
- Sledování a údržba systému
- Poskytování internetových a intranetových služeb
- Zabezpečení systému a síťové komunikace

Tyto oblasti považuji za základní pilíře správy operačních systémů firmy Microsoft a není se tedy co divit, pokud vám znějí povědomě a domníváte se, že „to už tu všechno bylo“. Ano, bylo a zřejmě ještě nějaký čas bude. Alespoň v publikacích, které se zabývají správou obecně a nejsou vyloženy dedikovaný některé specifické oblasti správy.

Kromě osmi uvedených témat zde přibyl ještě jedno, jehož účelem je přiblížit čtenáři novou verzi operačního systému Windows Server 2008, tedy Windows Server 2008 R2. Mezi těmito dvěma verzemi není tak markantní rozdíl jako mezi verzemi 2003 a 2008. Uvedená kapitola je tedy spíše jen takovou „ochutnávkou“ verze R2.

Rád bych zde rovněž okomentoval rozsah, který byl věnován jednotlivým tématům. Je mi bohužel jasné, že do této publikace nedostanu úplně všechna hotová řešení, která by někoho mohla zajímat. Zrovna tak chápu, že někdo mi bude zazlívát detailní popisy postupů v jedné oblasti a přílišnou stručnost až strohost v oblasti jiné.

Snažil jsem se však, abych se prostorem, který byl věnován jednotlivým tématům, „trefil“ do potřeb jakéhosi fiktivního, statisticky zprůměrovaného administrátora. Vycházel jsem při tom ze zkušeností získaných zejména při školení, kde jsem měl skvělou příležitost si utvořit představu o tom, co běžný administrátor umí, co by umět chtěl, co by umět měl, ale nechce se mu do toho, nebo co by umět měl, ale ani neví, že to existuje.

Doufám tedy, že čtenář zde najde alespoň většinou tu informaci, kterou právě potřebuje a nebude muset kvůli provedení nějakého úkonu prohledávat tuny jiné literatury (i když občas k tomu zcela jistě dojde).

Situaci při psaní této knihy jsem měl o to těžší, že na trhu již několik let existuje kvalitní kniha Patrika Maliny *Windows Server 2003* z edice „Hotová řešení“. Pan Malina jako již tradičně nasadil laťku poměrně vysoko a já se nesnažím mu nějakým způsobem konkurovat, nebo jej překonávat.

Jeho knihu jsem přečetl před několika málo lety z pozice „uživatele“ této knihy a při psaní své vlastní jsem se naopak bedlivě vyhýbal tomu, abych se jí nechával „inspirovat“. Je mi jasné, že čtenář znalý obou knih zde najde mnoho podobností, ať už ve formě skladby témat, jejich rozsahu, jednotlivých řešení a aniž bych takové srovnání provedl, je možné, že jsme některé postupy popsali velmi totožně.

Účelem posledních dvou odstavců je ujistit čtenáře, že tato kniha není jen jakýmsi „upgradem“ verze týkající se Windows Server 2003, ale vznikla zcela nezávisle a „od nuly“. Při tvorbě jsem vycházel ze svých vlastních znalostí a zkušeností a snažil jsem se poskytnout alespoň nepatrně odlišný pohled na některá témata.

## ***Obsah doprovodného CD***

V tomto směru se jedná o poněkud pionýrský počín, kdy jsme se rozhodli, že ke knize přiložíme i videozáznamy demonstrující některé složitější postupy.

Ve vzduchu však před námi viselo značné dilema, a to jakou formu prezentace pro tyto videozáznamy pojmout.

Sám jsem zhlédl několik hodin různých videokurzů převážně z produkce amerických firem a byl jsem si tedy vědom několika základních negativ, která takto prezentované informace provázejí.

Buď autor při hlasovém komentáři mluví monotónně (v tom jsem obzvlášť dobrý) a aby divák neusnul, stojí jej to značné množství energie a trpělivosti. Navíc ne každému vyhovuje dané tempo ukázek. Někomu přijde hlemýžďí, někomu zase nepřehledně rychlé a zběsilé.

Druhou variantou je, že komentátor je nesnesitelně hyperaktivní, brebentí a aby toho již tak zmatený divák neměl málo, občas při své kadenci 200 slov za minutu do výkladu zakomponuje pokus o vtip, historku ze života apod. Což také nemusí sednout každému.

Videozáznamy přiložené k této knize fungují jinak. Rozhodli jsme se pro variantu „němý film“, kde nebude žádný hlasový doprovod, ale místo něj se budou na obrazovce ve vhodný okamžik objevovat „bublíny“ obsahující vysvětlení daného kroku. V okamžiku, kdy se bublina objeví, je přehrávání pozastaveno, dokud uživatel neklepne na tlačítko myši. Sami si tak můžete sto procentně řídit tempo.



Toto řešení má také jistý psychologický základ. V okamžiku, kdy člověk sleduje namluvený videozáznam, nemusí mu nutně věnovat soustředění a pozornost. Víme, jak to chodí: člověk se po chvíli začne tak trošku nudit, poslouchat jedním uchem a po půl hodině už záznam nevnímá vůbec.

Díky systému pozastavování přehrávání se dá předpokládat, že divák je v dané chvíli plně soustředěn na dění na obrazovce a odnese si tak z vypozerovaných informací maximum toho podstatného a důležitého, neboť nebude muset plýtvat svou pozorností a časem na to, aby odlišil zrna od plev.

Snad se vám tedy budou uvedené postupy líbit a pokud budete mít nápady na jejich vylepšení nebo zcela jiný koncept, neváhejte kontaktovat vydavatelství Computer Press nebo autora samotného.

Videokurzy jsou v knize označeny ikonou kamery.



## Několik slov o operačním systému Microsoft Windows Server 2008

Microsoft na nové generaci serverového operačního systému pracoval poměrně dlouho a je třeba říci, že to jde poznat. Microsoft Windows Server 2008 je mimořádně výkonný, všestranný a vyspělý operační systém, který obstojí v konkurenci jiných platforem a v mnoha ohledech je doslova roznese na kopytech.

V čem je tak mimořádný nebo co může být důvodem k jeho nasazení? Odpověď je velice jednoduchá: to, co fungovalo, zůstalo zachováno. To, co vyžadovalo opravu, bylo opraveno. A tam, kde byl prostor k vylepšení, k vylepšení skutečně došlo.

Po první instalaci a spuštění tohoto systému mohou změny od předchozích verzí vypadat pouze kosmeticky, ale zdání klame. Pojďme se podívat na některé zásadní novinky a vylepšení, která v novém operačním systému najdeme:

- Nová architektura jádra operačního systému zajišťující vyšší stabilitu a robustnost. Ano, uznávám, tuto větu jsme slyšeli již mnohokrát a zní spíše jako citace z nějakého propagačního letáku. Ale tentokrát tomu tak skutečně je.
- Možnost nainstalovat operační systém v režimu Server Core, kdy systém nemá grafické rozhraní, místně je spravován pouze pomocí příkazového řádku a vzdáleně se dají použít běžné administrativní nástroje s grafickým uživatelským rozhraním. Výhoda je zřejmá: nižší požadavky na výkon a menší konzumace prostředků serveru, při současném zvýšení zabezpečení (absence grafického uživatelského rozhraní statisticky i prakticky snižuje počet chyb v zabezpečení a také zmenšuje tzv. plochu útoku, což je pomyslná kolekce vlastností operačního systému, které mohou být zneužity případným útočníkem).
- Možnost instalace doménového řadiče v režimu pouze pro čtení.
- Efektivnější a jednodušší správa s využitím nových integrovaných nástrojů.
- Nativní podpora skriptovacího prostředí PowerShell.
- Možnost individuálního nastavení zásad hesla pro různé skupiny uživatelů v jedné doméně Active Directory.
- Možnost nasazení adresářových služeb bez nutnosti instalace doménového řadiče (Active Directory Lightweight Directory Service – náhrada aplikačního módu ADAM).



- Active Directory nyní běží jako samostatná služba. Odpadá tedy nutnost někdy nekonečného restartování doménových řadičů.
- Integrovaná virtualizace operačních systémů pomocí technologie Hyper-V.
- Služby pro správu digitálních dokumentů v rámci organizace (Active Directory Rights Management Service).
- Zcela přepracovaný a detailně konfigurovatelný firewall.
- Lepší ochrana operačního systému proti nechtěným zásahům způsobeným omylem lidského faktoru (např. smazání objektu v Active Directory).
- Služba IIS 7, která od dob svých předchůdců prošla skutečně razantními změnami.

Tento výčet by mohl pokračovat ještě dlouho, ale propagace operačního systému není účelem tohoto úvodu. Účelem bylo vás, čtenáře této knihy, informovat o tom, co zde najdete a také vám popřát, aby vám byla užitečná.