# 14. Virtualizace a virtuální PC

## Virtualizace

Označení postupů, technik a prostředků, které umožňují v počítači přistupovat k dostupným zdrojům jiným způsobem, než fyzicky. Virtualizované prostředí může být mnohem snáze přizpůsobeno potřebám uživatelů, snáze se používat, případně před uživateli zakrývat pro ně nepodstatné detaily (jako např. rozmístění hardwarových prostředků). Virtualizovat lze na různých úrovních, od celého počítače, po jeho jednotlivé hardwarové komponenty (CPU, RAM…), případně pouze softwarové prostředí (OS).

## Emulace

Emulátory se všeobecně odkazují na schopnost počítačového programu nebo konkrétního zařízení napodobit, emulovat jiný program či zařízení. Typický příklad lze najít ve světě tiskáren. Mnoho tiskáren je navrženo tak, aby dokázaly napodobit tiskárny společnosti Hewllet-Packard, protože jsou popsané ve velkém počtu programů. Pokud tiskárny jiných výrobců dokáží emulovat tiskárny HP, jsou schopné tisknout z programů, které by s těmito tiskárnami normálně nepracovaly.

Emulátor nemusí vystupovat jen jako software, který napodobuje, emuluje jiné prostředí, ale také jako hardwarový emulátor. Jedná se například o DOS kompatibilní karty, které se vyskytly v dřívějších verzích Macintoshů pod názvem Centris 610 nebo Performa 630. Díky tomu byly majitelé takového počítače schopni spouštět programy známé z PC.

### Výhody

Emulátory zachovávají celkový vzhled i chování původní aplikace. To je stejně důležité jako samotná data takovýmto způsobem zobrazená.

Počáteční náklady na vývoj nebo pořízení emulátoru mohou být vyšší, ale s postupem času se taková investice rychle vrátí (nákup nových verzí aplikací …).

Emulátory zároveň snižují počet hodin strávených na migraci starších souborů do nových aplikací. Jakmile je emulátor naimplementován, využívá se pro všechny soubory a uživatel s nimi pracuje rovnocenně.

Mnoho emulátorů bylo vydáno pod GNU General Public License jako open source prostředí, což umožňuje významným způsobem minimalizovat náklady na pořízení, ale zároveň umožňuje využití ve velkém.

V zábavním průmyslu umožňují emulátory spouštění videoher, které jsou určeny pro konkrétní typy platforem, spouštět například na PC.

### Nevýhody

Největší překážkou emulace se často uvádí duševní vlastnictví. Mnoho dodavatelů technologií se snaží při vývoji programu rozšířit své místo na trhu a současně s tím stávající programy rozšiřovat a vylepšovat tak, aby zůstaly konkurenceschopné. Tito dodavatelé často vydávají takzvaný proprietární software, který jim zaručí výsadní postavení na trhu. Díky tomu je ale schopnost pozdější emulace jejich produktu znemožněna, protože produkt je chráněn licencí.

Autorské zákony ještě nepokročily do té podoby, aby emulaci proprietárního software dostatečně popsaly.

## Paravirtualizace

Samozřejmě plná virtualizace má svou cenu. 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 (především nabízí identický procesor a další periferie). Virtuální monitor totiž musí kompletně odstínit virtuální počítač od jakékoliv možné změny hardware. Toho dosáhne tak, že emuluje fyzické vybavení a většinu operací (včetně řady instrukcí procesoru, práce s pamětí, operace přístupu na disk a další) provádí ve vlastním software namísto, 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.

Za předpokladu, že se alespoň některé komponenty virtuálního a fyzického počítače shodují, pak se hovoří o paravirtualizaci. Ta se vyznačuje tím, že provádí jen částečnou abstrakci na úrovni virtuálního počítače, tj. nabízí virtuální prostředí, které je podobné tomu fyzickému, na kterém se virtuální počítač provozuje. Virtualizace v tomto případě není úplná, některé vlastnosti např. procesoru mohou být omezeny a operační systém může rozpoznat, že běží ve virtuálním prostředí. Na druhou stranu skutečnost, že virtuální a fyzický hardware se příliš neliší, umožňuje, aby virtuální počítač v maximální míře využíval vlastnosti základního fyzického prostředí (nemusí emulovat všechny komponenty virtuálního počítače).

Paravirtualizace je široce využívána při tvorbě virtuálních prostředí nad procesory Intel (AMD). VMWare workstation a Xen patří mezi neznámější systémy, které jsou postaveny na paravirtualizaci. Základní principy paravirtualizace si lze představit na (zjednodušeném) modelu, který používá právě prostředí Xen.

Prvním problémem, který je třeba vyřešit, je virtualizace procesoru. Každý procesor pracuje alespoň ve dvou různých režimech – privilegovaném, který je přístupný pouze jádru operačního systému, a 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 (přímý přístup na disk, složitější operace s virtuální pamětí…). Pokud se ale počítač virtualizuje, je zapotřebí 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, v případě paravirtualizace je to však mnohem složitější.

Virtuální monitor musí běžet na nejvyšším stupni ochrany. Na stejné úrovni však nemůže automaticky běžet operační systém, protože by mohl ovlivnit stav virtuálního monitoru. Jednou z možností je pozměnit kód operačního systému tak, že nebude provádět žádnou operaci, pro jejíž provedení je třeba oprávnění té nejvyšší úrovně. Provedení instrukce se změní ve volání příslušné funkce virtuálního monitoru, který nejprve zkontroluje, zda je operace povolena a následně ji provede tak, aby změnila stav virtuálního, nikoliv fyzického počítače. Nemalý problém však budou v tomto přístupu dělat instrukce čtení paměti. Jádro operačního systému předpokládá, že má přímý přístup k libovolné části fyzické paměti, to však samozřejmě v případě virtuálního počítače není možné. Protože nelze předem poznat, zda konkrétní operace čtení z paměti bude přistupovat k privilegovaným údajům, musely by se nahradit v operačním systému všechny instrukce čtení – tím se ale začne velmi nepříjemně přibližovat k plné virtualizaci. Další problém spočívá v ochraně operačního systému před běžícími uživatelskými programy. Pokud by existovaly 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 (okruhy; **rings**). Na nejvyšším stupni ochrany (ring 0) běží operační systém, uživatelské programy běží s nejnižším stupněm ochrany (ring 3). Ostatní stupně se běžně nevyužívají. Pokud se použije paravirtualizace, pak virtuální monitor pracuje na nejvyšším stupni ochrany (okruhu 0). Operační systém virtuálního počítače se posune o jeden stupeň (do okruhu 1), aplikační programy běží stále s nejmenší ochranou. Operační systém má tak stále vyšší úroveň ochrany než aplikační programy, na druhé straně už nemůže provádět operace, které vyžadují plně privilegovaný přístup. Úrovně ochrany však lze využít i místo výše zvýšené modifikace privilegovaných instrukcí – operační systém bude ve virtuálním počítači provádět všechny instrukce, pokud však bude chtít provést "zakázanou" operaci (takovou, na kterou teď nemá dostatečná oprávnění), pak dojde k přerušení a řízení převezme virtuální monitor. Ten operaci zkontroluje a provede ji tak, aby správně změnila stav virtuálního počítače. Není v principu třeba měnit operační systém, většina instrukcí běží přímo, pouze privilegované instrukce jsou výrazně pomalejší, protože je musí provést virtuální monitor. Operační systém však může zjistit, že běží ve virtuálním prostředí, protože může mít i na úrovni 1 možnost číst některé části paměti, které jsou ve virtuálním počítači jiné než ve fyzickém. Pro paravirtualizaci je proto třeba modifikovat některé součásti operačního systému, změny jsou však malé a dobře lokalizovatelné (zvlášť dobře je pak možné provést tyto změny u operačních systémů, k nimž jsou k dispozici zdrojové kódy; i proto začala být tak oblíbená (para)virtualizace v prostředí Linuxu).

Přístup k hardware je v prostředí Xen zajišťován vrstvou virtuálního monitoru (Virtual Machine Monitor, VMM). Nad touto vrstvou jsou pak vytvářeny virtuální počítače (Virtual Machines, VM). Jeden z těchto virtuálních počítačů má speciální postavení – v terminologii Xenu se nazývá Doménou 0 (Dom 0). Operační systém, který běží v tomto virtuálním počítači, má přímý přístup k rozhraní virtuálního monitoru, může tedy definovaným způsobem měnit jeho stav a může vytvářet a rušit ostatní virtuální počítače běžící nad VMM. Další zajímavou vlastností Xenu (opět související s paravirtualizací) je to, že může konkrétnímu virtuálnímu počítači přímo zpřístupnit konkrétní rozhraní.

V jednom z virtuálních počítačů běží uživatelský program, který intenzivně komunikuje s jiným počítačem prostřednictvím počítačové sítě. Pokud používá virtuální síťovou kartu, pak její propustnost je omezena a velmi zatěžuje procesor. Pokud ale příslušnému virtuálnímu počítači po dobu běhu tohoto uživatelského programu se přímo exportuje rozhraní na fyzickou kartu, pak může síťová komunikace probíhat plnou rychlostí, kterou podporuje příslušný hardware. Samozřejmě v takovém případě kartu může používat pouze tento virtuální počítač, to ale nemusí být na závadu (fyzický počítač může mít více síťových rozhraní, ostatní virtuální počítače pak sdílí ta ostatní).

Přestože má paravirtualizace řadu výhod proti plné virtualizaci, potřebuje určité modifikace operačních systémů, což komplikuje její nasazení (zejména u proprietárních operačních systémů) a vede k určité neefektivnosti. Intel proto v poslední době zavedl další systém podpory virtualizace v podobě 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. Operační systémy ve virtuálních počítačích není třeba modifikovat, přitom zůstávají základní výhody paravirtualizace (přímé vykonávání instrukcí virtuálního počítače fyzickým procesorem).

## Plná virtualizace

Pokud se postupuje tímto způsobem, virtualizují se důsledně všechny součásti počítače. V takovémto případě se nabízí prostředí, v němž běžící operační systém nemůže žádným způsobem poznat, že nemá přístup k fyzickému technickému vybavení. Operační systém ani aplikační programy nepotřebují žádné modifikace. 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. To má samozřejmě řadu výhod – lze virtuální prostředí navrhnout tak, aby vyhovovalo požadavkům (velikost paměti, typ procesoru, typ, kapacita disku…). Programy jsou rovněž nezávislé na konkrétním technickém vybavení, jeho změna nemá na virtuální prostředí vliv (samozřejmě kromě výkonnostních charakteristik).

U plné virtualizace nemusí existovat žádná jednoduchá vazba mezi virtuálním prostředím a konkrétním hardware, na němž je virtuální počítač provozován. To umožňuje plnou přenositelnost. A následně je lze přenést na počítače vybavené jiným procesorem, aniž by bylo nutné provést jedinou úpravu na úrovni virtuálního počítače. Podobně lze vytvořit virtuální počítač vybavený procesorem, který je teprve ve vývoji – návrh a ladění operačního systému a aplikací tak může probíhat paralelně s vývojem vlastního hardware.

Mezi profesionální systémy, které nabízí plnou virtualizaci počítačů s procesorem Intel, patří Microsoft Virtual Server a VMWare ESX ServerTM.