

Virtualizace výpočetního prostředí – přínosy

Luděk Matyska, ÚVT MU

Virtualizace výpočetního prostředí, jejíž všeobecné koncepty i konkrétnější technické informace byly obsahem předchozích dvou článků, není jen zajímavou oblastí výzkumu, ale má jednoznačný praktický přínos. V prvním přiblížení nám virtualizace zvyšuje počet počítačů, se kterými můžeme při plánování počítat. Mámeli zajistit provoz čtyř služeb (např. DNS server, webový server, mail server a ftp server), doporučení odborníků platné před návratem virtualizace říkala, že potřebujeme čtyři počítače, každý právě pro jednu službu. Jedině tak jsme mohli zajistit prostředí optimální pro každou ze služeb a současně garantovat její bezpečnost. Virtualizace umožní opět každou službu uzavřít v „jejím“ počítači, avšak virtuálním. A všechny tyto virtuální počítače pak můžeme spustit na jednom fyzickém, čímž ušetříme nejen prostředky na nákup tří počítačů, ale i náklady na jejich provoz (elektřina, chlazení) a správu.

Toto naivní 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 nám však umožní řešit efektivně i tento problém. Představme si, že místo jednoho použijeme 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, můžeme s co nejmenší časovou ztrátou spustit na tom zbývajícím počítači, aniž bychom jakkoliv zasáhli do na něm již běžících služeb. Dojde sice k určitému poklesu výkonu všech čtyř služeb, ale jsme schopni všechny služby provozovat s minimálním přerušením. A zejména nijak nemusíme měnit konfigurace jednotlivých služeb a jejich počítačů – řešení je v podstatě ekvivalentní tomu, že máme stále k dispozici záložní

fyzický počítač.

Virtualizace nám tak nejen umožnila snížit počet fyzických počítačů, ale současně velmi efektivně reagovat na případné výpadky bez nutnosti držet si záložní počítače. Držíme si pouze záložní *virtuální* počítače a dokud máme alespoň jeden fyzický počítač, jsme schopni zajistit funkci všech poskytovaných služeb.

Tento přístup můžeme dále rozšířit. Namísto pevného mapování virtuálních počítačů na fyzické můžeme rozhodovat dynamicky, zpravidla podle aktuální zátěže. Již v našem modelovém případě dvou počítačů a čtyř služeb můžeme třeba v době vyšší zátěže webového serveru jeho virtuální počítači přidělit jeden fyzický stroj a ostatní tři virtuální počítače (a jejich služby) ponechat na druhém. Při poklesu zátěže webového serveru pak můžeme nějaký z těchto tří virtuálních strojů přesunout a zvýšit tak poskytovaný výkon všech tří služeb.

V předchozím odstavci jsme použili obrat *přesun virtuálního počítače*. To je další oblast, ke nám virtualizace nabízí dříve (téměř) nedostupné možnosti. 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 můžeme virtuální počítač „uklidit“, tj. vzít veškerou paměť, kterou používá, a zkopírovat ji na disk. Takto vytvoříme *obraz* virtuálního počítače ve stavu, který odpovídá hibernaci operačního systému (bez virtualizace). Proti hibernovanému stavu, který zpravidla nelze spustit jinde než na tom počítači, kde došlo k hibernaci, můžeme virtuální obraz přesunout na jiný počítač a spustit jej tam – přesunuli (migrovali) jsme tak celý virtuální počítač na jiný fyzický, aniž by jakkoliv došlo k narušení vnitřního stavu virtuálního počítače. Samozřejmě reálná situace je komplikovanější kvůli vstup/výstupním operacím. Systém souborů můžeme přesunout též (s tím přesuneme i otevřené soubory), skutečný problém je však se sítíovou

komunikací. Pokud virtuálnímu počítači odebereme procesor, ztratí přirozeně schopnost přijímat data - pokud mu nějaký jiný (virtuální) počítač pošle paket, ten paket nemůže být přijat. 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 bezztrátovost síťové komunikace. Samozřejmě zůstává nebezpečí, že druhá strana čeká na odpověď a pokud ji nedostane v nějakém konečném časovém intervalu, spojení přeruší. Toto nebezpečí můžeme 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 máme k dispozici obraz virtuálního stroje, nemusíme jej pouze přesouvat, ale můžeme jej i kopírovat. Tímto způsobem si můžeme udělat *vzorovou instalaci* (gold image) a kdykoliv budeme potřebovat výpočetní prostředí s těmito parametry, vytvoříme kopii vzorové instalace virtuálního počítače a tu spustíme na vhodném fyzickém počítači. Kromě rychlosti nám tento přístup zejména zaručuje naprostou identitu všech spuštěných strojů. Dokonce si můžeme dovolit konkrétní virtuální počítač po použití (např. realizaci konkrétního výpočtu) zrušit a příští výpočet spouštět opět v „čistém“ prostředí původní vzorové instalace. Můžeme tak minimalizovat riziko ovlivnění následných použití virtuálního počítače (např. problémy způsobené chybnou implementací nějakých funkcí jádra, které mohou vést k postupnému vyčerpání paměti, zániku některých funkcí atd.).

Možnosti, které nabízí virtualizace, však zdaleka nejsou omezeny jen tím, co jsme prozatím diskutovali. Některé z těch pokročilejších si uvedeme dále.

Výše uvedený způsob migrace virtuálního počítače má charakter „ulož a přesuň“ (store and

forward). Možná je ale i tvorba kopie v reálném čase, kdy začneme kopírovat běžící virtuální počítač a dosáhneme stavu, kdy na dvou fyzických strojích máme 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). A ve vhodném okamžiku se přepne řízení a nově vytvořená kopie převezme aktivitu a původně 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 můžeme použít i k velmi významné *úspoře spotřeby elektrické energie*. Použijme opět původní příklad, ale při startu služeb spustíme všechny čtyři virtuální počítače na jednom fyzickém a druhý fyzický buď ponechme úplně vypnutý nebo jej držíme v nějakém energeticky úsporném režimu. Dokud bude stačit výkon prvního fyzického počítače, pouze ten spotřebovává energii (a generuje teplo). Teprve při jeho přetížení aktivujeme druhý počítač. Tento model můžeme rozšířit na více služeb, resp. jejich kopie a tím dosáhnout 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 nemusíme vytvářet jen když jej chceme migrovat, během výpočtu můžeme pravidelně vytvářet snímky stavu (checkpoints) a ty ukládat. Dojde-li z nějakého důvodu ke zhroucení počítače, můžeme aktivovat nějaký z předchozích snímků a výpočet dokončit s minimální ztrátou. Snímek celého virtuálního počítače nám poskytuje vyšší záruku spolehlivosti proti situaci, kdy se snažíme vytvořit pouze snímek (checkpoint) běžící aplikace (nemusíme speciálně kopírovat

vnitřní stavy struktur jádra operačního systému, ukládáme celý operační systém i s jádrem). S rostoucí rychlostí a zejména kapacitou disků nevádí vyšší režie tohoto přístupu (vytváříme snímek celého virtuálního počítače, jeho paměti a případně i systému souborů).

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 můžeme 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), tomu je 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. Způsoby použití zmíněné v tomto článku představují jen část již známých možností - nezmínili jsme např. vazbu na virtualizaci sítě, nové možnosti paralelních a distribuovaných výpočtů ve virtualizovaném prostředí - představují však určitý reprezentativní výsek a demonstrují, že s virtualizačními technologiemi i technikami jejich využití se budeme v budoucnosti stále více setkávat. Lze dokonce očekávat, že postupně

převážná většina výpočtů bude probíhat ve virtualizovaném prostředí a uživatelé nebudou příliš přicházet do přímého kontaktu s fyzickým prostředím. □