ÚVT MU

zpravodaj

Bulletin pro zájemce o výpočetní techniku na Masarykově univerzitě•prosinec 2007•roč. XVIII•č. 2

Federace identit aneb spolčení totožností

Daniel Kouřil, Martin Kuba, Martin Osovský, Radim Peša, Michal Procházka, ÚVT MU

Masarykova univerzita, stejně jako většina organizací, provozuje své interní webové informační systémy. Uživatelé, tj. zaměstnanci a studenti organizace, se do těchto aplikací přihlašují svými autentizačními údaji, kterými jsou obvykle jméno a heslo. Jedná se o standardní léty ověřená řešení, která v rámci jedné organizace svou funkcionalitou vyhovují.

Avšak v případě, že překročíme hranice jedné organizace, záhy narazíme na limity těchto řešení. Například pokud chceme provozovat webovou aplikaci dostupnou právě vybraným uživatelům různých vysokých škol, obvykle nezbude než pro všechny zúčastněné uživatele založit nové uživatelské účty včetně nového jména a hesla, u nichž nemáme možnost nijak využít žádné z údajů, které o uživatelích vedou jejich mateřské instituce. Nemluvě o tom, že nešťastným uživatelům přibude do sbírky další dvojice přihlašovacích údajů. Pokud se jedná o malý počet zúčastněných uživatelů, účty se jim metodou hrubé síly zřídí, protože jiná cesta prostě neexistuje. Ale pokud bychom chtěli například provozovat aplikaci dostupnout právě všem studentům medicíny v České republice, jednalo by se o úkol prakticky neřešitelný. A právě mimo jiné takovouto třídu úloh je velmi vhodné a ve výsledku i snadné řešit pomocí *federací identit* (anglicky *identity federation*, podle slovníku *spolčení totožností*).

V tomto článku popisujeme model federativních mechanismů pro autentizaci (ověření totožnosti) a autorizaci (povolení přístupu), který umožňuje oddělit správu uživatelů a jejich autentizaci od vlastní aplikace a standardizuje sdílení informací o uživatelích mezi organizacemi ve federaci. Aplikace tak mohou být jednodušší a zároveň poskytovat uživatelům pohodlné použití, protože uživatelé se mohou ve všech aplikacích autentizovat jedinou domovskou sadou přihlašovacích údajů. Zároveň mohou implementovat autorizaci založenou na aktuálních informacích o uživatelích, které jsou poskytovány z jejich domovských institucí. Údaje o uživatelích nejsou duplikovány pro účely jednotlivých aplikací a o jejich aktuálnost se stará ten nejpovolanější tj. domovská instituce.

Současné systémy nejčastěji řeší správu uživatelů a řízení jejich přístupu k poskytovaným službám každý zvlášť a nepočítají s jejich využitím v dalších systémech ani s možností využít data o uživatelích ze stávajících systémů provozovaných jinými organizacemi. Důsledkem této nezávislosti je nutnost registrovat všechny uživatele v databázi, která je součástí informačního systému. Pokud uživatel potřebuje využívat

více takto nezávislých systémů, tak se musí zaregistrovat do všech. Ke každému systému samozřejmě obdrží samostatné přihlašovací údaje, které jsou určené pouze pro přístup k tomuto systému a nelze je použít pro autentizaci k dalším systémům. Tato situace může vést až k faktickému oslabení bezpečnosti. Např. v případě, že autentizace je založena na použití hesla, lze předpokládat, že běžný uživatel bude používat stejné heslo pro přístup ke všem systémům. V případě kompromitování jednoho takového systému a prozrazení uživatelského hesla budou zranitelné i všechny systémy, které daný uživatel takto používá. Situace bude o to horší, že systémy jsou autonomní, nevědí o sobě a administrátoři nejsou informováni ani o kompromitaci jiného systému ani o tom, že byl používán také jejich uživatelem, a že tedy může být potřeba nasadit nějaká ochranná opatření.

Ve větších institucích si potřeba správy většího množství uživatelů a systémů vynutila využití nějakého systému pro centrální správu uživatelů, nejčastěji ve formě webového Single Sign-On řešení (WebAuth, CoSign, CAS, atd.). Na MU je možnost využití databáze uživatelů a hesel IS MU pomocí vlastního SSO řešení zvaného BCA Autentizace.

Obecnou nevýhodou těchto systémů je orientace výhradně na autentizaci (navíc v případě MU vždy řešenou na aplikační úrovni). Tyto systémy obvykle neposkytují standardní cestu pro přístup k dalším informacím o uživateli, které mohou být potřebné pro autorizaci (např. příslušnost ke konkrétní fakultě, předmětu, zda je student, učitel, neakademický zaměstnanec).

Dalším omezením je omezení působnosti pouze na lokální prostředí organizace. Uživatelé, kteří chtějí používat aplikaci provozovanou mimo MU, musí být vždy registrováni v koncovém systému a dostat (a spravovat) tak další autentizační data, například v naduniverzitních projektech. Podobně, pokud s aplikacemi na MU chce pracovat uživatel, který není registrován v IS MU, je nutné uživatele buď zavést do systému (se stejným problémem pro uživatelské pohodlí jako výše) nebo v horším případě řešit jeho přístup ad-hoc způsobem. Navíc v tomto případě nemáme reálnou možnost, jak ověřovat, že uživatelská data jsou pravdivá, případně aktuální po celou dobu jejich existence.

1 Federační model

Hlavní myšlenka federačního uspořádání je založena na faktu, že zpravidla každý uživatel spadá pod nějakou „domovskou" organizaci, která o něm spravuje informace ve svém systému. Takovou organizací je např. škola v případě studentů nebo zaměstnavatel v případě zaměstnanců. Domovská organizace ve vlastním zájmu pečuje o to, aby spravovaná data byla aktuální, protože to potřebuje pro zajištění své provozní agendy (výplaty mezd, organizaci studia apod.). Organizace také zpravidla pro své uživatele provozují informační systémy, včetně sekcí s řízeným přístupem, kam se uživatelé musí přihlásit pomocí autentizačních mechanismů a údajů získaných od své instituce. Federační model umožňuje využít informací spravovaných domovskou institucí i informačními systémy, které nejsou s touto institucí přímo propojeny, ale které jsou zapojeny v infrastruktuře pro výměnu dat o uživatelích – „federaci". Systémy zapojené do federace jsou schopné získat informaci o uživateli přímo z jeho domovské instituce, kde je největší záruka toho, že informace jsou aktuální, a není tedy potřeba aby si udržovaly vlastní systémy spravující uživatelské záznamy. Takové uspořádání navíc usnadňuje práci i samotným uživatelům, protože se vždy prokazují pouze autentizačními údaji, které používají pro přístup do svého domovského systému. Infrastruktura federace pak zajistí, že systémy si mezi sebou předávají potřebné údaje, tato komunikace je však pro uživatele transparentní.

Pro ustavení federace je nutné, aby se zúčastněné organizace dohodly na jednotném rozhraní, kterým budou získávat informace z institucí. Toto rozhraní (tzv. *Identity Provider*, IdP, poskytovatel identit) pak nabízí každá zapojená instituce poskytující data o svých uživatelích, zpravidla ve formě specializované služby běžící nad vnitřním systémem správy uživatelů. Identity Provider nabízí data o uživatelích, která jsou využívána koncovými službami ve federaci (*Service Providers*, SP, poskytovatelé služeb).

Tímto standardizovaným způsobem mohou koncové služby získávat informace o svých klientech, které lze použít pro následné řízení přístupu. Takto poskytované *atributy* mohou určovat např. kategorii poměru uživatele k instituci (např. zda se jedná o studenta, akademického pracovníka nebo pracovníka administrativy), zpřesňovat kategorii zaměstnání (lékař, uklízečka), určovat vztah k vnitřní struktuře organizace (člen konkrétní fakulty) apod. Autorizace na těchto atributech lze s výhodou použít např. na straně poskytovatelů digitálních knihoven s placeným přístupem. V současné době je řízení přístupu v této oblasti založeno na síťových IP adresách, kdy je přístup povolen, pokud uživatel přistupuje ke knihovnímu systému z předem specifikovaného rozsahu IP adres. Samozřejmě tento přístup není ideální ani pro provozovatele knihovny (protože přístup tak mohou mít i uživatelé, na které se licence nevztahuje), ani pro uživatele (protože jsou buď omezeni na práci ze své organizace nebo musí složitě konfigurovat různé síťové tunely apod.). Řada poskytovatelů těchto zdrojů proto nabízí napojení na federační infrastrukturu, která umožňuje přístup k atributům o konkrétním uživateli, což je výhodnější pro obě strany.

Přistupuje-li uživatel ke službě, musí nějakým způsobem poskytnout informaci, kde je jeho Identity Provider. K tomuto účelu slouží služba WAYF (*Where Are You From*). Tato služba je předřazena přístupu ke každé službě v rámci federace, uživatel zde vybere ze seznamu všech Identity Providerů celé federace toho, kdo provede jeho ověření. Služba WAYF je pevně svázána s federací, protože musí pracovat s aktuálním seznamem Identity Providerů.

Další oblastí, kterou je potřeba definovat během zakládání federační infrastruktury je tzv. schéma atributů, které specifikuje, jaké atributy popisující uživatele jsou pro danou federaci zajímavé a potřebné. Je potřeba dohodnout syntax těchto atributů i jejich přesnou sémantiku. Praktické zkušenosti ukazují, že zejména tato druhá část je velmi problematická, protože každý zapojený člen federace má trochu odlišnou interpretaci atributů. Příkladem může být atribut `eduPersonAffiliation` ze schématu `eduPerson`, které vzniklo pro popis atributů člena akademické instituce. Atribut `eduPersonAffiliation` popisuje zařazení v rámci organizace, např. student, zaměstnanec, učitel. Zde vyvstávají otázky typu „je učitel zároveň zaměstnanec?" apod. Zatím neexistuje shoda na mezinárodní a často ani na národní úrovni o přesné sémantice jednotlivých atributů.

Federace přinášejí možnost efektivního přístupu k uživatelským záznamům, ale také zavádějí nový model důvěry, kdy služba (Service Provider) přestává nést zodpovědnost za správu uživatelů, kteří ji využívají. Tato zodpovědnost je delegována na domovské instituce uživatelů, a služba tak ztrácí přímý vliv na fungování této složky. Nezbytnou součástí každé produkční federace tedy musí být specifikace politik, které se všechny jednotlivé organizace zavážou dodržovat při implementaci. Přesná podoba politik závisí na zamýšleném zaměření federace. Politiky mohou být specifikovány neformální dohodou zúčastněných stran, ale také to mohou být velmi podrobné dokumenty popisující přesně procedury, které jsou systémy používány pro provoz. Z definice federačního prostředí musí organizace při zapojení do federace souhlasit s tím, že bude informace o svých uživatelích zpřístupňovat všem poskytovatelům služeb ve federaci.

Federované prostředí je velmi příjemné pro uživatele, protože jim stačí jediná sada přihlašovacích údajů pro přístup ke všem systémům zapojeným ve federaci. Přístup k dnešním informačním systémům je často založen na protokolu HTTP, který podporuje mechanismus přesměrování, kdy server může odkázat klientský prohlížeč na jinou adresu, kterou je nutné navštívit před použitím samotné služby. Díky tomuto mechanismu může Service Provider odkázat uživatele zprvu na stránku jeho domovské organizace, kam se uživatel nejprve přihlásí. Po úspěšné autentizaci je opět jeho prohlížeč přesměrován na původní Service Provider s tím, že jako součást přesměrování je předána informace o uživateli. Tuto informaci použije Service Provider pro řízení přístupu k poskytované službě.

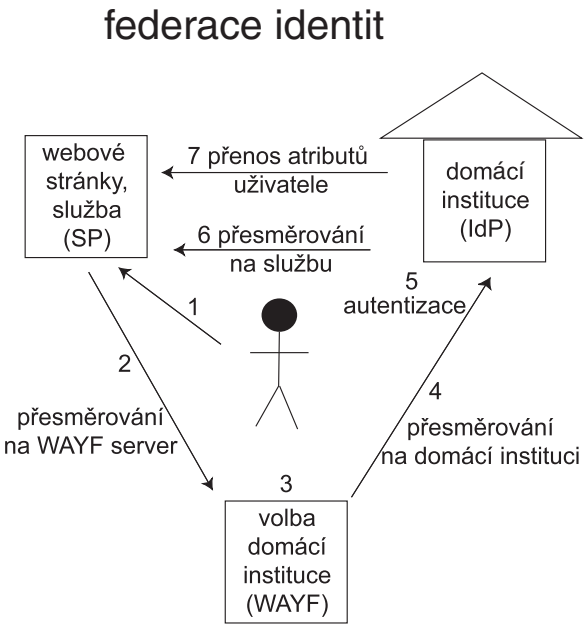
Uživatelé na tomto mechanismu ocení zejména to, že se vždy autentizují pomocí své domov-

ské webové aplikace, na kterou jsou zvyklí, a to i v případě, že požadují přístup ke službě, která není provozována jejich domovskou organizací. Mají tak pouze jednu sadu přihlašovacích údajů pro přístup ke všem systémům, které jsou zapojené ve federaci. Vedle toho, že takové uspořádání je uživatelsky příjemné, poskytuje i větší bezpečnost. Uživatelé si totiž zvyknou zadávat údaje vždy na jediné aplikaci, která má stálý vzhled. Po náležitém proškolení tak vzrůstá pravděpodobnost, že uživatelé nebudou automaticky zadávat přihlašovací údaje do všech aplikací, které od nich tyto údaje mohou vyžadovat. Pěstování těchto „hygienických návyků" je velice užitečné zejména v době, kdy vzrůstá počet phishingových útoků, které lákají z uživatelů citlivá data.

1.1 Shibboleth

Mezi nejpoužívanejší systémy implementující federační model patří middleware Shibboleth[1], který se používá pro zabezpečení přístupu k webovým aplikacím a podpoře SSO ve webovém prostředí. Shibboleth vyvíjí aktivita Internet2 a jsou na něm založeny akademické federace ve Švýcarsku (SWITCH), USA (InCommon), Velké Británii (UK Federation) a jinde.

Schéma systému Shibboleth je znázorněno na obr. 1. Na počátku je uživatel, který použije webový prohlížeč pro přístup k webové službě zabezpečené systémem Shibboleth (krok 1). Jelikož uživatel dosud není autentizovaný, jeho prohlížeč je přesměrován na službu WAYF (krok 2), která uživateli nabídne seznam institucí a jejich poskytovatelů identit. Po výběru své domovské instituce je uživatelův prohlížeč přesměrován na příslušnou stránku instuce (kroky 3 a 4), kde se autentizuje pomocí svého běžného jména a hesla, které používá pro přístup k lokálním systémům (krok 5). Po úspěšné autentizaci je prohlížeč nakonec přesměrován zpět na původní webovou aplikaci (krok 6), která tak dostane informaci o uživatelově úspěšné autentizaci a může také požádat uživatelovu instituci o poskytnutí dodatečných atributů. Tyto atributy jsou poskytnuty ve formě dokumentu v jazyce SAML (Security Assertion Markup Language, založen na XML) a dočasně uloženy na straně poskytovatele služby. Na základě těchto informací a lokální politiky pak služba rozhodne o povolení přístupu uživatele. Explicitní autentizační mechanismus složený z kroků 2 až 6 uživatel absolvuje pouze při přístupu k první službě v rámci jedné seance, všechny další přístupy k dalším službám jsou již autentizovány implicitně, a uživatel tak nemusí opakovaně zadávat své přihlašovací údaje.



Obrázek 1: Postup při přihlašování ve federaci

2 Federace CZTestFed

V České republice byly základy národní akademické federace identit položeny v dubnu 2007 propojením dvou institucí CESNET a ČVUT FEL. Tím vznikla testovací federace czTestFed využívající middleware Shibboleth. Později se postupně do federace czTestFed zapojili poskytovatelé identit dalších akademických institucí. V současné době jsou členy federace METACentrum, Masarykova univerzita, Karlova univerzita, Západočeská univerzita a již zmíněný CESNET a ČVUT FEL. Mimo těchto poskytovatelů identit je do federace zapojeno také několik aplikací (poskytovalů služeb), zatím převážně testovacího charakteru. Jejich seznam a další podrobnosti o

[1] http://shibboleth.internet2.org/

federaci czTestFed jsou uvedeny na www stránkách federace[2]. V současné době se připravuje přechod federace z testovací fáze do fáze pilotního provozu se skutečnými údaji o uživatelích, a příprava na zapojení reálných aplikací.

Masarykova univerzita je do federace czTestFed zapojena od června 2007, kdy byl zprovozněn poskytovatel identit pro osoby z MU. V průběhu měsíce října byla na MU zprovozněna i první aplikace využívající federační autentizační mechanismy. Jedná se o aplikaci pro zřizování guest účtů, která je blíže popsaná na konci článku v části 4.3.

V budoucnu se očekává využití federativních mechanismů především pro přístup k placeným elektronickým informačním zdrojům, ale je pravděpodobné, že najdou využití i v řadě dalších aplikací.

3 Konfigurujeme poskytovatele služeb

Jak již bylo řečeno, Masarykova univerzita má zprovozněného svého poskytovatele identit. Co je tedy dalšího potřeba pro využití autentizační a autorizační infrastruktury na bázi Shibboleth v konkrétní webové aplikaci? Je potřeba nainstalovat a zkonfigurovat softwarovou komponentu poskytovatele služeb (Shibboleth Service Providera, SP) pro příslušný server. SP existuje pro www servery Apache a IIS. Skládá se z Apache modulu, démona shibd (respektive ISAPI filtru a služby shibd v případě IIS) a souvisejících konfiguračních souborů.

Klíčovou částí Shibboleth SP je Apache modul (resp. ISAPI filtr), který zpracovává požadavky na přistup do chráněných oblastí webové aplikace. Pokud není uživatel autentizován, modul přesměrovává jeho požadavek na WAYF stránku, případně přímo na stránky poskytovatele identity. Poté co se uživatel na stránkách svého poskytovatele identit autentizuje, je přesměrován zpět do oblasti chráněné webové aplikace. Modul prostřednictvím démona shibd kontaktuje poskytovatele identit a získá dostupné uživatelské atributy. Díky tomu získává modul k dispozici informace jak o autentizaci uživatele, tak o uživatelských atributech potřebných k autorizačnímu rozhodnutí.

Instalace Shibboleth Service Providera není náročná. Pro Windows je instalace připravena v podobě balíku Microsoft instaleru (msi), pro Debian Linux je připraven debiánovský balíček, pro Red Hat balík RPM atd. Samozřejmě jsou k dispozici i zdrojové kódy k připadné kompilaci pro zvolenou platformu. Po instalaci a základní konfiguraci je potřeba informovat ostatní členy federace o existenci nového poskytovatele služeb. To se provede přidáním informací o poskytovateli služeb do *federačních metadat*, což je seznam všech poskytovatelů identit a služeb ve federaci.

Po ukončení instalace a zapojení poskytovatele služeb do federace můžeme začít řídit přístup k chráněným souborům. To můžeme provést například pomocí direktiv v souboru `.htaccess`. Přímočarost konfiguraci si můžeme ilustrovat následujícím příkladem:

```
AuthType shibboleth
ShibRequireSession On
require affiliation student@muni.cz
require user tonda@cuni.cz
require user helena@cesnet.cz
```

Uvedený příklad povoluje přístup k chráněnému adresáři všem uživatelům, kteří jsou studenty na Masarykově univerzitě, a dále uživateli s identifikátorem `tonda` z Karlovy univerzity a uživatelce `helena` ze sdružení CESNET.

Využití direktiv souboru .htaccess je jednou z možností jak definovat autorizační nastavení. Přistupová práva mohou být definována také ve speciálním xml souboru. Výhodou těchto dvou způsobů je to, že nevyžadují žádné zásahy do aplikace samotné. Autentizace a autorizace je ošetřena prostředky webového serveru. Pokud je to však vhodné, může autorizační rozhodnutí provádět samotná aplikace, které Shibboleth modul předá informace o přistupujícím uživateli prostřednictvím systémových proměnných.

Zpravidla jsou předávány informace jako jméno a příjmení, e-mail, zda se jedná o zaměstnance nebo studenta atd. Množina předávaných údajů závisí především na dohodě jednotlivých organizací, které jsou členy federace.

[2] `https://cztestfed.feld.cvut.cz/`

Takovéto předávání údajů o uživatelích mimo vlastní organizaci může vyvolávat obavy v souvislosti s ochranou osobních údajů. Proto jsou v systému Shibboleth implementovány mechanismy pro ochranu osobních údajů uživatelů. Na úrovni každeho poskytovatele identit se definuje jaké údaje mohou jednotlivé aplikace (poskytovatelé služeb) o uživatelích získávat. Aplikaci může být například předávána pouze informace, že přistupující uživatel je student či zaměstnanec bez toho, že by aplikace byla schopna osobu identifikovat nebo získat osobní údaje dotyčné osoby. Existují nadstavby, které samotným uživatelům umožňují ovlivňovat rozsah informací o jejich osobě předávaných poskytovatelům služeb.

Při zájmu o bližší informace o možnostech využití autentizačních a autorizačních mechanismů federovaných identit ve vaší www aplikaci kontaktujte prosím `idp@ics.muni.cz` nebo některého z autorů tohoto článku.

4 Aplikace

Při převodu webové aplikace na využívání federace je nejdříve třeba si rozmyslet, zda do aplikace budou moci pouze přihlášení uživatelé, nebo i nepřihlášení. Oba přístupy jsou možné, například známý software MediaWiki má rozšíření pro přihlašování se pomocí systému Shibboleth, kdy stránky může prohlížet kdokoliv, ale pro jejich editaci je nutné se nejdříve přihlásit. V aplikaci se pak pohybují zároveň jak přihlášení, tak nepřihlášení uživatelé, a je nutné mezi nimi rozlišovat. Naopak v jiných aplikacích musí být všichni uživatelé přihlášení.

Dále je třeba rozmyslet, zda autorizaci provádět na úrovni webového serveru nebo aplikace.

Informace o přihlášeném uživateli se z Apache dostávají do webové aplikace ve formě speciálních HTTP hlaviček, jejichž názvy a mapování na atributy je možné konfigurovat. Případně lze nastavit, aby byl v jedné z hlaviček i celý dokument s údaji o uživateli poskytnutý Identity Providerem v jazyce SAML.

Obvykle je jeden z atributů (např. `eduPersonPrincipalName`) mapován na proměnnou `REMOTE_USER`, aby bylo možné využít standardní mechanismy pro kontrolu přístupu uživatelů a zapisovat identitu uživatele do logů Apache.

Přenos informací o uživateli ve speciálních HTTP hlavičkách je natolik obecný, že samotná aplikace může být vytvořená na libovolné platformě, např. PHP, Java servlety, Perl a další.

V následujících odstavcích jsou uvedeny příklady služeb, které budou zavedeny do české federace.

4.1 Online elektronické zdroje

Oblast poskytování online elektronických zdrojů počítá s největším využitím konceptu federací. V současné době je přístup k těmto zdrojům většinou řešen na základě rozsahu IP adres. Federace umožní poskytovatelům precizně definovat, kdo může ke kterým zdrojům přistupovat. Zároveň uživatelé budou moci ke zdrojům přistupovat odkudkoliv. Poskytovatelé obsahu jako je Elsevier, Ovid, SilverPlatter a EBSCO umožňují přístup přes federaci. V ČR jsme zatím ve stádiu jednání o připojení.

4.2 Patologický atlas

Ve stádiu příprav je také zpřístupnění patologických atlasů[3] přes federaci. Tyto atlasy poskytují tisíce klinických a histologických obrazů kožních chorob, vývojových poruch a dále obsahují výukové materiály pro studenty medicíny. Nyní je pro práci s atlasy nutná registrace a obržení přístupových údajů. Po zapojení do federace budou moci studenti medicíny ze všech škol zapojených v české federaci přistupovat k těmto atlasům přímo.

4.3 Aplikace pro zřizování guest účtů

Jako příklad již existující aplikace, která využívá federativní autentizační middleware Shibboleth je možné uvést aplikaci pro zřizování tzv. *guest účtů* na MU. Tato aplikace umožňuje zřizování a údržbu tzv. guest učtů pro přístup k vybraným službám počítačové sítě MU. Guest účty jsou zřizovány pro osoby, které nejsou v přímém vztahu k MU a nevzniká jim tudíž automaticky nárok na využívání služeb dostupných v rámci sítě MU, nicméně je v zájmu MU jim na určitou dobu

[3] `http://atlases.muni.cz`

přístup poskytnout. Může se jednat o učastníky konferencí, osoby spolupracující na společných projektech, návštěvníky univerzitních knihoven atd. Na straně služeb se jedná například o přístup do VPN, do wifi sítě počítačových studoven. Jádrem aplikace pro vytváření guest účtů je webová služba, která operuje nad databází a adresářovou službou. Tato služba poskytuje metody pro vytvoření účtu, pro editaci údajů o uživatelích těchto účtů, a také pro povolování a zakazování časově omezených přístupů k různým zdrojům, jako jsou počítačové studovny, virtuální privátní síť, wifi síť. S touto službou pak komunikují webové aplikace, které zpřístupňují její funkcionalitu uživatelům pomocí grafického uživatelského prostředí.

V současné době mohou guest účty zřizovat pouze vybrané osoby v rámci MU. Tyto aplikace používají federativní autentizaci Shibboleth, takže bude výhledově možné aplikaci zpřístupnit osobám z dalších institucí zapojených do národní federace a v odůvodněných případech umožnit samoobslužné zřizovaní přístupu k službám počítačové sítě MU.

4.4 Testovací aplikace

V rámci testování vzniklo několik demonstračních aplikací, například Wiki s možností editace pouze pro členy federace a „chat pro vyvolené"[4], kde lze vytvářet místnosti s přístupem omezeným na osoby s určitými atributy, například místnost jen pro osoby se jmény Martin nebo Michal. Seznam aplikací v testovací federaci je uveden na stránkách federace czTestFed[5]

4.5 Aplikace bez webového rozhraní

Jak již bylo zmíněno, současné middlewary podporující federace jsou orientovány pouze na prostředí webových aplikací. Ne všechny aplikace však poskytují webový přístup, proto bylo nutné najít řešení jak do federace zapojit poskytovatele služeb, kteří nemají webový přístup. Jednou z možností je využít překladové služby, která převede informace od poskytovatele identit do formátu jiného autentizačního a autorizačního mechanismu. Další možností je „obalit" atributy jiným autentizačním mechanismem. Pro testování jsme využili druhou možnost, kde ukládáme atributy od poskytovatele identit ve formě rozšíření do osobního certifikátu. Experimentálně jsme nasadili tzv. Online-CA. Jedná se o certifikační autoritu, jak je definovaná v konceptu PKI, která vydává osobní certifikáty, ve formátu X.509, uživatelům, kteří se úspěšně autentizovali přes federaci. Tímto způsobem jsme schopni do federace zapojit služby, které umí pracovat s certifikáty. Samotný certifikát slouží jako autentizační mechanismus a atributy uložené uvnitř certifikátu jsou využity k autorizaci.

5 Závěr

Mechanismus federací identit vypadá velmi nadějně pro řešení problému ověřování totožnosti velkého množství uživatelů, protože po uživatelích vyžaduje nulové množství práce, což je přesně to množství práce, které jsou sami ochotni vynaložit pro zabezpečení přístupu k aplikacím. Dále dramaticky snižuje počet hesel, které si uživatelé musí pamatovat.

Z hlediska poskytovatelů služeb federace odbourávají nutnost implementovat vlastní systém pro správu uživatelů, a zároveň zajišťují aktuálnost dat o uživatelích.

Zkušenosti z již existujících federací ukazují, že se jedná o životaschopný koncept a lze očekávat jeho rozšíření v následujících několika letech.

Modernizace hardwarového vybavení IS MU

Michal Brandejs, Jan Kasprzak, Miroslav Křipač, FI MU

Jeden z důležitých projektů, které byly realizovány v letošním roce v rámci vývoje Informačního systému Masarykovy univerzity (IS MU), se týkal modernizace hardwarového vybavení. Ačkoliv výsledky projektů obvykle běžný uživatel zakusí velmi brzy po jejich realizaci, ať už se

[4] https://meta.cesnet.cz/shibchat/

[5] https://cztestfed.feld.cvut.cz/wiki/cztestfed/members/

jedná o nové aplikace nebo o zlepšení funkčnosti aplikací stávajících, dopady výměny serverů často nejsou na první pohled vůbec patrné. Přesto může nově navržená a připojená infrastruktura systému přinést velký užitek a nebo naopak naprostý krach. V tomto článku se čtenářům pokusíme přiblížit technické aspekty povýšení základních serverů IS MU, ke kterému došlo během letošního léta. Volně tak navážeme na náš předchozí článek [1], který popisoval stav hardwarového vybavení v roce 2004.

Motivace

Důvodů pro rozsáhlé změny uvnitř systému je hned několik. První z nich je doslova překotný vývoj aplikací IS MU, které pokrývají stále širší spektrum univerzitních činností, a které musí reagovat na nové a vyšší nároky. Tento vývoj je doprovázen nejen většími nároky na koncové uživatele, kterým však zároveň usnadňuje práci, ale také na systém samotný. Každý nový nástroj, který IS MU poskytuje, znamená přirozeně další zátěž pro servery, které jej realizují.

Další příčinou růstu nároků na systém je stále rostoucí počet uživatelů. Nejedná se pouze o celkový počet uživatelů, kteří se systémem mohou pracovat, ale také o vzrůstající počet těch, kteří využívají stále více služeb ke své každodenní činnosti. Zatímco před lety běžný učitel vystavoval známky a zadával zkušební termíny, dnes mohou učitelé běžně se studenty diskutovat, zadávat různé druhy studijních materiálů, testovat znalosti on-line za pomoci počítače nebo naskenováním a automatickým ohodnocením písemných testů apod. Došlo také ke zrušení papírových indexů a obecně k zavedení snazší elektronické administrativy do běžné výuky.

Vyšší nároky na systém vedly v uplynulých třech letech k postupnému vyčerpání kapacity původního hardwarového vybavení. Zatímco pro běžný provoz uprostřed semestru bylo ještě možné stávající zátěž úspěšně obsloužit, během období se zvýšenými nároky – zejména na začátku a konci výuky – začalo přibývat situací, kdy systém nebyl schopen zvládnout obsloužit všechny uživatele v požadované kvalitě bez zbytečné prodlevy způsobené čekáním na některou z klíčových komponent. Již během roku 2006 se začaly projevovat náznaky tohoto vyššího zatížení.

Prvním krokem v takové situaci je vždy ladění výkonnosti systému, a to jak na úrovni aplikací tak na úrovni systémových komponent, tedy zejména aplikačního a databázového serveru. V průběhu provozu se většinou ukáže, že některé součásti mohou obsahovat výkonnostní rezervy, které typicky přinesou zlepšení celkové odezvy systému v kritických situacích.

V další fázi rostoucí zátěže systému přichází v úvahu změna aplikací tak, aby byla omezena funkčnost pouze na služby, které jsou v provozní špičce nezbytně nutné. Tím dochází k dočasnému omezení méně významných služeb jako je volná diskuse v Plkárně, inzerce nebo některé výpočetně náročné statistiky, které nevyžadují bezprostřední reakci a je tedy možné je odložit na klidnější dobu.

S postupným rozvojem systému a zvyšováním počtu zátěžových špiček se však musí dostatečně dopředu naplánovat také samotné povýšení kapacity, které vzhledem k celkové složitosti a finanční náročnosti přichází na řadu jako poslední krok. V našem případě bylo plánovaní modernizace hardwarového vybavení zahájeno v létě roku 2006, tedy ještě v době, kdy běžný uživatel zvýšené zatížení nijak významně negativně nepociťoval. Bylo však důležité jednak zamezit zmiňovaným omezením a jednak naplánovat kapacity systému pro nové aplikace, zejména v oblasti e-learningu, ale i plánovaného prodeje kurzů a vzdělávání pro širokou veřejnost pomocí tzv. Obchodního centra, které mají významně rozšířit činnost univerzity a tím i zatížit IS MU.

Cíle

Prvním z cílů povyšování hardwarové infrastruktury IS MU bylo proto zrychlení jednotlivých operací. Zejména u velmi náročných výpočtů, které se provádějí v reálném čase, může zvýšení rychlosti výpočtu jednoho dotazu zvýšit pohodlí práce se systémem. Například v oblasti složitého vyhodnocování přístupových práv, které musí být dynamické a naprosto přesné, se zvýšení rychlosti výpočtu projeví při každodenní

práci v podstatě se všemi základními agendami systému.

Důležitějším přínosem zvýšení kapacity systému je však celková propustnost systému. Tedy vlastnost, která zajistí, že každý jednotlivý dotaz je obsloužen pokud možno stejně rychle bez ohledu na to, kolik dalších různých dotazů systém zpracovává. Přestože obě vlastnosti se navzájem prolínají, zajištění celkové prostupnosti není obvykle snadné a vyžaduje složitější architektury celého systému.

Vedle navýšení kapacity, a tím i rychlosti a propustnosti systému, byla důležitým faktorem také stabilita nového řešení, která je kriticky důležitá pro bezproblémový chod a tím i spokojenost uživatelů. Přestože počítačové systémy obecně nedosahují takových spolehlivostí, jako o mnoho let starší inženýrská řešení, snahou vývojářů systému je nabídnout službu, která bude dostupná kdykoliv odkudkoliv stejně samozřejmě, jako například elektrická energie.

Použitá architektura

Základem pro provoz systému IS MU je webový přístup, to znamená, že webový prohlížeč pro přístup k IS MU používá každý uživatel od namátkově přistupujících studentů kombinovaného studia až po administrativní pracovníky s rutinní každodenní prací se systémem. Prohlížeč se pomocí redundantního spojení připojuje do fyzicky oddělené sítě několika desítek počítačů IS MU. Jednotlivé dotazy jsou v rámci této sítě rozeslány mezi jednotlivé aplikační servery, které jsou vzájemně zastupitelné a obsahují v sobě jak zpracování HTTPs požadavků, tak samotnou aplikační funkčnost. K tomuto účelu používá IS MU cluster běžných jednoprocesorových serverů s operačním systémem Linux a webovým serverem Apache, na který je navázáno vlastní aplikační prostředí využívající programovací jazyk Perl. Výhodou tohoto řešení jsou zejména velmi nízké pořizovací a provozní náklady, kdy každý server lze jednoduše odpojit pro případnou údržbu, ale i povýšit výkon jeho jednotlivých komponent tak, jak to známe z běžných kancelářských počítačů. Efektivita celého řešení se navíc ještě zvyšuje tím, že aplikační servery, které mohou mít zapojeny až čtyři velkokapacitní pevné disky, slouží také jako obrovské distribuované úložiště pro celou řadu dat včetně objemných studijních materiálů, videí a studentských prací.

Navýšení celkového výkonu na aplikační úrovni je rovněž poměrně jednoduché, neboť vzhledem k tomu, že aplikační servery téměř nesdílí žádná data, dojde k navýšení výkonu pouhým přidáním dalších uzlů. Přestože výkon jednotlivých serverů aplikačního clusteru není nikterak vysoký, celková propustnost může být ohromující. Tím dochází k poměrně značné úspoře zejména v oblasti cenných investičních prostředků.

Naproti tomu databázová část realizuje sdílení všech dat zpracovaných v systému. Změny, které byly zavedeny pomocí aplikace běžící na jednom aplikačním serveru, musí být bezprostředně k dispozici všem ostatním serverům tak, aby mohlo být bezpečně realizováno zpracování všech kritických transakcí. Právě výkon databázové části je z toho důvodu kritickou stránkou architektury celého řešení.

Pro navýšení výkonu databázové vrstvy lze v současné době použít v zásadě dva přístupy. První z nich je, podobně jako v předchozím případě, založen na distribuci databázové zátěže do clusteru několika menších nezávislých uzlů, které dohromady poskytují potřebnou propustnost. Ze zkušeností nasazování databázových clusterů v rámci IS MU se však ukazuje, že režie spojená se zajištěním konzistence všech dat napříč uzly databázového clusteru výrazně ovlivňuje výkon celého řešení. Navíc sofistikované softwarové řešení, které databázové clustery představují, může zvýšením složitosti celého systému přinést řadu nových chyb a problémů při provozu, které snižují stabilitu takového řešení. V neposlední řadě je cena za licence pro využití této funkcionality tak vysoká, že při reálném nasazení v rozsáhlé infrastruktuře přestává být konkurenceschopná.

Druhým způsobem pro navýšení výkonnosti systému pro on-line transakční zpracování na databázové úrovni je využití systému se sdílenou pamětí, kdy procesy obsluhující jednotlivé požadavky přistupují ke všem údajům jednotně, přičemž komunikace je realizována operačním systémem a hardwarově. Právě tento přístup byl

zvolen pro další rozvoj IS MU, a to ze dvou důvodů: efektivita dosažení požadovaného výkonu a celková stabilita řešení. Tento způsob se například hojně využívá ve velkých bankovních ústavech uvnitř rozsáhlých finančních systémů.

Technická realizace

Konkrétních řešení, která nabízí daný způsob zpracování vysokého výkonu, je v současné době na trhu více. My jsme se omezili pouze na ta, která jsou založena na databázovém software Oracle Database, který IS MU využívá a pro který je optimalizován. Zároveň je prostředí IS MU omezeno na systémové úrovni na operační systémy unixového typu, což nevylučuje žádného z dodavatelů velkých hardwarových řešení, pouze reálně omezuje některé typy serverů.

Na základě upřesněných podmínek pak byl v rámci výběrového řízení vybrán systém *Altix 450* společnosti SGI, který nabídl nejvyšší výkon při zachování nízké ceny a dodržení podmínek záruční i pozáruční podpory, které v sobě zahrnovaly velmi důležitý servis včetně dostupnosti náhradních dílů.

Systém Altix 450 je založen na modulární architektuře, která umožňuje propojit více nezávislých komponent do jednoho systému tak, že výměna jednotlivé komponenty v případě poruchy nebo povýšení je podobně snadná, jako tomu je v případě zmiňovaných clusterů. Zároveň však systém propojení jednotlivých komponent, který je založen na proprietárních kabelech pro komunikaci mezi procesory navzájem a procesorem a pamětí (jedná se o architekturu typu NUMA), nevyžaduje nejprve zapojení složitější infrastruktury, která by dále zvyšovala cenu. Další výhodou je použití procesorů typu Intel Itanium 2, které oproti RISCovým procesorům lépe kopírují cenovou hladinu levných komoditních serverů.

Altix 450 sestavený pro IS MU je tak v současné době složen ze 4 modulů, které dohromady obsahuji 3 nezávislé servery, plně propojitelné do jednoho systému. To znamená, že v případě výpadku kterékoliv komponenty bude možné systém provozovat až do její výměny nejméně na 66 % výkonu. Běžné komponenty jsou pak obvykle na centrálním skladu běžně dostupné, což v praxi díky otevřenosti hranic Evropské unie znamená, že dojde k jejich výměně následující pracovní den po nahlášení.

Celkový výkon databázového systému je nyní 52 procesorových jader (jedná se o dvoujádrové procesory), přičemž všechna procesorová jádra mohou využít celých 104 GB operační paměti. Redundantně propojené diskové pole s 16 výkonnými disky obsahuje přibližně 2 TB hrubé kapacity, která je v současné době rozložena zejména pro navýšení výkonu přístupu k diskům. Samotná databáze je optimalizovaná tak, aby podstatná její část byla permanentně přístupná v paměti serveru tak, že k přístupu na disk dochází asynchronně při ukládání změn.

Zajímavosti o novém serveru

Přemýšlivého čtenáře jistě napadá, zda nejsou tři roky na provoz jednoho systému příliš krátká doba. Tedy zda nebylo výhodnější pouze navýšit výkon stávajícího serveru při zachování většiny dosud fungujících komponent. V praxi se však ukazuje, že obchodní politika firem dodávajících tato řešení přeje spíše nákupu nového systému, než povyšování stávajícího. Jinými slovy výkon dosažený novým systémem za stejných nákladů je často výrazně vyšší, než při povyšování starší technologie.

Zároveň nákupem nového systému otevíráme možnosti využít výhodnějších nabídek od jiných dodavatelů. Nejdůležitějším důvodem pro nákup nového serveru však byla skutečnost, že IS MU doposud nedisponoval dostatečnou výpočetní kapacitou pro případ zničení celého serveru. V takovém případě jsou data sice bezpečně umístěna na jiném místě v Brně a jejich obnova by nebyla problém. Provozovat systém takového rozsahu na běžně dostupném hardwarovém vybavení ale není možné, a proto by došlo k delší odstávce systému. Navíc pokud by došlo k chybě z důvodů nepokrytých zárukou dodavatele (požár, zaplavení apod.), trvalo by dodání nového systému až několik týdnů. Vyšší míra záruky, kterou výrobci pro tento případ také nabízí, ve skutečnosti obvykle znamená, že dodavatel udržuje na skladě přesnou konfiguraci téhož stroje ještě jednou, což také zákazník zaplatí. Ukazuje se tedy výhodné využít pro tento případ původní

hardware umístěný v jiném místě tak, aby byl zároveň dostupný pro případ katastrofy a zároveň mohl být dostupný pro další úlohy nebo vývoj nových aplikací.

Server byl vyroben na zakázku ve Spojených státech a na MU dorazil v červnu 2007. Jeho provoz byl spuštěn o víkendu 11. srpna 2007.

Operační systém serveru je Linux, stejně jako na 85 % nejvýkonnějších počítačů na světě.

Celková cena za popisovaný hardware nepřesáhla 65,- Kč na jednoho aktivního uživatele systému a rok, což v daném rozsahu a ve srovnání s obdobnými systémy je velmi příznivá cena.

Server již zaznamenal rekordní výsledky ve všech měřených hodnotách. Například dosáhl 46 000 operací za pět minut, 2 100 000 operací za den, 5 300 uživatelů v jeden okamžik a 27 000 uživatelů v jednom dnu. Server dosud nebyl zatížen špičkovým provozem ani z poloviny.

Dosažená dostupnost celého systému byla 99,989 % což představuje 100 % dostupnost hardwaru a operačního systému a jeden výpadek v řádu několik minut způsobený chybou v databázovém softwaru.

Server se stal jednou z nejvýznamnějších dodávek společnosti SGI v dané oblasti za poslední roky.

Výhled

Ukazuje se, že zvolená cesta tzv. vertikální škálovatelnosti výkonu na databázové úrovni je efektivním způsobem řešení architektury rozsáhlých on-line informačních systémů. Předpokládáme, že při zachování současného tempa zavádění nových služeb a podsystémů (jako je systém na odhalování plagiátů s propojením do archivu závěrečných prací na národní úrovni, Obchodní centrum pro administrativu placené výuky apod.) bude stávající hardware dostatečný nejméně následující tři roky.

Ruku v ruce s navýšením výkonu na databázové straně však došlo, a zřejmě bude ještě docházet, k modernizaci aplikačních součástí, kterou lze, vzhledem k charakteru jednotlivých dodávek, provádět jednodušeji postupně, podle aktuálních potřeb. Celkově tedy doufáme, že stávající architektura bude dostatečně pevným základem pro další rozvoj univerzity v řadě oblastí.

Literatura

[1] M. Brandejs, J. Kasprzak, M. Křipač. *is.muni.cz na novém hardware*. Zpravodaj ÚVT MU. ISSN 1212-0901, 2004, roč. XV, č. 1, s. 5-7. □

Tipy z Inetu: Evidencia súkromného volania z mobilných telefónov

Michal Oprendek, ÚVT MU

Písať o rozšírení mobilnej komunikácie a jej význame pri riadení a správe by bolo nosením dreva do lesa – veď každý z nás mobilný telefón má a o jeho výhodách vie. Podobne, ako v komerčnej sfére, i niektoré pracoviská Masarykovej univerzity poskytujú svojim zamestnancom služobné telefóny a pripúšťajú ich používanie aj na súkromné účely, najmä ak sa „zmestí" do predplatených minút.

Kontrolu a riadenie používania mobilných telefón podporuje i systém Inet. V súčasnej dobe v ňom beží pilotná prevádzka zahŕňajúca evidenciu mobilných telefónov zamestnancov Ústavu výpočetní techniky.

1 Aplikácie

Aplikačná podpora sa skladá z rozhrania pre správcov, pomocou ktorého riadia spracovanie údajov, a z aplikácii pre samotných užívateľov mobilných telefónov. V Inete teda nájdete aplikácie:

Seznam služebních mobilních telefonů
`https://inet.muni.cz/app/mobile/list`, ktorý informuje o Vašich súčasných i bývalých mobilných telefónoch; označovať súkromné hovory je potom možné v aplikácii

Výpis mobilních hovorů
`https://inet.muni.cz/app/mobile/calls`, v ktorej nájdete Vaše hovory roztriedené podľa mesiacov. Označovanie uľahčuje prepojenie s aplikácou

Osobní adresář
`https://inet.muni.cz/app/telef/osobni.adresar`, ktorý je spoločný s aplikáciami na správu hovorov realizovaných pomocou Jednotné hlasové sítě.

2 Spracovanie údajov

Spracovanie údajov o hovoroch je podobné ako pri hovoroch cez Jednotní hlasovou síť MU, má však svoje špecifiká. Operátor (Telefónica O_2) poskytuje podrobné výpisy uskutočnení hovorov a využitia služieb (SMS a MMS správy, dátové prenosy,...), ktoré sa importujú do systému Inet spolu s účtovanou cenou. Po importe sa výdavky za jednotlivé hovory prepočítajú, akoby tvorili jeden veľký spoločný paušál. Medzitým majú zamestnanci možnosť (a povinnosť) označiť svoje súkromné hovory. Po uzávierke označovania za ne zaplatia.

Hlavný rozdiel oproti spracovaniu hovorov uskutočnených prostredníctvom Jednotné hlasové sítě je, že v prípade pevných liniek sú údaje o hovore (a tým aj možnosť označiť súkromné hovorné) dostupné takmer bezprostredne po zložení slúchadla. Dáta o mobilných hovoroch sú bohužiaľ k dispozícii až začiatkom ďalšieho mesiaca. Na druhej strane, užívateľ vie, koľko presne za hovory zaplatí, keďže prepočet hovorného a uzávierka označovania sú oddelené akcie. V čase medzi nimi, kedy prebieha označovanie súkromného hovorného, sú už známe konečné ceny hovorov.

3 Prepočet hovorného

Prepočet cien za hovory má podobnú filozofiu ako v prípade hovorov z pevných liniek – zotiera rozdiely medzi počtom voľných minút v jednotlivých tarifách. Nezáleží ani na tom, či v konkrétnom prípade boli prečerpané voľné minúty alebo nie – každý platí za minútu hovoru rovnakú cenu. Budete namietať, že je tento prístup nespravodlivý, opak je však pravdou. Zahrnutie veľkosti paušálu by vytvorilo neľahko obhájiteľné rozdiely medzi zamestnancami (zamestnanci s menšími paušálmi by boli znevýhodnení), zahrnutie prečerpania či nevyčerpania voľných minút by mohlo mať za následok „šetrenie" minút na súkromné volania.

Takto navrhnutý systém motivuje zamestnancov používať mobilný telefón na súkromné volania iba v nutnej miere, čo otvára managementu možnosť optimalizovať náklady – po niekoľkých mesiacoch je zrejmé, ktorý zamestnanec skutočne potrebuje väčší paušál a ktorému by stačil i polovičný.

V tejto forme funguje systém na Ústave výpočetní techniky už štvrtý mesiac, je overený a použiteľný i pre iné pracoviská Masarykovej univerzity. V prípade záujmu o pridanie mobilných telefónov Vášho pracoviska do tohto systému píšte na `tel-op@muni.cz`. □

Z historie výpočetní techniky na MU. Sálové počítače

Petr Pištěk, ÚVT MU

Až do 90. let minulého století představovaly hlavní výpočetní kapacitu univerzity sálové (střediskové) počítače, tzv. *mainframes*. Na Ústavu výpočetní techniky MU, který tato zařízení provozoval, se postupem doby vystřídalo několik různých počítačů a zařízení vycházejících z technologií firmy IBM:

- EC-1033,
- EC-1027,
- terminálové centrum IBM-3090,
- Hitachi HDS 6600.

Počítač EC-1033

V létě roku 1979 byl v provizorních prostorách, které si univerzita zapůjčila od VUT Brno v Laboratoři počítacích strojů na Údolní ulici (po vyřazeném počítači MINSK 22), uveden do provozu první univerzitní sálový počítač – sovětský počítač EC-1033. Byl to typický představitel první řady tzv. *Jednotného Systému Elektronických Počítačů – JSEP* zemí RVHP, které byly vlastně implementací řady IBM 360 na součástkové základně „východního bloku". Po dvou letech, po dokončení počítačového sálu ÚVT v areálu přírodovědecké fakulty na Kotlářské ulici (vzniklého přestavbou bývalé „velké chemické" posluchárny), jej čekala demontáž, stěhování a několikatýdenní proces (znovu)oživení.

Ve své prvotní podobě byl počítač EC-1033, stejně jako jeho ideový vzor, určen pro čistě *dávkový provoz*. Dávkový provoz spočíval v tom, že uživatelé své zadání formulovali pomocí balíčku děrných štítků ve speciálním jazyce (tzv. Job Control Language, JCL), balíček odevzdali pracovnici vstupní/výstupní kontroly – a po různě dlouhém čase (zpravidla v řádu několika málo hodin až několika hodně dnů) jej dostali zpět spolu s tištěnými výsledky a protokolem o zpracování úlohy.

Pro tento režim byl také sálový počítač patřičně technicky a programově vybaven. Kromě procesoru a paměti (na počátku 512 KB feritové RAM) měl 6 jednotek výměnných disků po 29 MB, 4 jednotky magnetických pásek (šířka pásky byla 1/2", hustota záznamu až 800 bpi), 2 snímače děrných štítků (až 10 štítků/s), 2 řádkové rychlotiskárny (10 řádků/s), snímač a děrovač děrné pásky, souřadnicový zapisovač DIGIGRAF 1008 a elektromechanický psací stroj pro obsluhu.

Spolu s hardwarem byl dodán také operační systém OS/EC, který vznikl u výrobce (tehdy běžným) procesem „osvojování" cizího vzoru, v tomto případě systému IBM OS/360. Tento systém již umožňoval souběžné zpracování menšího počtu úloh (teoreticky až 15, prakticky podle jejich skutečných nároků na operační paměť), jejich prioritní nebo cyklické plánování a výstup do tiskových front místo fyzických tiskáren. Součástí dodaného základního programového vybavení byly mj. standardní překladače programovacích jazyků FORTRAN IV, COBOL, PL/1, RPG, Assembler a také poněkud nepovedený Algol 60. Záhy se také podařilo, již mimo základní dodávku, získat překladač jazyka Pascal.

Podle původních představ měl EC-1033 zajistit potřeby univerzity v oblasti vývoje a provozu ekonomických agend, vědeckotechnické výpočty (pro vědeckou a výzkumnou činnost) a výuku. Pro první dvě oblasti poskytoval tento počítač na svoji dobu celkem přijatelné služby. Pravda, bylo to za cenu povolení přístupu vybraných osob v předem naplánovaných hodinách přímo na sál počítače, aby se dosáhlo zrychlení obratu v cyklu *zadání úlohy – zpracování – oprava chyby - zadání úlohy…* Zato pro výuku představoval dávkový režim skutečnou pohromu. Na většině přírodovědných oborů se již tehdy věnovala značná pozornost zvládnutí výpočetní techniky a výuka spočívala především ve vyučování programování. Pokud mezi zadáním studentské úlohy a zjištěním, že ve zdrojovém textu je pár syntaktických chyb, uplynul typicky týden, nemohla praktická část výuky mít patřičné výsledky. Naštěstí univerzita záhy získala počítač Digital PDP 11/34, který značnou část výuky převzal a nabízel pro ni efektivnější interaktivní režim práce.

Počítač EC-1033 byl vyroben v Kazani, v tatarské autonomní oblasti Sovětského svazu. Tamtéž, přímo u výrobce, absolvovala školení skupina elektroinženýrů ÚVT a jeden systémový programátor, jejichž úkolem bylo udržovat tento stroj v chodu. Úkol to nebyl zrovna snadný. Poruchy byly na denním pořádku a největší problém nastával (dosti často), když se v názoru na zdraví hardwaru rozcházely nezávislý systém technických testů KPTO na straně jedné a operační systém OS/EC na straně druhé. Zatímco první optimisticky tvrdil, že vše je v pořádku, druhý (lakonicky, ale o to zarputileji) odmítal dokončit úvodní sekvenci zavádění operačního systému, tzv. IPL – Initial Program Loading, bez jakéhokoliv bližšího komentáře. Pak přicházela na řadu schémata na velkých výkresech, početné bedny s náhradními díly, případně specialisté z Kancelářských strojů. Významnou část technické péče představovala tzv. *profylaxe*, která mimo pravidelného spouštění oněch optimistických testů obsahovala mj. také nastavování čtecích/zapisovacích hlaviček magnetických disků pomocí osciloskopu v intervalu několika týdnů. Bez této činnosti by se rychle ztratila čitelnost nedávno zapsaných dat. I tak se pořizování záložních kopií dat z disků na magnetické pásky musela věnovat trvalá pozornost a obnovení obsahu nečitelného disku bylo také častou a zcela rutinní záležitostí.

Počáteční sestava EC-1033 dosti limitovala jak celkovou propustnost systému, tak zejména snahu po zvýšení produktivity programátorů (a připomeňme si, tehdy byl programátorem prakticky každý uživatel). Proto se postupně, podle finančních možností, rozšiřovala sestava o další sadu diskových jednotek, operační paměť (ve

dvou krocích až na finální 2 MB) a nakonec i o komplex lokálních terminálů. Operační systém byl převeden na vyšší verzi s podporou komponenty TSO (TimeSharing Option), která již umožňovala interaktivně upravovat zdrojové texty, spouštět jejich překlad, zadávat úlohy do dávkového zpracování a prohlížet na terminálu jejich výsledky.

Další větví rozšiřování systému byla podpora distribuovaného pořizování dat v rámci MU. Ta spočívala především ve vývoji vlastní softwarové podpory pro čtení velkých disket formátu 8", na které se data zapisovala na zařízeních řady Consul 271x. „Východní" verze operačního systému totiž ještě podporu disket neobsahovaly. Zbrojovka Brno, která počítače Consul vyráběla, souběžně vyvíjela adaptér pro připojení na standardní kanálové rozhraní sálových počítačů. Původní servisní program pro čtení datových souborů z disket přes zařízení Consul byl postupně rozšířen o podporu snímače disket ARITMA EC-5075 (s automatickým podáváním disket), čtení souborů operačního systému CP/M (z osmibitových mikropočítačů) a úpravy operačního systému, umožňující na disketách zadávat i samotné dávkové úlohy.

Počítač EC-1027

Podle plánů ministerstva školství byla první vlna sálových počítačů koncem osmdesátých let nahrazována modernějšími modely z řady JSEP II, kompatibilními s rodinou IBM 370. Nová řada sálových počítačů byla zpětně kompatibilní na úrovni strojového kódu se svou předchůdkyní a obsahovala rozšíření směrem k posílení výkonu a zlepšení možností interaktivního provozu. Za všechna jmenujme alespoň implementaci mechanismu virtuální paměti a nový typ řízení rychlých periferií, tzv. blokově multiplexní kanál. Univerzitě byl v rámci plánování přisouzen (a v létě 1989 nainstalován) model EC-1027, vyvinutý ve VÚMS Praha a vyráběný v ZPA Čakovice. Samotná centrální jednotka (procesor, operační paměť, kanály pro řízení periferií) jistě představovala výrazný pokrok oproti starému EC-1033 jak ve výkonu tak i spolehlivosti. Problém ovšem znamenal fakt, že tyto počítače byly standardně vybavovány výměnnými disky s kapacitou 100 MB nebo 200 MB bulharské výroby, které byly nechvalně známy svojí nespolehlivostí. Po značném úsilí se však podařilo zařídit dovoz repasovaných pevných disků Memorex (4 jednotky po 317 MB) z „kapitalistické ciziny" a tak zajistit odpovídající úroveň celého systému. Součástí sestavy byla také řídící jednotka sériových synchronních a asynchronních linek (tzv. teleprocesor), určená k řízení vzdálených terminálů, a další komplex lokálních terminálů. Do dodávky se také podařilo „vpašovat" několik nedostatkových počítačů TNS AT (kompatibilní s IBM PC AT, vyráběné v JZD Slušovice z komponent dovážených od asijských výrobců).

Operační paměť 8 MB umožňovala provozovat operační systém SVM (odvozený od IBM VM/370) s podstatně lepšími možnostmi interaktivní práce. Základní myšlenkou tohoto systému bylo vytvořit pro každého uživatele *virtuální počítač*, který je „k nerozeznání" od hardwarového rozhraní počítače reálného. Interaktivní uživatelé pak ve svých virtuálních počítačích provozovali operační systém pro interaktivní práci PTS (v originále IBM Conversational Monitor System, CMS). V jednom z virtuálních strojů běžel dávkový systém OS SVS pro zpracování rutinních úloh. Principiálně i prakticky bylo možné spustit ve virtuálním stroji i další instanci samotného SVM, např. pro testování vlastností jiné verze. V dodávce programového vybavení byl navíc překladač jazyka Fortran 77, později byl pořízen také překladač jazyka C.

Vlastní vývoj podpůrného programového vybavení se zpočátku soustřeďoval na rozvoj distribuovaného sběru a zpracování dat v rámci MU, od přenášení datových médií na ruční (přesněji nožní) pohon k přenášení dat „po drátech". Přítomnost teleprocesoru v sestavě umožnila vyvinout programy pro přenos dat mezi EC-1027 a PDP 11/34 a mezi EC-1027 a PC, připojeným několika různými způsoby, podle vzdálenosti a speciálního vybavení osobního počítače.

Mezitím ovšem události podzimu 1989 uvedly do rychlého pohybu spoustu věcí, včetně výpočetní a komunikační techniky. Pád železné opony s sebou strhl postupně veškerá vývozní omezení na pokročilé technologie, takže některé jinak nevyhnutelné fáze vývoje bylo možno přeskočit.

Místo postupného vývoje dálkového přenosu dat z domácích komponent a vlastními silami se začalo pracovat na počítačových sítích z komponent, které se daly poměrně snadno zakoupit.

Terminálové centrum IBM-3090

Prvním velmi hmatatelným výsledkem pádu omezení exportu pokročilých technologií byla tzv. *Akademické iniciativa IBM v Československu*, která demonstrovala možnosti moderních technologií (jakkoli v tehdejším pojetí konkrétního výrobce). Na ČVUT v Praze byl instalován sálový počítač řady IBM-3090 a na čtyřech univerzitách (ČVUT, UK Praha, MU v Brně a SVŠT v Bratislavě) byly umístěny čtyři komplexy po 20 terminálech a 10 osobních počítačích řady IBM PS/2 (s operačním systémem OS/2). Ve své době to byl nejvýkonnější počítač ve východním bloku. Co ale bylo daleko důležitější: byl to pro akademickou komunitu první počítač připojený ke globální datové síti. Ještě se nejednalo o Internet, byla to síť EARN/BITNET – síť sálových počítačů IBM (řady 360 a vyšší, včetně kompatibilních klonů a emulací protokolu), která ve svém největším rozkvětu dosáhla přes 3000 propojených uzlů. I když každý z připojených terminálových komplexů (kromě lokálního na ČVUT) měl k dispozici pouze komunikační linku o kapacitě 9600 bitů/s, význam byl průlomový. Síť umožňovala globální elektronickou poštu, a tím nás posouvala nejméně na polovinu cesty z počítačového dávnověku do tehdejší(!) současnosti.

Inspirace Akademickou iniciativou IBM samozřejmě vedla k úvaze o připojení sálového EC-1027 k síti EARN/BITNET. První experimenty ovšem nebyly příliš povzbuzující. Spustit na klientském terminálu program na čtení elektronické pošty trvalo dlouhé desítky sekund. Program byl totiž napsán v interpretovaném jazyce REXX, jehož vysoká režie na strojích běžných na západ od Šumavy nepůsobila žádné praktické problémy.

Počítač HDS 6600

Nedlouho po instalaci terminálového komplexu Akademické iniciativy IBM dostala MU nabídku na bezplatnou dodávku repasované centrální jednotky a diskového subsystému počítače HDS 6600 (výrobce Hitachi Data Systems, kompatibilní s IBM/370). Vzhledem k možnostem, které se nabízely, bylo těžko odmítnout. A realita skutečně naplnila očekávání – počítač měl 16 MB operační paměti (maximum dané „čistou“ architekturou IBM/370), byl osmkrát rychlejší než EC-1027 na běžných výpočtech a po doplnění akcelerátoru aritmetiky asi 30× rychlejší na vědeckotechnických výpočtech. Přestože měl za sebou kolem 25 000 provozních hodin, neměl žádné poruchy a umožňoval přejít na nepřetržitý provoz, jak si vyžaduje logika počítačových sítí, tehdy ještě umocněná slabostí komunikačních linek. Bez odmlouvání také strpěl připojení periferních zařízení východní provenience, původní to výbavy EC-1027, jako byly řetězové a bubnové rychlotiskárny, magnetické pásky a hlavně klíčový teleprocesor. Tím se vytvořil pozitivní příklad řešení střednědobé inovace klasického výpočetního centra a patrně se i naplnila očekávání výrobce (a dárce).

Linku Brno-Praha, provozovanou pro terminálový komplex Akademické iniciativy IBM, se podařilo vybavit speciálními modemy, které vytvořily dva kanály, každý o původní rychlosti 9600 b/s. V jednom zůstal provoz terminálů, přes druhý se HDS 6660 připojil k síti EARN/BITNET jako uzel CSBRMU11. Interaktivní práce s elektronickou poštou na lokálních terminálech byla samozřejmě řádově rychlejší, než tatáž práce přes slabou linku na (výkonnějším) vzdáleném počítači. Tento kanál také začal zajišťovat transport elektronické pošty do vznikající datové sítě MU. Ta již byla koncipována jako součást Internetu, ale zpočátku jí scházelo páteřní spojení, aby s globální sítí mohla komunikovat přímo.

Přímé spojení MU s Internetem přinesl až projekt CESNET (Czech Educational and Scientific NETwork). Pro HDS 6660 byl současně pořízen nezbytný hardware (adaptér pro připojení k lokální síti Ethernet) a nový operační systém (originální IBM VM/SP-370) s podporou protokolu TCP/IP. Sálový počítač (jako jeden z mála na našem území) se stal součástí Internetu jako uzel vm.ics.muni.cz. Spojení s vnějším světem tak obstarávala linka 64 kb/s, o kterou se v té době dělily vznikající sítě MU a VUT. Vzhledem k tomu,

že tyto sítě neměly dnešní tisíce uzlů, ani dnešní „hladové“ aplikace, byl to opět pro uživatele příjemný posuv k lepšímu. A navíc, v rámci projektu CESNET se většinou dařilo zvyšovat kapacitu páteřních tras tak, aby uživatelé nebyli brzděni v rozletu.

Rychlý rozvoj schopností výpočetních prostředků „lehké váhy“, především následníků někdejších minipočítačů s procesory typu RISC a výkonných variant architektury osobních počítačů způsobil, že potřebné aplikace začaly být zvládnutelné na levnější výpočetní technice. Sálové počítače jako specifická kategorie výpočetní techniky si udržovaly (a udržují dodnes) svou pozici především tam, kde je třeba zajistit extrémní množství transakčního zpracování, a kde je nákladově neúnosné (byť jen pomyslet na) přeprogramování rozsáhlých aplikací do jiného prostředí. Nic z toho ale nebyl případ Masarykovy univerzity. Ukončení provozu posledního sálového počítače pak urychlilo stěhování ÚVT do budovy na Botanické 68a na konci roku 1995.

O autorovi

RNDr. Petr Pištěk vystudoval obor (aplikovaná) matematika na Přírodovědecké fakultě UJEP Brno. Ihned po absolutoriu nastoupil na právě vznikající univerzitní Ústav výpočetní techniky v pozici systémového programátora počítače EC-1033. Postupně přebíral do systémové správy i další sálové počítače přicházející na ÚVT MU. Od počátku 90. let minulého století se věnoval také budování počítačové sítě na univerzitní a metropolitní úrovni, v těsné spolupráci se sdružením CESNET. V současnosti zastává na ÚVT MU funkci zástupce ředitele pro rozvoj a integraci. □

Obsah

Editor: Miroslav Bartošek • Vydavatel: Masarykova univerzita • Žerotínovo náměstí 9, 601 77 Brno, CZ
tel.: 549 492 100 • e-mail: zpravodaj@muni.cz • WWW: http://www.ics.muni.cz/zpravodaj/
Sazba systémem LaTeX 2ε písmem LucidaBright • Tisk: Grafex Blansko • *Neprodejné* • ISSN: 1212–0901