Infrastruktura univerzitních počítačových studoven

Jakub Dobrovolný, Vít Bukač,FI a ÚVT MU

Systém univerzitních počítačových studoven (UPS) představuje jednotně spravovanou síť počítačových studoven na různých místech MU, která nabízí uživatelům v každém svém bodě jednotné pracovní prostředí, přístup ke svým datům a standardizovanou sadu služeb [1]. Uživatel může podle svých aktuálních potřeb navštěvovat kteroukoliv ze studoven a využívat veškeré jí nabízené informační technologie a služby. V libovolné učebně fungující v režimu UPS mají všichni přístup ke svým centrálně uloženým datům, se kterými mohou pracovat v jednotné množině aplikací sahající od textových editorů až po speciální matematické nástroje.

Základní technologií používanou pro správu tohoto prostředí je *Microsoft Active Directory*. Doménová struktura se skládá z forest root domény a čtyř child domén, z nichž je jedna vyhrazena právě pro univerzitní počítačové studovny. Root doména obsahuje uživatelské účty všech studentů a zaměstnanců Masarykovy univerzity, zatímco v child doménách jsou soustředěné pouze počítače, ke kterým je možné se pomocí těchto účtů přihlašovat. O správu na nejvyšší úrovni se stará malá skupina doménových administrátorů, zaměstnanců Ústavu výpočetní techniky MU, naproti tomu jednoduché a opakované úlohy (instalace stanic, lokální změny politik) vyřizují lokální správci každé z child domén (zaměstnanci jednotlivých zařazených fakult).

Uživatelé

Centralizace správy podle zásady 1 člověk = 1 účet výrazně usnadňuje správu uživatelských účtů. Přidávání a zakazování účtů je automatizované, provádí se několikrát denně na základě změn v Informačním systému MU. Studenti jsou rozdělováni do skupin podle fakulty, oboru atd. až do úrovně jednotlivých předmětů, zaměstnanci až do úrovně pracovišť.

Častým problémem je existence *hostů* (guests), tedy osob, které z nějakého důvodu potřebují přístup k informačním službám, ale přitom nemají s organizací žádný bližší vztah (např. návštěvníci knihoven, návštěvníci konferencí). V takovém případě je této osobě díky jednoduché webové aplikaci vytvořen nový účet na pevně danou dobu. Tento účet má práva běžného uživatele a přístup ke všem obvyklým zdrojům (Wi-Fi, VPN,...) s výjimkou tiskáren. Záznam o existenci hosta je uchován i poté, co je účet smazán.

Po přihlášení uživatele ke stanici v libovolné učebně v režimu UPS jsou mu zpřístupněna jeho data a profil. Při odhlášení jsou veškeré změny propagovány zpět na server. Data jsou souběžně uložena na dvou diskových polích Hewlett-Packard o celkové kapacitě 2 TB, přičemž každému uživateli je vyhrazen diskový prostor o velikosti 100 MB. Kvůli vzrůstajícím nárokům je však v plánu nasadit do léta 2009 nové úložiště a kvótu navýšit.

Počítačové stanice univerzitních studoven

V současné době je v systému univerzitních počítačových studoven Masarykovy univerzity provozováno více než 500 počítačů, které se nachází v šesti lokalitách (Celouniverzitní počítačová studovna MU na Komenského náměstí, Fakulta sociálních studií, Filozofická fakulta, Přírodovědecká fakulta, Pedagogická fakulta a knihovna univerzitního kampusu). Aby se předcházelo nutnosti dojíždění doménových administrátorů na uvedené lokality, starají se o ně lokální fakultní správci. Jedná se převážně o instalaci/reinstalaci stanic, hardwarovou podporu, správu software, případně řešení problémů uživatelů.

Servery v doméně UCN

Technologie Microsoft Active Directory je v každé doméně nasazena vždy na dvou doménových řadičích (v případě výpadku jednoho přebírá jeho úlohu druhý). Doménoví administrátoři mají přístup ke všem serverům. Lokální administrátoři mají k dispozici třetí *member server* včetně předinstalované aplikace Adminpack umožňující správu infrastruktury bez nutnosti přístupu přímo na stroje. Tento přístup má značně omezená práva, konkrétně se jedná pouze o tvorbu a správu skupinových politik

a úpravu nebo zakazování a povolování účtů (nikoliv jejich vytváření nebo mazání). Na svém member serveru jsou tito správci lokálními aministrátory, tudíž jej mohou využívat pro vlastní potřeby, např. spravování software typu antivir.

Instalace OS a aplikací

Instalace operačních systémů probíhá pomocí technologie *Unattended* spolu se síťovými kartami s podporou PXE (Preboot Execution Environment). Při startu stroje administrátor zvolí bootování ze sítě, zadá heslo a stanice si stáhne všechny potřebné soubory a bezobslužně nainstaluje systém. Soubory jsou uloženy na datovém úložišti tří serverů, které tvoří cluster (tím je zajištěna vysoká dostupnost v případě poruchy). Zde se nachází kopie instalačních souborů ve všech konfiguracích potřebných pro počítače používané ve studovnách.

Po instalaci se stroj pomocí skriptu přidá do domény a po potřebném restartu se aplikují příslušné politiky a nainstaluje se vybraný software. Pro instalace software je využita technologie *Microsoft Installer*. Většina MSI balíčků je připravena enterprise administrátory pomocí administrativní instalace. Někteří výrobci dodávají se svými aplikacemi už hotový balíček, který stačí stáhnout a je připraven k použití.

V root doméně je zřízeno centrální úložiště (Distributed File System – DFS), a to se replikuje do každé child domény. Balíčky jsou tak většinou přístupny po rychlejší síti LAN a nezatěžují tolik celkový provoz na síti, pouze v případě výpadku serveru se MSI balíček stáhne z centrálního úložiště.

Instalace MSI balíčků je centrálně spravována pomocí *Group Policy Management*. Vytvoří se politika, v níž je nadefinována instalace, a lokální administrátoři sami rozhodují, který software pomocí dané politiky chtějí mít k dispozici pro uživatele a povolí její aplikování.

Práce z domova

Studenti mají možnost používat vybrané aplikace (z důležitějších můžeme jmenovat Matlab R2007a, STATISTICA 8, ArcView GIS 3.0, ArcGis atd.) i mimo studovny MU. Každý student má možnost připojit se pomocí *Vzdálené plochy* na server `tserver.ucn.muni.cz` [2], kde se přihlásí pomocí svého UČA a sekundárního hesla. Zde má již k dispozici svůj profil a svoje data a může pracovat i z domova tak, jako by seděl u stanice přímo ve studovně.

Bezpečnost

Základním principem bezpečnosti v takovéto infrastruktuře je nedávat uživatelům větší práva, než potřebují ke své práci. Proto mohou všichni uživatelé pracovat pouze s běžnými, nikoliv administrátorskými právy, a dopad případného útoku na systém je tak minimalizován.

Podstatným bodem je správa aktualizací. Již samotné instalační soubory jsou udržovány aktualizované. Všechny stanice jsou do infrastruktury zapojeny již s nejnovějšími záplatami. Následná distribuce záplat je řízena ze dvou univerzitních WSUS serverů. Servery WSUS udržují přehled o již aplikovaných updatech a umožňují specifikovat, které záplaty mají být uplatněny na které počítače. Skript kontroluje pravidelně každý týden stav všech strojů, a pokud některému z nich chybí důležité aktualizace, jsou jeho lokální správci informováni e-mailem.

Centrálně je řízena také ochrana proti virům. Všechny stanice v univerzitních počítačových učebnách mají nainstalován antivirový software NOD32, jehož správa a distribuce virových definic probíhají ze serveru pod správou doménových administrátorů. Posledním ze základních lokálních softwarových bezpečnostních prvků je firewall integrovaný v použitém operačním systému Windows XP, jehož nastavení je prováděno pomocí technologie Group Policy.

Součástí zajištění bezpečnosti UPS jsou i opatření pro bezpečnost fyzickou, která v sobě zahrnují především omezení přístupu do prostor s výpočetní technikou pouze pro osoby s platným ISICem nebo zaměstnaneckou kartou, a to buď přes turniket (případ Celouniverzitní počítačové studovny) nebo pomocí čteček karet. Počítače jsou proti krádežím zajištěné zvukovým alarmem, který se spustí, pokud je počítač odpojen z elektrické sítě.

Literatura

[1] R. Peša, O. Krajíček, L. Rychnovský. *Počítačové studovny MU.* Zpravodaj ÚVT MU. ISSN 1212-0901, 2005, roč. XVI, č. 1, s. 9-11.

[2] L. Rychnovský, P. Babinec, P. Tuček. *TServer - terminálový server UCN.* Zpravodaj ÚVT MU. ISSN 1212-0901, 2008, roč. XVIII, č. 5, s. 9-11.

[3] Univerzitní počítačové studovny – webové stránky. `http://www.muni.cz/ics/services/ups/about` □