Provozní data a co s nimi

Provozní data jsou vedlejším produktem činnosti všech informačních systémů. Článek se zabývá možnými výnosy z tohoto zdroje informací.

Každý systém generuje různé vedlejší informace o svém provozu. Jak je ale vydolujeme z logů? Pomůže nám průběžné sledování provozu předcházet blížícím se problémům? Jak řešit situaci, pokud je sledovaných systémů více? A jak provozní údaje získané tímto sledováním využít pro rozhodování na manažerské úrovni?

Kde se berou provozní data

Především se jedná o různé logové soubory systémových služeb, záznamy sledování výkonových a provozních charakteristik systémů (vytížení procesorů, alokovanou fyzickou, virtuální nebo diskovou paměť, počty procesů a vláken, počty aktivních uživatelů, otevřené relace, otevřená síťová spojení a další parametry síťového provozu), speciální aplikační charakteristiky – výkonové a statistické tabulky databázových systémů, počty transakcí, počty aktivních uživatelů, aktuální využití zdrojů databázového stroje apod. Každý si jistě dokáže dosadit další konkrétní zdroje informací podle svých znalostí a odborných zájmů. V podstatě jakákoli veličina či údaj přímo či nepřímo související s provozem informačního systému jsou z tohoto pohledu zajímavé.

Jak je z uvedených příkladů vidět, zdrojů provozních dat je nepřeberné množství. Jejich společnou vlastností je velká rozmanitost a nekompatibilita formátů. Data jsou uložena ve tvaru závislém na zdroji. Z principu věci neexistuje nějaký standard uložení provozních dat. Textový formát je například obvyklý u systémových logů, jinde se používají různé binární formáty, databázové tabulky se používají u databázových strojů nebo u specializovaných aplikací pro podrobnější analýzu. Můžeme však najít i mnohé další formáty.

Ad hoc dolování z logů

S využitím provozních informací pro řešení konkrétního dílčího problému se jistě setkal každý uživatel. Při reklamaci chybné funkce služby se správce dané služby ponoří do hloubi informačních systémů a po kratší či delší době se vynoří s nějakým výsledkem. Do jaké míry je tento výsledek užitečný, závisí na schopnostech a znalostech administrátora a také na rozsahu dat, která jsou k dispozici.

Někdy postačí nahlédnout do jednoho logu (pokud řešíme třeba problém s přihlašováním, nahlédneme do logu autentizačního serveru), jindy je třeba absolvovat dlouhou cestu z jednoho logu do druhého a spojovat informace přes různé vazební údaje (IP adresa, číslo portu, uživatelské jméno, ID relace atd.), než získáme požadovanou informaci. Tato metoda je použitelná pro jednotlivé případy, kdy hledáme příčinu konkrétního problému. Může být poměrně časově náročná a nehodí se pro rutinní operace, například pro preventivní vyhledávání možných anomálií. Příslovečné hledání jehly v kupce sena je mnohdy nepoměrně efektivnější než přebírání mega nebo gigabajtů vstupních dat pro výsledné vytěžení několika málo čísel nebo identifikátorů.

Souvisejícím problémem je dostupnost logů a ostatních provozních informací – příliš podrobné logování zatěžuje systémové zdroje (disková kapacita není neomezená a podrobné logování stojí také nějaký strojový čas), příliš hrubé logování zase neposkytuje dostatek informací pro zpětné řešení problémů. Obvyklý kompromis pracuje s časem. Za delší období se logují základní a agregované informace, podrobnější logy se drží jen po krátkou dobu a detailní logování se zapíná jen na dobu nezbytně nutnou v případě akutní potřeby.

Průběžné sledování provozního stavu

Pokud se nad věcí trochu zamyslíme, je jasné, že v těchto zdrojích musí být dobře viditelné anomálie provozu a nestandardní stavy. Stačí si vybrat veličiny, které vhodným způsobem reprezentují vitalitu informačního systému,

a sledovat je. Průběžným sledováním se pak můžeme dozvědět o blížícím se problému dříve, než nastane v plné síle, nebo alespoň dříve, než ho zaznamenají uživatelé.

Je výhodné použít nástroje, které zobrazí sledované veličiny v jejich časovém průběhu během dne nebo týdne. Pokud pracujeme se službou, která podléhá periodickému zatížení, snadno z grafu odhadneme, co může být ještě běžný průběh a co už ne – viz obr. 1. Pomocí těchto grafů může nestandardní situaci poznat i méně zdatný pracovník, protože graf veličiny za několik dní dává jasnou představu o obvyklých hodnotách i bez přesné znalosti významu sledovaných veličin. Příkladem takového monitorovacího nástroje je MRTG – viz Box 1.

Anomálií je pochopitelně příliš velká hodnota sledované veličiny, ale z hlediska detekce problémů může být zajímavá i neobvykle nízká hodnota – například pokud je zatížení emailového serveru v pracovním dni neobvykle nízké, může to znamenat potíže s přihlašováním uživatelů do poštovního systému nebo problémy se síťovou konektivitou. Samotný poštovní server sice žádné potíže nemá, ale nezvykle nízká hodnota zatížení nás může upozornit na problém nějaké jiné navazující služby.

Hromadné sledování služeb

Problém nastává, pokud máme větší počet sledovaných systémů. Máme-li desítky nebo stovky serverů, není možné každý z nich kontrolovat jednotlivě, je třeba použít odpovídající nástroj. Tím je specializovaný monitorovací systém. V principu nedělá tento systém nic jiného, než by dělal přepečlivý administrátor, kdyby neměl nic užitečnějšího na práci. Periodicky se v několikaminutových intervalech přihlašuje na všechny monitorované servery a ověřuje funkčnost služeb. Pokud některý z parametrů překročí nastavenou mez, zobrazí se varovné hlášení, konkrétní systém na obrazovce zčervená či jinak na sebe upozorní.

Pokročilé systémy navíc umožňují definovat závislosti mezi službami a sdružovat je do skupin – viz obr. 2. Také lze službám nebo skupinám přiřadit konkrétního správce, který pak v případě potíží dostane automaticky emailovou zprávu nebo SMS. Monitorovací systém může také archivovat konkrétní naměřené parametry a zobrazovat pak průběh provozních veličin, což opět pomáhá při diagnostice závady. Získáme tím také globální pohled na výpočetní prostředí, z jednoho místa můžeme dobře posoudit celkovou kondici rozsáhlé skupiny systémů. Typickým zástupcem této kategorie nástrojů je Nagios – viz Box 2.

Optimalizace vybrané služby

Pokud se vrátíme k detailnímu sledování jedné služby, můžeme uvést další

MRTG – The Multi Router Traffic Grapher BOX 1

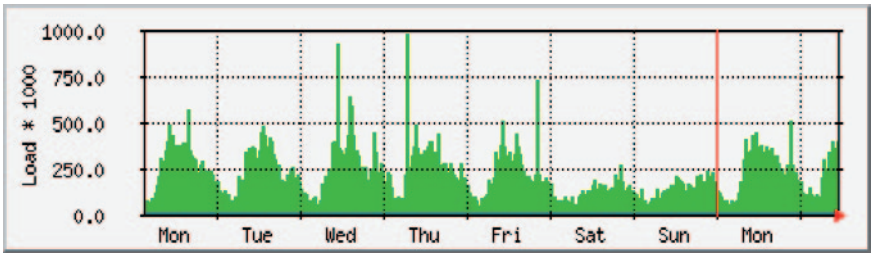
Nástroj vyvinutý původně pro monitoring provozu síťových prvků, v současnosti umí zobrazovat časová data v podstatě z libovolného zdroje. Snadno použitelný pro zobrazení zátěžových parametrů serveru (load systému, volná paměť, zatížení síťových rozhraní, velikost poštovních front, počty otevřených spojení apod.).

Sebraná data ukládá ve vlastní textové databázi. Provádí automatickou agregaci dat pro zobrazení intervalu 1 den, 7 dní, 1 měsíc, 1 rok. Agregovaná data jsou dostupná graficky na webovém rozhraní.

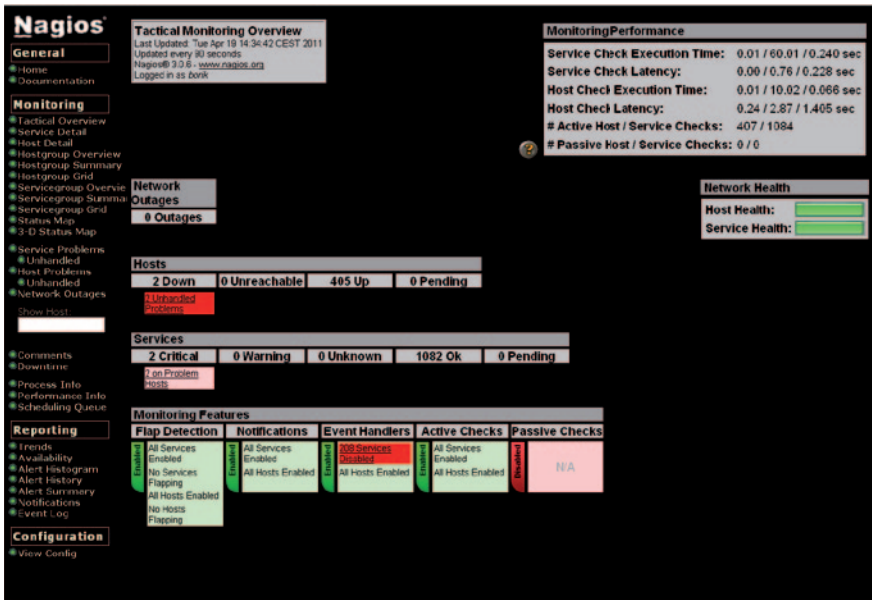
Podporované operační systémy: Unix/Linux, Windows, Netware.

Licence: svobodný software pod licencí GPL.

Zdroj: viz [1]



Obr. 1: Týdenní průběh provozní veličiny dle mrtg.



Obr. 2: Přehledová obrazovka monitorovacího systému Nagios.

příklad využití provozních dat. Jedná se o případy mimořádných špiček zatížení, které se obtížně simulují a v reálném prostředí se dostavují nepravidelně nebo jen jednou za dlouhou dobu.

Konkrétně v našem prostředí je to předzápisová aplikace, kdy si studenti elektronicky zapisují nabízené předměty do studijního plánu. Protože si všichni chtějí zapsat ty nejzajímavější předměty v nejvhodnějším čase, je v okamžiku povolení zápisu obrovský nápor na uvedenou aplikaci – viz obr. 3. Administrativním opatřením lze špičku rozdělit na více etap (např. podle ročníků), ale velký zájem uživatelů stejně vygeneruje zatížení systému o několik řádů vyšší, než je obvyklý průměr během školního roku.

Protože se předzápis koná jen jednou za rok, není přílišný prostor k opakovaným experimentům s nastavením systému v reálném provozu. Při předběžných testovacích zápisech a simulacích zátěže se nejprve odhadnou a dle možností odstraní potenciální slabiny. Zároveň se určí zdroje dat a rozsah logování. V průběhu skutečného zápisu se pak podrobně zaznamenávají všechny potřebné provozní informace. Získaná data pak analyzujeme s cílem optimalizovat nastavení všech subsystémů při příštím předzápisu a minimalizovat případné výpadky aplikace způsobené přetížením.

Detekce anomálií a incidentů

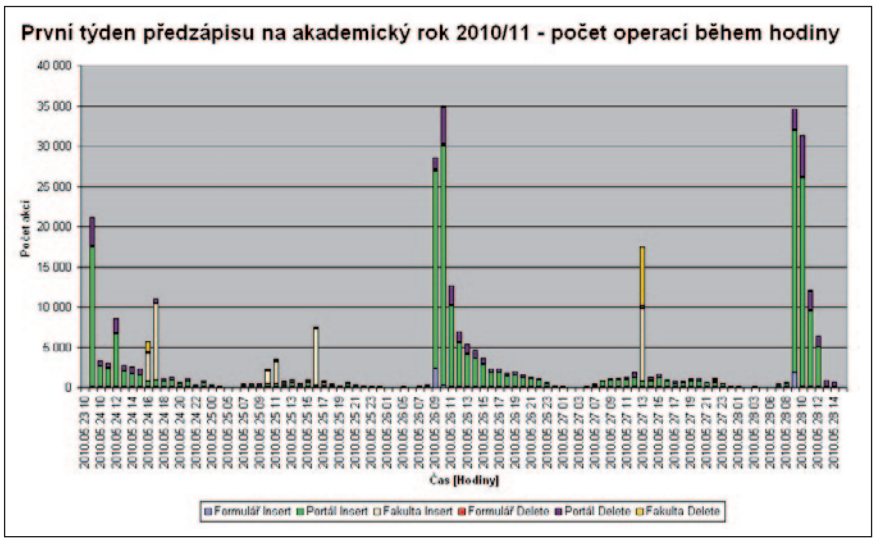
Specifickou oblastí je detekce anomálií a bezpečnostních incidentů v oblasti síťového provozu. Vzhledem k důležitosti konektivity pro každý počítačový systém je k dispozici rozsáhlý aparát specializovaných nástrojů, které umožňují sledovat provoz sítě a detekovat nežádoucí činnosti (spamování, útoky na špatně zabezpečené počítače apod.).

Nagios –. The Industry Standard In IT Infrastructure Monitoring BOX 2

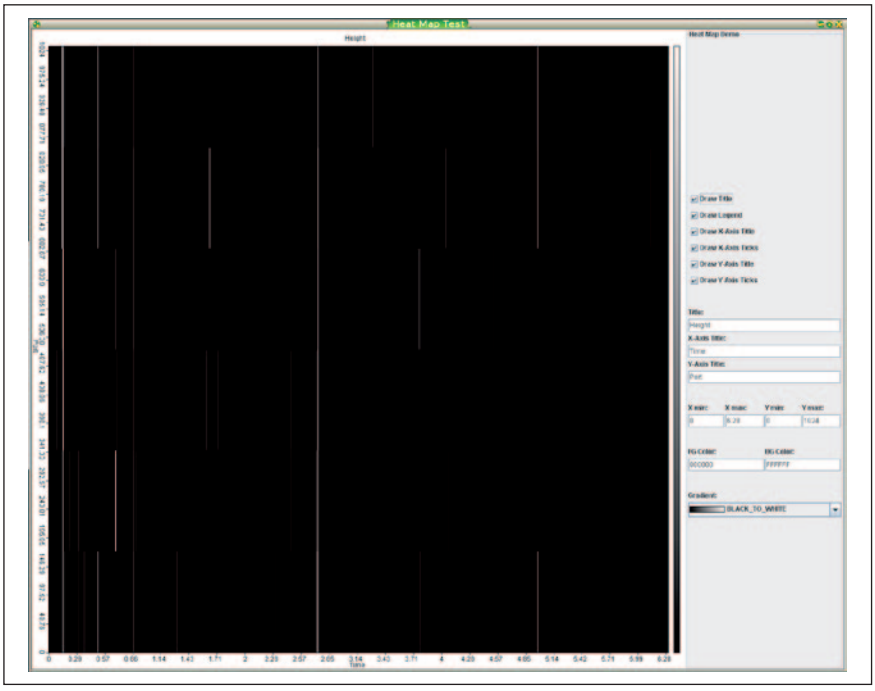
Dlouhá léta vyvíjený a podporovaný monitorovací systém. Základní verze (Nagios Core) je volně k dispozici, je například součástí mnoha běžně používaných Linux distribucí. Obsahuje plně funkční monitoring, grafické rozhraní, email a SMS alerty a sadu monitorovacích sond (pluginů) pro běžně používané systémy a služby. K dispozici jsou dále desítky sond naprogramovaných přímo uživateli Nagiosu (zadejte do vyhledavače termín „nagios plugin“). Sondu pro atypický systém lze také naprogramovat například pomocí skriptovacích jazyků.

V rámci placených služeb lze získat profesionální podporu a další nadstavbové moduly a rozšířené verze.

Zdroj: viz [2]



Obr. 3: Průběh zatížení databázového serveru při předzápisu.



Obr. 4: Skenování sítě útočníkem

Na obr. 4 je vidět příklad výstupu jednoho z takových nástrojů. Útočník (automat) přerušovaně, v nepravidelném pořadí a z různých počítačů skenoval otevřené porty v naší síti (s cílem najít nějaký počítač s chybou v zabezpečení). Při normálním zobrazení z logů služeb nebo síťového provozu by tato skutečnost zapadla v množství normálních „legálních“ spojení. Pokud však použijeme

vhodně definovaný filtr a jednoduchou zobrazovací komponentu [5], vyloupne se nám rázem ze záplavy běžných dat informace o aktivním útočníkovi, který prohledává vaši síť.

Pokud si chcete udělat přesnější představu, co lze od různých detekčních a zobrazovacích metod očekávat, vyzkoušejte si například The DAVIX Live CD – viz Box 3.

The DAVIX Live CD BOX 3

Live CD založené na Slackware, ze kterého můžete rovnou spustit a vyzkoušet téměř 40 volně dostupných nástrojů pro sběr, zpracování a vizualizaci dat souvisejících se síťovým provozem. CD je použitelné nejen jako demo, ale i jako regulérní servisní nástroj (specifická nastavení lze uložit do distribuce například na USB disk). S ohledem na stáří kolekce (2008) je vhodné konkrétní vybrané nástroje pro reálné použití nainstalovat v aktuálních verzích z jejich originálních zdrojů.

Licence: svobodný software, pro případná omezení viz též licenční podmínky jednotlivých programů v distribuci.

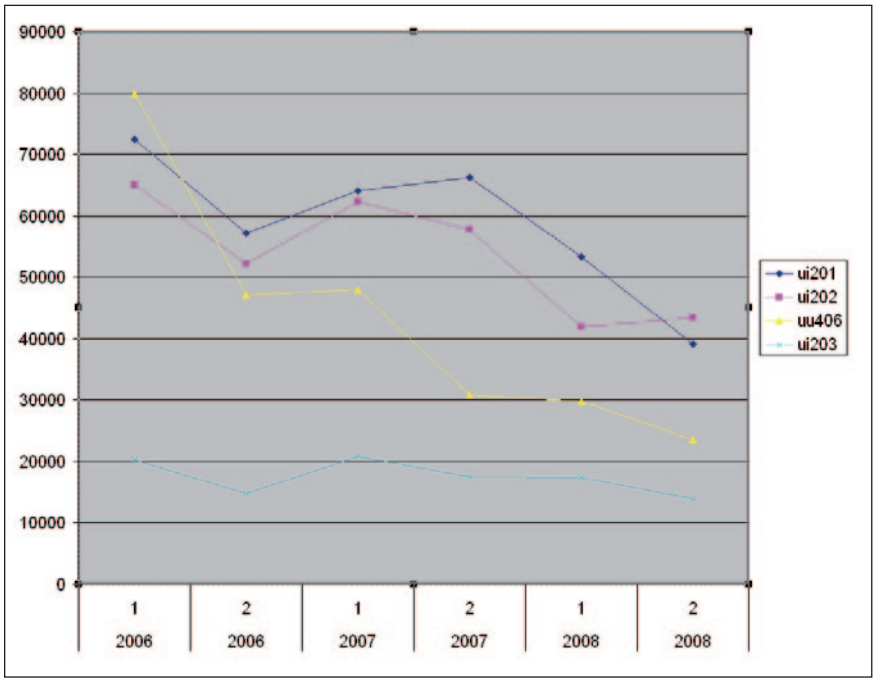
Zdroj: viz [3]

Manažerské rozhodování

Pro rozhodování na manažerské úrovni mohou provozní data poskytnout cenné podklady. V různých situacích, třeba při úvahách o rozšiřování služeb nebo při omezení zdrojů financování, je potřeba kvalifikovaně rozhodnout o změnách v objemu a uspořádání služeb. Rozhodování musí být podloženo dostatečnými informacemi a zde mají provozní data opět své nezastupitelné místo.

Příkladem je optimalizace rozmístění veřejných učeben a počtu strojů v nich. Pro rozhodování stačí udělat přehled využití učeben, například podle počtu přihlášení uživatelů za den – viz obr. 5. K tomu potřebujeme informace z autentizačních serverů. Je pravda, že samotný akt přihlášení nezohledňuje rozdílnou délku práce uživatele na konkrétním místě, ale při početné skupině uživatelů je to metoda dostačující pro porovnání jednotlivých učeben. Úlohu jen lehce komplikuje objem vstupních údajů (logy autentizačních serverů), který u nás činí desítky gigabajtů ročně.

Pro další příklad lze udělat časový snímek provozu pracoviště HelpDesku s ohledem na optimalizaci pracovní doby. Vycházet lze například z času vytvoření uživatelského požadavku v RT systému (Request Tracker – evidence uživatelských požadavků). Časový snímek průběhu dne za delší období nám poskytne dostatek informací pro rozhodnutí, jak upravit provozní dobu HelpDesku a počty pracovníků v jednotlivých směnách.



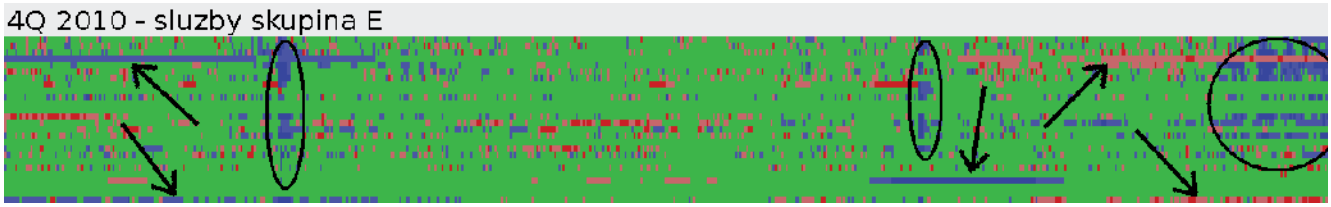
Obr. 5: Manažerská charakteristika – využití učeben.

Chceme-li zobrazit několikaletou historii například pro stanovení trendů a odhadu dalšího vývoje, potřebujeme i delší historii provozních dat. Jak už bylo zmíněno, nebývá zvykem všechna provozní data uchovávat po dlouhou dobu, právě s ohledem na jejich obrovský objem. Ale na druhou stranu jakákoli selekce, předzpracování, agregace a komprimace jsou nutně spojeny se ztrátou detailních informací. Podle zákona schválnosti se pak někdy dostaneme do situace, kdy uchováváme objemná data, která zřejmě nikdy nebudeme potřebovat, a naopak jiná data nám chybí nebo jsou nevhodně agregována se ztrátou některého důležitého parametru. Prostě a jednoduše proto, že dopředu nedokážeme odhadnout, které historické informace nás po třech nebo pěti letech budou zajímat.

Hrátky s daty

Na závěr zde máme jakousi volnou disciplínu. Na rozdíl od předchozích případů máme už spoustu údajů z různých zdrojů shromážděných a připravených na stejné platformě. Pak se můžeme pustit do zpracování dat různými metodami s různými cíli.

Z této báze dat mohou specializované nástroje odhadovat blížící se anomálii. Výstup jedné analytické aplikace můžete vidět na obr. 6. Algoritmus zpracoval provozní charakteristiky skupiny serverů za tři měsíce bez znalosti konkrétního významu veličin a jen na základě obvyk-



Obr. 6: Automatická detekce anomálií (jsou označeny šipkami a zakroužkováním).

lých denních a týdenních průběhů označil podezřelé oblasti – červenou barvou neobvykle vysoké a modrou neobvykle nízké hodnoty. Pokud se zaměříme jen na větší, barevně odlišené plochy, snadno zaregistrujeme:

- dvě profylakční odstávky systémů (modré svislé linie);
- delší odstávka jednoho systému (modrá vodorovná linie);
- začátek vánočních prázdnin (náhlý pokles parametrů služeb v pravé části obrázku);
- dlouhodobě stoupající zatížení dvou serverů (vodorovné linie přecházející postupně z modré do červené).

Při průběžném získávání dat do této databáze pak může takový algoritmus sloužit jako zdroj varování, že se děje cosi podezřelého. Administrátor pak může konkrétní podezřelý systém prošetřit standardními metodami a zjistit, zda se jedná o blížící se problém nebo jen o planý poplach.

Podobných využití báze provozních dat může být celá řada: Můžeme hledat podklady pro zvýšení spolehlivosti (srovnání poruchovosti zařízení různých značek). Lze hledat souvislosti mezi přetížením nebo výpadky zdánlivě nesouvisejících systémů. Můžeme se zabývat statistikou využití systémů jednotlivými pracovišti, ať už pro účely účtování nákladů nebo pro zlepšení služeb nejpočetnějším skupinám uživatelů. Pro manažerské rozhodování můžeme nabídnout odhad budoucího vývoje (očekávaný nárůst počtu uživatelů, potřebné diskové prostory, počty serverů a výkony potřebné pro aplikace apod.), a to vše tentokrát na vyžádání obratem a ve variantách podle různých scénářů dalšího rozvoje.

Dalších možností je celá řada, stačí si jen uvědomit, jaké všechny informace v sobě provozní data vlastně obsahují. Podrobněji se oblasti vytěžování dat (datamining) věnovaly také články v jednom z předchozích čísel DSM [5].

Shrnutí

Výše uvedené příklady využití provozních dat vycházejí z našich praktických zkušeností v univerzitním prostředí. Rozmanité výukové i vědecké činnosti vyžadují celé spektrum různých výpočetních systémů a služeb. V neposlední řadě studenti tvoří mimořádně aktivní a pokročilou kategorii uživatelů, ať už ve významu pozitivním (vyžadují a používají nejnovější technologie) či negativním (sami se někdy podílejí na bezpečnostních incidentech), což zvyšuje nároky na preventivní sledování stavu systémů.

Postupy zmíněné v tomto článku používají obdobně v různé míře správci jakýchkoli větších systémů či sítí. Rozsah použití jednotlivých metod je závislý kromě jiného na konkrétních vlastnostech prostředí i možnostech dílčích subsystémů.

A jako u každé činnosti je třeba pečlivě rozvážit i náklady a výnosy – dolování informací z provozních dat není jednoduchou a levnou záležitostí, ale výsledky této činnosti nám mohou poskytnout cenné informace.

Jiří Bořík
borik@civ.zcu.cz

Ing. Jiří Bořík

Absolvent Fakulty aplikovaných věd Západočeské univerzity. V minulosti se zabýval vývojem databázových aplikací a integrací informačních systémů v několika komerčních firmách. V současné době pracuje v Centru informatizace a výpočetní techniky ZČU. Jako člen týmu Laboratoře počítačových systémů se zabývá rozvojem univerzitního výpočetního prostředí.

POUŽITÉ ZDROJE

[1] *OETIKER+PARTNER AG Open Source Projects* [online]. 2011 [cit. 2011-04-29]. The Multi Router Traffic Grapher. Dostupné z WWW: <http://oss.oetiker.ch/mrtg/>.
[2] *Nagios – The Industry Standard In IT Infrastructure Monitoring* [online]. 2009-2011 [cit. 2011-04-29]. Nagios Core. Dostupné z WWW: <http://nagios.org/projects/nagioscore>.
[3] *SecViz | Security Visualization* [online]. February 17th, 2008 [cit. 2011-04-29]. The DAVIX Live CD. Dostupné z WWW: <http://www.secviz.org/node/89>.
[4] BECKLER, Matthew. *Matthew Beckler Home Page* [online]. 2010-07-26 [cit. 2011-04-29]. Java Heat Map. Dostupné z WWW: <http://www.mbeckler.org/heatMap/>.
[5] MRÁZEK, J. *Bezpečnost a datové sklady*. DSM 1/2005, s. 30–33.