Dohled a správa serveru

Co a jak při administraci serveru

Jiří Kadaník (jiri@kadanik.org)

Středisko Un*xových technologií

30.březen 2010

Obsah

- Úvod
- Zjišťování stavu serveru
- Monitoring
- Logy a jejich analýza
- Správa pomocí grafických rozhraní
- Ukázky

Úvod

- Proč vůbec monitorovat?
- Je to k něčemu?
- Co s logy?
- Jak prohlížet logy?

Zjišťování stavu serveru

- ps, top, htop, pstree, atop
- netstat, iptraf, tcpdump, nmap, nload
- vmstat, free, pmap
- w, who, uptime (uptimed)
- /proc
- strace, lsof
- sysstat (sadf, iostat, mpstat, pidstat, sar)
- apachetop

Zjišťování stavu serveru

top

- prohlížení procesů, CPU, paměti
- neintuitivní ovládání

htop

- vylepšený top
- lepší ovládání a konfigurace

ps, pstree

- snapshot současných procesů
- pstree, ps -ejH, ps axjf

Zjišťování stavu serveru

w, who

- umožní zjistit přihlášené uživatele a jejich procesy
- $ w franta

uptime

- umožní zjistit jak dlouho server běží, počet uživatelů a aktuální zátěž

uptimed

- daemon
- eviduje záznamy kdy a jak dlouho server běžel

Zjišťování stavu serveru

iptraf

- interaktivní IP LAN monitor
- ukazuje nejrůznější statistiky (TCP, UDP, ICMP)

nmap

- port scanner
- dobrý na prozkoumávání otevřených portů (kontrola firewallu)

nload

- zobrazuje aktuální vytížení sítě

Zjišťování stavu serveru

strace

- sleduje systémová volání
- použití na debugování programu, který padá

lsof

- vypíše otevřené soubory
- $ lsof /var

/proc

- pseudo file-systém vytvořený při bootu
- obsahuje informace o procesech a dalších věcí z jádra
- http://www.kernel.org/doc/Documentation/filesystems/proc.txt

Monitoring

- MRTG
- RRDtool
- Cacti

- Nagios
- Zenoss
- Zabbix

Monitoring

MRTG - Multi Router Traffic Grapher

- primárně určený k monitorování a měření trafiku
- umí SNMP protokol, ale lze používat i bez něj
- vytvoří HTML stránku se 4-mi grafy

RRDtool

- první verze 1990 - "správně napsané MRTG"
- data ukládá do round-robin databáze
- nadefinování RRA souboru
- předhazovaná data jsou pak interpolována aby odpovídala danému rra archivu

Monitoring

Cacti

- Webový frontend k RRDtool
- Uživatelé, práva, stromy grafů
- Sbírání dat: buď cmd.php (PHP) nebo spine, původně cactid (C)
- Velký počet šablon a návodů: http://forums.cacti.net/ a http://cactiusers.org/

Monitoring

Nagios

- Začal jako Netsaint, 2002 Nagios

Zabbix

- 1998 začátek vývoje, 1999 vyšel pod GPL
- 2004 vyšla verze 1.0, nyní Zabbix 1.8

Zenoss

- 2002 začátek vývoje, listopad 2006 vyšla verze 1.0

Logy a jejich analýza

- Syslogd
- Syslog-ng
- Metalog

- Logrotate

- Logwatch
- Swatch
- Logcheck

Logy a jejich analýza

Syslog

- Nabízí logování na vzdálený server

Metalog

- Oproti syslogu nabízí regulární výrazy a pouštění skriptů při matchi
- Nelze logovat na vzdálený server

Syslog-ng

- Open source implementace syslog protokolu
- Kombinuje výhody syslogu a metalogu
- Filtrování podle obsahu a druhu, vzdálené logování, logovací server
- Zápis na TTY, spouštění programů,

Logy a jejich analýza

syslog-ng.conf

- Options
- Sources
- Filters
- Destinations
- Logs

Logy a jejich analýza

logrotate

- Konfigurace v /etc/logrotate.conf
- Přidávání pravidel do /etc/logrotate.d/*
- Defaultní pravidla v konfiguračním souboru
- Pro každý soubor možnost nadefinovat vlastní pravidla
- Definování skriptů, provedených před nebo po rotaci souboru
- Možnost poslat si rotované logy na mail
- man logrotate

Logy a jejich analýza

logwatch

- Sumarizuje logy a generuje email popisující je
- Obsahuje předpřipravené skripty pro většinu potřebných služeb
- Je možné nastavit jakýkoliv rozptyl (–range 'between -5 days -3 hours')
- Nutné při hodně upraveném logu upravit konfiguraci
- Lze vyexportovat report pro každého hosta v logfiles
- + jednoduchý zdrojový kód (PERL)
- - špatná dokumentace

další nástroje

- Logcheck
- Swatch

Správa pomocí grafických rozhraní

Komerční systémy

- cPanel
- WebHost Manager
- Plesk

Open-source řešení

- Webmin
- Usermin - navržen pro neprivilegované uživatele
- Virtualmin - alternativa cPanel nebo Plesk

Závěr

- monitorujte
- logujte
- procházejte logy
- naučte se PERL ;)

Děkuji za pozornost

Prostor pro dotazy