

ENLOGIT

Dohledový systém

Jiří Hlinka
Ondřej Suchý
Enlogit s.r.o.

Business case

Problém

- **Finanční ztráty** spojené s výpadky infrastruktury
- Neřízený nákup technologií vede ke **zbytečným výdajům**
- **Nespokojenost** uživatelů, zákazníků, nadřízených při výpadcích

Řešení

- Díky **upozornění na výpadky** se zkrátí downtime a tím se minimalizují ztráty a nespokojenost sponzorů
- Díky **znalosti trendů** se racionalizují nákupy nových technologií



Řešení: dohledový systém

Funkce dohledového systému

- Upozorňuje na problémy díky proaktivnímu monitoringu
- Umožňuje předvídat vývoj a předcházet problémům
- Konsoliduje systémové záznamy – logy
- Offline diagnostika (dohledání logů a trendů)



Dohledový systém od Enlogit

Virtuální "appliance" od Enlogit

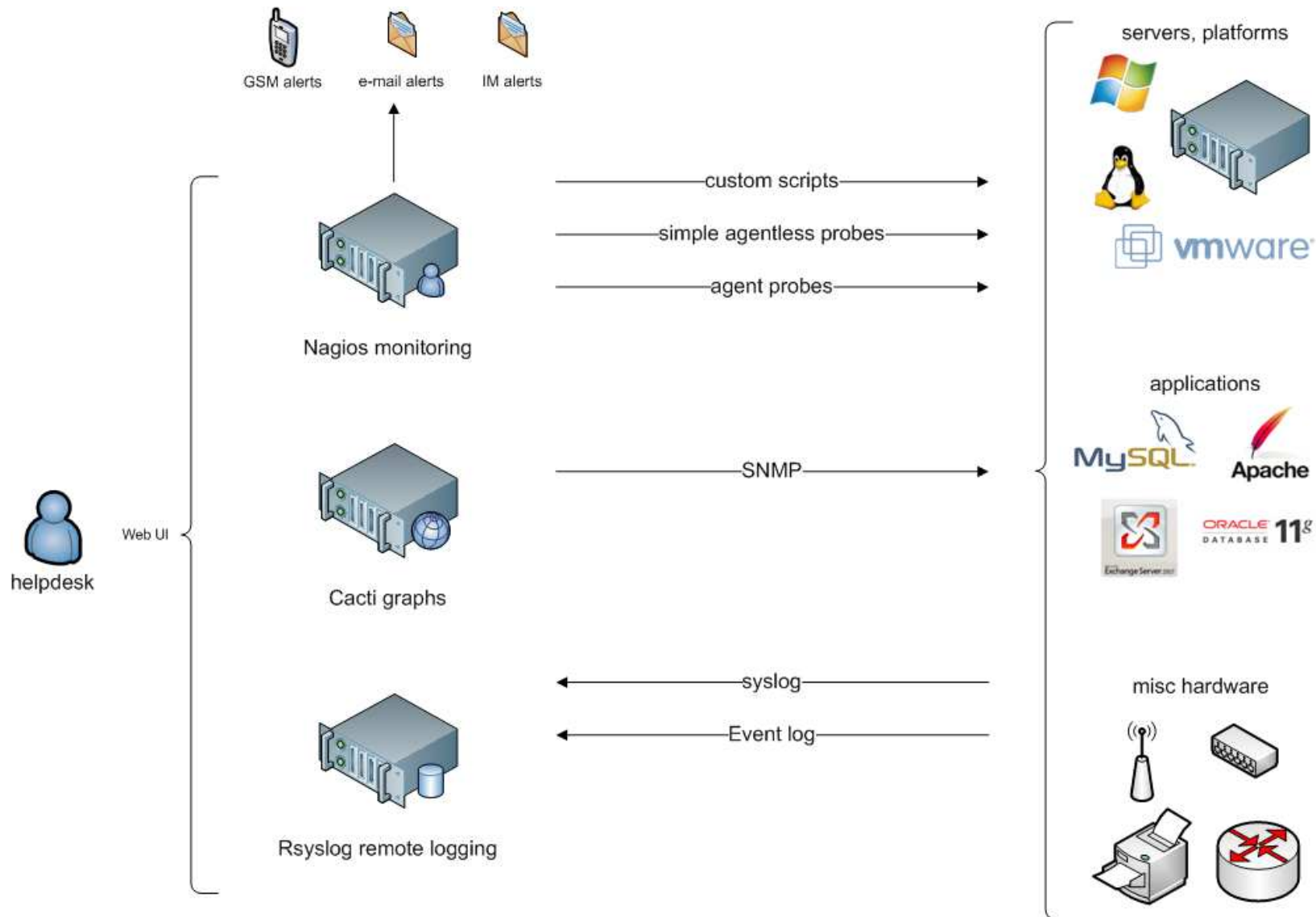
- Integruje open source aplikace Nagios, Cacti, Rsyslog
- Vše nainstalováno a nakonfigurováno
- Integrace s GSM modemy a hardwarovými čidly (teplota, vlhkost)
- Xen nebo VMware VM nebo fyzická instalace RHEL/CentOS

Služby Enlogit




- Instalace a nastavení
- Přizpůsobení (skriptování pokročilých kontrol apod.)
- Training (administrátor dohled. systému, operátor helpdesku)



Komponenty systému



Nagios

| Host ▲▼ | Service ▲▼ | Status ▲▼ |
|---|-------------------|-----------|
| backup  | check_ping | OK |
| | check_ssh | OK |
| fw  | check_ssh | OK |
| localhost  | check_http | OK |
| | check_local_disk | OK |
| | check_local_load | OK |
| | check_local_procs | OK |
| | check_local_swap | OK |
| | check_local_users | OK |

System pro sledování stavu ICT infrastruktury

- open source, velká komunita, velký počet předpřipravených skriptů, definice vlastních kontrol, web UI

Možnosti

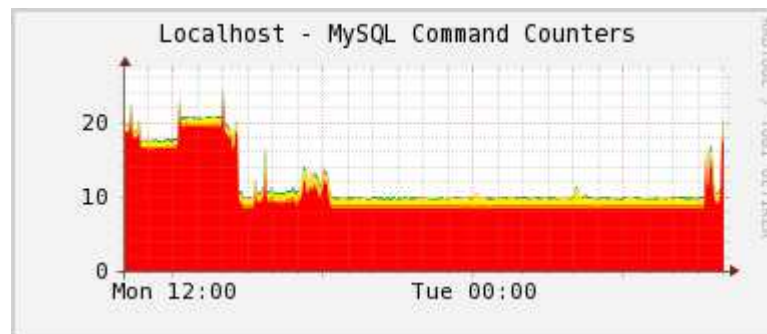
- Základní test dostupnosti serverů, služeb, tiskáren a dalších zařízení
- Překročení prahových hodnot (CPU load, místo na disku, teplota apod.)
- Aktivní testování služeb (např. database query)
- Korektivní akce (např. restart služby, automatická oprava databáze)

Notifikace

- Notifikace při změně stavu (SMS, e-mail, jabber)
- Omezení notifikací na časový interval (např. pracovní doba)
- Zasílání notifikací na skupiny kontaktů (linux support, windows support)



Cacti



Sledování vývoje parametrů v čase

- Network traffic, CPU load, využití paměti, využití disků
- Podrobné informace o vytížení služeb (Apache, MySQL, Postfix apod.)
- Sledování trendů
- Upozornění při překročení prahové hodnoty
- Upozornění při změně trendu (např. nárůst teploty o určitou hodnotu)



RSyslog

| Date | Facility | Severity | Host | Syslogtag | ProcessID | Message |
|--------------------|----------|----------|----------------|---------------------|-----------|--|
| Today 04:02:03 | CRON | NOTICE | monitored-test | anacron[6595]: | | Updated timestamp for job 'cron.daily' to 2009 |
| Today 04:02:01 | CRON | NOTICE | l-monitoring | anacron[21175]: | | Updated timestamp for job 'cron.daily' to 2009 |
| Today 02:20:43 | SECURITY | CRIT | monitored-test | sshd[6094]: | | fatal: Read from socket failed: Connection reset |
| Yesterday 21:03:39 | USER | ERR | l-monitoring | restorecond: | | Will not restore a file with more than one hard link |
| Yesterday 17:15:00 | DAEMON | WARNING | l-monitoring | avahi-daemon[1905]: | | last message repeated 2 times |
| Yesterday 17:14:48 | DAEMON | WARNING | l-monitoring | avahi-daemon[1905]: | | Invalid query packet. |

Alternativa k syslogd, centrální syslog server

- Přijímá logy ze vzdálených serverů, routerů a dalších zařízení
 - kompatibilní se syslog (UNIX/Linux) a EventLog (Microsoft Windows)
- Data ukládá do databáze, případně do souborů
- Web rozhraní PhpLogCon (filtrování, statistiky, vyhledávání)
- Možnosti zaslání notifikací Nagiosu
 - možnost definice textových řetězců, regexp
 - *např. poplach při výskytu smartd chyb*
- Nahradí syslogd v RHEL 6, již nyní integrován v dohledovém systému od Enlogit



KONEC



redhat.
PREMIER
PARTNER

Jiří Hlinka & Ondřej Suchý

jiri.hlinka@enlogit.com

ondrej.suchy@enlogit.com

ENLOGIT