Návrh riešenia softérovej a hardvérovej infraštruktúry pre projekt elektronického zberu dát ŠÚ SR

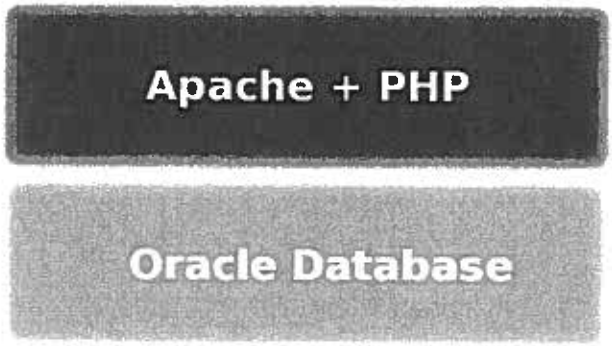
Ciele

Cieľom riešenia je vytvorenie infraštruktúry pre zber dát z externých zdrojov pre Štatistický úrad SR. Infraštruktúra pozostáva z optimálnej kombinácie hardvéroveho a softvérového vybavenia a musí spĺňať tieto kritériá:

- výkon
- vysoká dostupnosť
- škálovateľnosť
- bezpečnosť

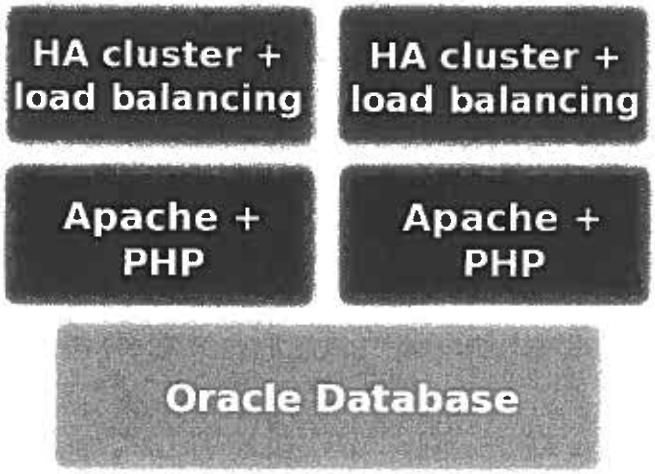
Základný popis

Aplikácia webStat, je web aplikácia slúžiaca pre zber dát z externých zdrojov pre Štatistický úrad SR. Aplikácia využíva open source technológie - web server Apache, server-side skriptovací jazyk PHP. Dátovú vrstvu zabezpečuje databázový server Oracle.



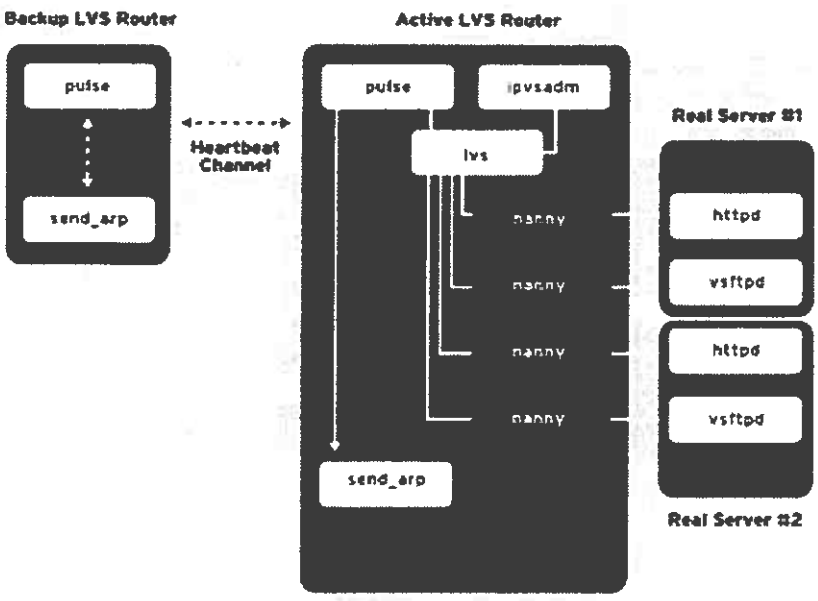
obr.1 existujúca infraštruktúra

Pre dosiahnutie cieľov riešenia, je vytvorená farma webových serverov (web farm) pozostávajúca zo základných modulov - clustrov.



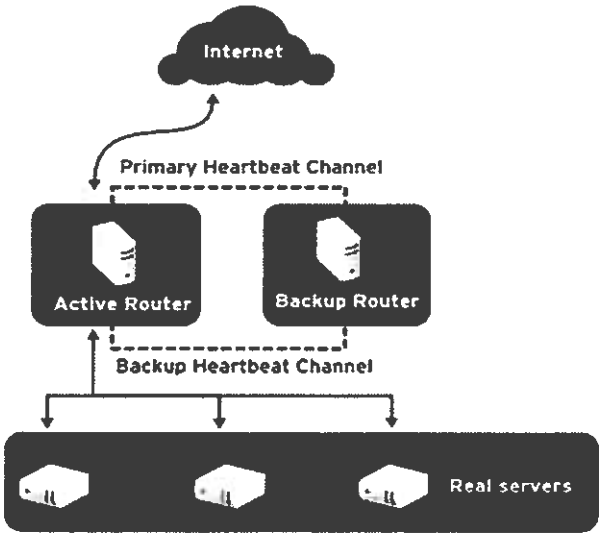
obr.2 navrhovaná infraštruktúra

- **požiadavku na výkon** zabezpečuje load balancing front end cluster - LVS. LVS distribuuje záťaž na skupinu backend (real) serverov, pozri obr. 3. LVS zabezpečuje persistentné spojenie klienta s back end web serverom, podľa aktuálneho zaťaženia. V prípade zlyhania ktoréhokoľvek back end web servera dynamicky presmeruje spojenie na iný web server a vyradí nefunkčný web server z clustra back end serverov. Nody LVS clustra tvoria výkonné multiprocesorove servery s CPU architektúrou x86_64, viď. špecifikácia hardvéroveho vybavenia.



obr. 3 - funkčná schéma load balancing clustra - LVS

- **požiadavku na vysokú dostupnosť** zabezpečuje HA cluster - heartbeat. HA cluster sa používa na zvýšenie dostupnosti služieb, ktoré cluster poskytuje. Eliminuje tzv. single point of failure tým, že v prípade výpadku jedného prvku clustra (load balancera) ho dynamicky nahradí iným. Pozostáva z 2 prvkov - nodov, pozri obr. 4.



obr. 4 - funkčná schéma HA clustra - heartbeat

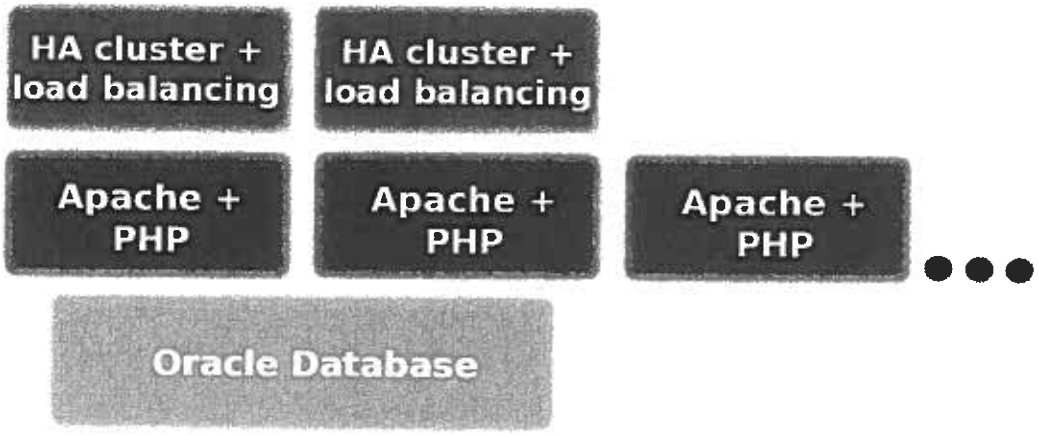
Pre dosiahnutie vysokej dostupnosti cluster obsahuje aj monitoring server. Je to samostatný server monitorujúci všetky prvky clustra, ktorý zasiela notifikácie na e-mail alebo SMS / pager administrátora, čím výrazne skracuje reakčný čas pri riešení nepredvídaných okolností - zlyhanie nodu clustra, softvérová / hardvérová chyba, bezpečnostný incident, prekročenie prahových hodnôt pri prevádzke (aktuálny počet aktívnych spojení a pod., prekročenie bežnej záťaže, príliš dlhý čas pri obsluhe jednej požiadavky a pod.)

Všetky servery v clustri sú vybavené redundantnými komponentami a servisným procesorom alebo kartou pre vzdialený menežment servera s podporou vzdialenej konzoly, možnosťou vypínania alebo zapínania serverov na diaľku, podporou prediktívnej analýzy chybného komponentu a softvérom na správu a menežment serverov.

Servery v clustri neuchovávajú žiadne dáta. Zálohovať preto nie je nutné denne (nevylučuje sa), ale postačuje napríklad po zmene konfigurácie a pod. Zlyhanie ktoréhokoľvek nodu clustra nemá vplyv na stratu dáta ani funkčnosť celého clustra, tj. RPO=0. Strata dát v neuloženom formulári klienta nie je považovaná za stratu dát, o konzistenciu dát počas zápisu formulárov do databázy sa stará databázová tranzakcia. RTO pre úplnú obnovu jedného nodu clustra je približne 2h.

- **požiadavku na škálovateľnosť** zabezpečuje cluster **n** * backend web serverov. Cluster web serverov je vytvorený výkonnými multiprocesorovými servermi s CPU architektúrou x86_64. Rozširovaním clustra web serverov o ďalšie backend web servery je možné rozložiť záťaž na viacej fyzických strojov a tak zabezpečiť lepšiu odozvu pri poskytovaní weboveho obsahu klientom. Navrhovaná konfigurácia nie je obmedzená iba pre prevádzku plánovanej aplikácie na danej softvérovej a hardvérovej platforme, ale je možné pridať nezávislú skupinu (obyčajne aspoň dvoch) web serverov, ktorá pracuje s iným databázovým zdrojom - napr. webservery IIS s databázou MS SQL. Rozširovanie je možné do maximálneho počtu limitovaného 23 portmi v použitých ethernet switchoch a priestorom v 19" racku.

  Riešenie databázovej vrstvy nie je predmetom zadania. K dispozícii je existujúci databázový server s databázou Oracle 10g. Obecne škálovateľnosť a vysokú dostupnosť databázovej vrstvy rieši Oracle Real Application Cluster (RAC). RAC umožňuje beh viacerých databázových inštancií nad jednou databázou. Každá inštancia v RAC beží na vlastnom serveri (node), databáza je umiestnená na zdieľanom úložisku, spravidla SAN alebo diskový subsystém zdieľaný cez shared SCSI bus.



obr. 5 - škálovateľnosť clustra

- **požiadavky na bezpečnosť**
  - pre navrhovaný operačný systém sú k dizpozícii bezpečnostné aktualizácie po dobu **7 rokov** od uvedenia na trh, pozri sekcia softvérové vybavenie
  - operačný systém má implementovaný Manadatory Access Control mechanism SELinux (*Security-enhanced Linux)*
  - infraštruktúra je umiestnená v demilitarizovanej zóne (DMZ). Infraštruktúra obsahuje web cluster a databázový server Oracle. DMZ oddeľuje navrhovanú infraštruktúru od Internetu a od infraštruktúry ŠÚ SR. Pozri obr. 6
  - databáza Oracle nie je prepojená so žiadnou databázou mimo DMZ. Prístup k dátam je dávkový a iniciovaný z lokálnej siete ŠÚ SR.
  - DMZ je chránená firewallom (netfilter/iptables), ktorý je súčasťou nodov LVS clustra. Default politika je DENY. Medzi zónou Internet a DMZ je povolené komunikácia výhradne s web servermi. Každý systém je chránený vlastným firewallom a poskytuje iba tie porty a tie služby ktoré sú nevyhnutné pre funkčnosť.
  - pri spojení klienta z Internetu s web serverom je použité TLS/SSL šifrovanie spojenia. SSL certifikát od dôveryhodnej certifikačnej autority odporúčame použiť.
  - medzi DMZ a inými uvažovanými vzdialenými lokalitami bude prepojenie realizované virtuálnou privátnou sieťou VPN. Odporúčame použitie IPsec.
  - pre vzdialenú administráciu systémov sa používa šifrované spojenie - OpenSSH
  - všetky zmeny na systémoch monitoruje Intrusion Detection System (IDS).

Špecifikácia softvérového vybavenia

Operačné systémy

- Red Hat Enterprise Linux 5 (RHEL). RHEL je enterprise serverovská Linux distribúcia s podporou na komerčnej báze. RHEL je certifikovaný ako platforma pre väčšinu podnikového softvéru ako napr. Oracle Database a tiež beží a je certifikovaný pre väčšinu hardvéru na platforme x86, x86_64 od významných dodávateľov serverov - IBM, HP, DELL ... Spoločnosť Red Hat poskytuje niekoľko úrovní podpory líšiacich sa časovým rozsahom pokrytia a rýchlosťou odozvy. Support kontrakt za obstaráva na 1 alebo 3 roky. Doporučujeme udržanie aktívnej podpory na celú plánovaná dobu životnosti clustra. Spoločnsť Red Hat garantuje podporu pre každú verziu OS 7 rokov od uvedenia verzia na trh.
    - Basic - web support, 2 dni reakčný čas
    - Standard - 12x5 telefonická podpora, web support
    - **Premium** - 24x7 telefonická podpora, web support (doporučujeme)

Cluster softvér

- Red Hat Cluster Suite. Obsahuje všetky potrebné komponenty pre vytvorenie HA + load balancing clustra. Obstaráva sa ako nadstavba nad RHEL, podpora sa zakupuje na dobu 1 rok.

Iné softvérové vybavenie, zálohovací softvér

- web server Apache, PHP, firewall, iné - sú súčasťou vybavenia RHEL5. Všetky aplikácie majú podporu pokrytú podporou pre RHEL, vrátane security updates.
- zálohovací softvér je súčasťou riešenia. Zálohy je možné uploadovať na dedikovaný zálohovací priestor na fileserveri ŠÚ SR (1st stage backup), ten je možné zálohovať (2nd stage backup) stávajúcim zalohovacím softvérom ŠÚ SR - HP Data Protector bez nutnosti dokupovania ďalších licencií.

Špecifikácia požiadaviek na sieťové pripojenie clustra

Pripojenie na sieťovú infraštruktúru ŠÚ SR bude realizované 2x 100 mbps ethernetom za sieťovým prvkom provider ISP. Web cluster vyžaduje vlastnú verejnú IPv4 adresu alebo prekladanú IP adresu z rozsahu použitého za routrom ISP. Sieťová konektivita ŠÚ SR k poskytovateľovi Internetu (ISP) je pre účely riešenia postačujúca (30 mbps).

Špecifikácia požiadaviek na zdokumentovanie IS

- Prevádzková (systémovo-prevádzková) dokumentácia.

Kalkulácia ceny: **Konfigurácia SW infraštruktúry a technická podpora SW vybavenia pre potreby fungovania aplikácie webStat**

Konfigurácia SW infraštruktúry:

	bez DPH 19 % Sk	s DPH 19% Sk	DPH 19% Sk
Konfigurácia Red Hat Enterprise Linux Premium	64680	76969	12289
Konfigurácia clusterového riešenia Red Hat Enterprise Linux Premium	50820	60476	9656
Konfigurácia SW www serverov	25410	30238	4828
Konfigurácia manažérskeho servera	50820	60476	9656
Konfigurácia CISCO switchow	13860	16493	2633
spolu	**205590**	**244652**	**39062**

Ceny podľa platného cenníka firmy Partner Soft za rok 2008.

Technická podpora SW vybavenia:

	jedn.cena Sk	ks	cena spolu Sk bez DPH	s DPH Sk	DPH Sk
MCT0798F3 Red Hat Enterprise Linux Premium (up to 2 sockets)	31301	5	156505	186240	29736
RedHat Cluster Suite MCT0367F3	12020	2	24041	28608	4568
Spolu			**180545**	**214849**	**34304**

Ceny produktov za ročný update. (Podľa cenníka Red Hat)